Table of Contents

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Andreessen Horowitz ("a16z")

March 3, 2023

BY E-MAIL

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
[redacted]

Re: Request for Information: Digital Assets Research and Development (2023-01534)

Dear Ms. Wallace,

Andreessen Horowitz ("a16z") welcomes the opportunity to reply to the Request for Information, entitled "Digital Assets Research and Development" (the "Request"), issued by the Office of Science and Technology Policy (the "OSTP") on January 25, 2023.[1] Federal investments in research and development ("R&D") are essential to maintaining the United States' technological leadership in the world, and we applaud the OSTP for transparently soliciting information from the private sector about how the government can best deploy its limited resources to support R&D in the blockchain ecosystem.

At a16z, we believe that blockchain technology is a momentous achievement in the development of the Internet and that it has incredible potential to promote innovation and economic growth. Since it was first developed in 2008, the blockchain ecosystem has grown rapidly, and our firm has been at the forefront of advancing the industry through investments in web3 companies. Like the OSTP, we are also deeply committed to technology R&D. As part of that commitment, we announced the formation of a16z crypto research last year, which includes a team of academic researchers from Columbia, Georgetown, Harvard, and Stanford Universities who specialize in cryptographic protocols, zero-knowledge proofs, computer and web security, and many other subjects.[2] We hope that our observations, drawn from our experience in investing in the blockchain ecosystem and internal R&D projects, can be of assistance to the OSTP in accomplishing its aims.

Our comment letter is divided into three parts: ***First***, we discuss R&D opportunities for lowering the environmental costs of participating in the blockchain ecosystem, as well as how leveraging

[1] Off. of Sci. & Tech. Pol'y, *Request for Information: Digital Assets Research and Development*, 88 FR 5043 (Jan. 26, 2023), *available* here.
[2] Ali Yahya & Chris Dixon, *Announcing a16z crypto research*, Andreessen Horowitz (Apr. 21, 2022), *available* here.

blockchains can improve traditional climate solutions. ***Second***, we describe the benefits of privacy-preserving technologies and how R&D related to zero-knowledge proofs could mitigate certain illicit finance risks. ***Lastly***, we discuss the resilience of well-functioning decentralized finance ("DeFi") protocols to recent market pressure, and how R&D relating to collateralization requirements and algorithmic settlement mechanisms for borrowing and lending protocols as well as algorithmic stablecoin protocols can help increase consumer protection and confidence.

A. About a16z

Andreessen Horowitz, also referred to as a16z, is a venture capital firm that backs entrepreneurs building the future through technology. We invest in seed, venture, and late-stage technology companies, focused on bio/healthcare, consumer, crypto, enterprise, fintech, and games. The firm currently has $35 billion in committed capital under management across multiple funds.

A16z aims to connect entrepreneurs, investors, executives, engineers, academics, industry experts, and others in the technology ecosystem. We have built a network of experts, including technical and executive talent, top media and marketing resources, Fortune 500/Global 2000 companies, as well as other technology decision makers, influencers, and key opinion leaders. A16z uses this network to help our portfolio companies grow their businesses.

At a16z, we believe we need an Internet that can help the United States retain leadership in a world of increasing competition, unlock opportunity for the millions on the margins of the innovation economy, and enable people to take control of their digital information. The solution is web3 — the third generation of the Internet — a group of technologies that encompasses digital assets, decentralized applications and finance, blockchains, tokens, and decentralized autonomous organizations. Together, these tools enable new forms of human collaboration. They can break through the stalemates that define too many aspects of public life and help communities make better collective decisions about critical issues, such as how networks will evolve and how economic benefits will be distributed. We are radically optimistic about the potential of web3 to restore trust in institutions and expand access to opportunity.

I. Climate

We strongly support the efforts of the Biden administration to address climate change and work toward a future of net-zero carbon emissions, and we believe that blockchain technology has an essential role to play in this regard. Based on our experience, we suggest that the best way to approach climate

R&D in the blockchain ecosystem is to focus on two research topics.[3] The first is how to lower the environmental costs of participating in the blockchain ecosystem, and the second is how to leverage blockchain technology to address carbon emissions across industries.

A. Lowering the Environmental Costs of Blockchain Technology

Consensus Mechanisms: Consensus mechanisms — the technological methodology that governs how blockchain network participants agree on transactions to verify and add to a network[4] — should be a focus of R&D, as advancements in this area have already proven to significantly decrease energy consumption in blockchain ecosystems. When developers first introduced blockchains more than one decade ago, the networks consumed significant electricity because they relied on an energy-intensive consensus mechanism known as "Proof of Work."[5] But, as discussed below, that is generally no longer necessary because industry has developed newer consensus mechanisms, including "Proof of Stake,"[6] that do not require significant energy expenditure. The success of these efforts suggests that blockchains need not have seriously detrimental effects on the environment, and that there is considerable value from investing public resources into R&D on how to further lower the environmental costs of blockchains.

Industry's shift toward greater environmental responsibility has become particularly apparent in the last three years. Arguably, the most important example of this occurred last year with the conversion of Ethereum, the second-largest blockchain network, to the Proof of Stake consensus mechanism.[7] As a result, Ethereum's energy consumption decreased by approximately 99.95%,[8] which in practical terms is equivalent to the difference between the total energy requirements of Finland and that of a small town of 2,100 homes.[9] Notably, other networks have also made significant strides toward energy efficiency. The Avalanche network, for instance, uses a novel consensus model that requires only a small fraction of the

---

[3] For more information, *see* Jai Ramaswamy et al., *Comments in Response to the Commission's Request for Information on Climate-Related Financial Risk*, Andreessen Horowitz (Oct. 25, 2022), *available* here.
[4] *See Consensus Mechanisms*, Ethereum (Jan. 13, 2023), *available* here.
[5] *See Proof-of-Work*, Ethereum, *available* here (last updated Sept. 26, 2022).
[6] *See Proof-of-Stake*, Ethereum, *available* here (last updated Jan. 12, 2023).
[7] *See The Merge*, Ethereum, *available* here (last updated Mar. 1, 2023).
[8] Carl Beekhuizen, *Ethereum's Energy Usage Will Soon Decrease by ~99.95%*, Ethereum (May 18, 2021), *available* here.
[9] *See id.*; Sam Kessler, *The Ethereum Merge Is Done, Opening a New Era for the Second-Biggest Blockchain*, CoinDesk (Sept. 14, 2022), *available* here (last updated Nov. 7, 2022).

energy used by the Bitcoin network.[10] And there are many other network examples as well,[11] which suggests that consensus mechanisms are still fertile ground for further R&D.

Sharding: R&D should also focus on a network update known as "sharding." Sharding refers to the splitting of a database or network horizontally into different hubs, i.e., "shards," to handle large amounts of data and transaction loads.[12] Each shard comprises different nodes on the network, and those nodes are responsible for verifying only a portion of a network's transactions, instead of all of the network's transactions. Separating nodes into shards reduces the burden on each node, increases throughput (i.e., capacity), and decreases hardware requirements. The overall effect is a more energy-efficient network.[13] The emergence of this network update has also given rise to certain challenges, like the potential for malicious actors to manipulate individual shards,[14] but for that reason, increased R&D is essential to making sharding a more widespread network feature.

Zero-Knowledge Proofs: We discuss zero-knowledge proofs in further detail below in Section III, but we note here that advancements in such proofs could also help lower the environmental costs of blockchains because they allow for more scalable execution of transactions and thus a lower carbon footprint.[15]

B. Leveraging Blockchain Technology to Address Carbon Emissions Across Industries

Carbon Credits: Carbon credits represent reductions of carbon emissions that may be utilized to offset emissions produced by a corporate entity. The market for carbon credits is largely unregulated and

[10] Avalanche, *CCRI Finds Avalanche to Consume 35,000x Less Energy Than Ethereum and 200,000x Less Than Bitcoin*, Medium (Feb. 2, 2022), *available* here. A16z crypto is an investor in Avalanche. *See* Avalanche, *AVA Labs Newsletter #1*, Medium (June 10, 2019), *available* here. A list of investments made by funds managed by a16z is available here.
[11] *See, e.g.*, Celo, Chia Network, Solana. A16z crypto is an investor in Celo, the Chia Network, and Solana. *See* Katie Haun & Denis Nazarov, *Celo*, Andreessen Horowitz (Apr. 2, 2019), *available* here; *Our Investors*, Chia Network, *available* here; Austin Federa, *Solana Labs Completes a $314.15M Private Token Sale Led by Andreessen Horowitz and Polychain Capital*, Solana (June 9, 2021), *available* here. Note that Celo is also the first carbon-negative blockchain. In addition to using Proof of Stake, Celo contributes daily carbon offsets through its network, making the operational resources powering its platform carbon-negative from the outset. Celo Foundation, *A Carbon Negative Blockchain? It's Here and it's Celo.*, The Celo Blog (May 26, 2021), *available* here.
[12] *What is sharding?*, Ethereum, *available* here (last updated on Mar. 1, 2023).
[13] For example, the NEAR Protocol has a fully-sharded network. *See* Near Team, *Blockchain & Sustainability: How NEAR Uses Sharding for a More Sustainable Future*, Medium (Dec. 29, 2021), *available* here. A16z crypto is an investor in the NEAR Protocol. Mike Butcher, *NEAR Protocol raises $21.6M from A16Z and launches its MainNet, beating Ethereum 2.0*, TechCrunch (May 4, 2020), *available* here.
[14] *See* Vitalik Buterin, *Why sharding is great: demystifying the technical properties* (Apr. 7, 2021), *available* here.
[15] *Zero-Knowledge Rollups*, Ethereum, *available* here (last updated Jan. 22, 2023).

notoriously opaque,[16] making it possible for entities to purchase and claim offsets that either have a dubious connection to bona fide reductions in carbon emissions, or have already been claimed.[17] But by using digital tokens to represent a carbon credit, it is possible to establish an inalterable, easily accessible, and publicly available record for carbon credits.

One of our portfolio companies, Flowcarbon, has led industry efforts to develop tokens for reliable, voluntary carbon credits. Earlier last year, in a comment to the OSTP, Flowcarbon and others described the potential for blockchains to improve the markets for carbon credits by increasing liquidity and transparency and lowering costs of engaging in transactions, among other things.[18] Since then, Flowcarbon has continued its vital work, raising an additional $70 million in a fundraising round led by our fund[19] and announcing new efforts to advance the tokenized carbon credit market, including originating the first-ever on-chain syndication of a forward carbon contract[20] and leading blockchain advocacy efforts with Verra and Gold Standard, two major voluntary carbon crediting agencies. These achievements indicate an increasing likelihood of success for integrating blockchain in carbon credit markets, and that additional R&D could help boost the process.

Peer-to-Peer Energy: Micro-grid or off-grid energy is energy that is not generated on a main power grid, but rather is produced by autonomous individuals through wind, sunlight, and other sources. In recent years, individuals have increased production of micro-grid and off-grid energy,[21] but the peer-to-peer market for it has remained largely nascent because such individuals cannot efficiently transfer excess energy to others. This results in significant inefficiencies because small scale and retail producers are treated differently than utility scale producers, effectively forcing potential consumers to depend on increasingly unreliable centralized power sources.[22]

Blockchains could potentially address these inefficiencies. More specifically, producers of micro-grid and off-grid energy could use digital tokens to record data regarding energy generation and consumption, which would both aggregate the data and make it available and transparent for potential consumers. And blockchain project developers could program smart contracts to enable the delivery of

---

[16] *Voluntary Carbon Markets: Analysis of Regulatory Oversight in the US*, ISDA (June 2022), *available* here; Brad Denig et al., *Voluntary Carbon Markets in 2023: A Bumpy Road Behind, Crossroads Ahead*, Bain & Co. (Feb. 13, 2023), *available* here.
[17] *See, e.g.*, Ben Elgin, *These Trees Are Not What They Seem*, Bloomberg (Dec. 9, 2020), *available* here.
[18] Dana Gibber et al., *An Open Letter to the Office of Science & Technology Policy* (May 9, 2022), *available* here.
[19] *Flowcarbon Raises $70M to Tokenize Carbon Credits and Build an On-chain Market*, Flowcarbon (May 24, 2022), *available* here.
[20] Flowcarbon Nature Offsets Series 1, *available* here.
[21] *Distributed Generation of Electricity and its Environmental Impacts*, Environmental Protection Agency, *available* here (last updated June 23, 2022).
[22] Katherine Blunt, *America's Power Grid Is Increasingly Unreliable*, Wall St. J. (Feb. 18, 2022), *available* here.

energy.[23] These conceptual tools increase the potential for a blockchain-based peer-to-peer energy market, but importantly, R&D is still needed to address preliminary challenges, like the lack of grid infrastructure and regulatory uncertainty. Given the possibilities for this market, we suggest that the federal government consider deploying its resources in this area.

II. Privacy-Preserving Technologies

Transparency is a significant and frequently praised attribute of blockchains because it virtually exposes fraud and provides real-time access to all of a network's transactions. But full transparency also has important drawbacks. On most public blockchains, for example, all of a person's digital assets and transactions are readily available for anyone to see, including adversaries of the United States, non-state cybercriminals, and others.[24] While it is true that a veneer of anonymity does exist on transparent chains because wallet addresses are pseudonymous, data analytics have become increasingly good at discovering wallet owners' true identities.[25] As a result, without additional privacy, many people will forgo opportunities to use blockchains.[26]

Privacy-preserving technologies, including enhanced layer-1 blockchains and similar technologies, have emerged as an effective solution to this problem, decreasing the risk of bad-actor surveillance, honey-potting data, and other potentially harmful consequences of transparency.[27] But the development of these tools has also raised novel challenges with respect to bad actors taking advantage of these technologies to launder money and engage in financial crimes. Because these legitimate national security concerns could ultimately prevent the American public from realizing the benefits of privacy-preserving technologies, we have invested resources in researching new risk mitigation tools that would help expose nefarious activities. As discussed below, our research indicates that developers can use zero-knowledge proofs to mitigate the most serious risks, and we suggest that federal R&D focus on these proofs as a starting point for further innovation in this area.

[23] Ayman Esmat et al., *A novel decentralized platform for peer-to-peer energy trading market with blockchain technology*, Appl. Energy (2021), *available* here.
[24] Elena Nadolinski, *Is Bitcoin & Ethereum really private?*, Iron Fish (Mar. 3, 2021), *available* here. A16z Crypto is an investor in Iron Fish. Ali Yahya et al., *Investing in Iron Fish*, Andreessen Horowitz (Nov. 30, 2021), *available* here.
[25] *See* Justin Sherman, *Big Data May Not Know Your Name. But It Knows Everything Else*, Wired (Dec. 19, 2021), *available* here.
[26] Alex Pruden, *What does Transparency Cost You?*, Aleo (Feb. 3, 2021), *available* here. A16z Crypto is an investor in Aleo. Katie Haun & Ali Yahya, *Investing in Aleo*, Andreessen Horowitz (Apr. 20, 2021), *available* here.
[27] Craig Timm, *The Importance of Responsible Privacy in Digital Assets*, Iron Fish (Oct. 6, 2022), *available* here.

A. Using Zero-Knowledge Proof to Mitigate the Risks of Privacy-Preserving Technologies

Zero-knowledge proofs enable private transactions on a public blockchain. At their core, a zero-knowledge proof is a way for one party, called a "prover," to convince another party, a "verifier," that a certain statement is true, while revealing nothing about the underlying data that makes the statement true.[28] As described in our paper linked below, the same zero-knowledge proof technology that enables privacy-preserving technologies could also be used to prevent the abuse of such privacy-preserving protocols by bad actors. In particular, this can be achieved because zero-knowledge proofs could enable selective disclosures of information necessary for regulatory compliance, without compromising sensitive user data.

Based on our research, we suggest the following potential methods for mitigating risks associated with privacy-preserving technologies: (1) *Withdrawal screening* to prevent withdrawals from sanctioned addresses or addresses associated with illegal activity; (2) *Voluntary selective de-anonymization*, which provides persons who believe that they have been erroneously added to a sanctions list with the option to de-anonymize the details of their transaction to selected or designated parties; and (3) *Involuntary selective de-anonymization*, which involves a private-key-sharing arrangement between a gatekeeper entity (like a non-profit or other trusted organization) and the government, where the gatekeeper entity evaluates requests from the government to use the private keys to de-anonymize wallet addresses.[29] These options above all utilize zero-knowledge proofs.

At this preliminary stage of research, we believe that these are the best available options for using zero-knowledge proofs to mitigate the risks of illicit activities and other financial crimes. But we suggest that additional government R&D focus on whether a particular one of these methods, a combination of them, or an entirely different method altogether is best suited to provide the optimal safeguards. A diversity of activity in the blockchain ecosystem may require developers to consider multiple approaches, and investment of public resources would be of significant value to them in finding the correct approach.

III. Decentralized Finance

While still in their early days, DeFi protocols have shown enormous potential to provide significant advantages over traditional financial institutions. These advantages include real-time value movement, cheaper settlement, incentive alignment, automation of multi-party operational activities, increased liquidity and transparency, less asymmetric information, and many others.[30] Importantly,

[28] *What are zero-knowledge proofs?*, Ethereum, *available* here (last updated Mar. 1, 2023).
[29] For more information on mitigation methodologies using zero-knowledge proofs, *see* Joseph Burleson et al., *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs*, Andreessen Horowitz (Nov. 16, 2022), *available* here.
[30] Jason Ekberg et al., *It's Time to Explore Institutional DeFi*, Oliver Wyman (Nov. 2, 2022), *available* here.

millions of market participants already benefit from these advantages. In spite of recent market turbulence, DeFi protocols have demonstrated significant resilience to pressure,[31] and the total value locked ("TVL") in DeFi platforms was $42 billion at the end of last year.[32]

Given DeFi's large market share of web3 activity, its potential for growth, and its potential importance to the United States' financial system, the government should focus R&D on ways to encourage further development in the sector. Many research opportunities are available, but we suggest that the government focus its efforts on collateralization and algorithmic settlement tools utilized in borrowing and lending protocols (e.g., Compound Finance[33] and Aave), as well as in algorithmic stablecoin protocols (e.g., Maker[34] and Frax). In particular, the government should conduct research regarding the types and amounts of collateral as well as the algorithmic settlement mechanisms that would make such protocols sufficiently safe for public use. This research topic is particularly important because borrowing and lending protocols and algorithmic stablecoin protocols are an essential part of the DeFi ecosystem, but also are frequently misunderstood and sometimes the target of legislative proposals that seek to ban them. As discussed further below, we believe that these proposals are highly misguided because current evidence, drawn from the performance of borrowing and lending protocols and algorithmic stablecoin protocols in recent market volatility, already suggests that reasonable collateralization requirements and algorithmic settlement mechanisms are sufficient to protect consumers, and increased R&D in this area could help in determining standards and specifications that would ensure consumer safety.

A. Algorithmic Settlement Mechanisms Are Not Inherently Problematic

As mentioned above, lawmakers and regulators commonly focus on stablecoins that employ algorithms, i.e., algorithmic stablecoins, as a risk area. But that overly broad concern is largely misplaced because it focuses on algorithms as a source of instability, rather than the real problem — under-collateralization. Nearly one year into the current market volatility, we now know that the vast majority of algorithmic stablecoin projects have performed remarkably well, and the exceptional few that did not were significantly under-collateralized, and they relied on collateral created by the issuers

---

[31] Shai Bernstein & Scott Duke Kominers, *Why Decentralized Crypto Platforms Are Weathering the Crash*, Harv. Bus. Rev. (Dec. 7, 2022), *available* here.

[32] DeFi's TVL lost 76% in dollar terms in 2022, but the total figure is up 6,900% since 2020 and 264% since the start of 2021. *See* Nansen Team, *DeFi Statistics [updated in 2023]*, Nansen (Dec. 29, 2022), *available* here. A16z crypto is an investor in Nansen. Nansen Team, *Nansen Raises $12 Million in Series A Funding*, Nansen (June 29, 2021), *available* here.

[33] A16z Crypto is an investor in Compound. *See* Leigh Cuen, DeFi Startup Compound Finance Raises $25 Million Series A Led by A16z, CoinDesk (Nov. 14, 2019), *available* here (last updated Sept. 13, 2021).

[34] A16z Crypto is an investor in Maker. *See* Katie Haun & Jesse Walden, *Maker*, Andreessen Horowitz (Sept. 24, 2018), *available* here.

themselves.[35] Importantly, the reason for the relative safety of algorithmic stablecoins was precisely because of the blockchain programmability that creates certain key risk controls typical in traditional clearing infrastructure, including, among other things, the liquidation of collateral, which protected investors and protocol safety and soundness far more transparently and efficiently than a manual process would have.

One of the core principles of DeFi is that automated smart contract safeguards of user funds are a suitable replacement for human intermediaries. For borrowing and lending protocols as well as algorithmic stablecoin protocols, such safeguards depend on algorithmic settlement mechanisms that function similarly. These protocols typically allow users to deposit approved collateral (e.g., bitcoin, ether, etc.). Borrowing and lending protocols then enable users to borrow other cryptocurrencies up to the approved collateralization ratios of the protocol's decentralized autonomous organization ("DAO") for such deposited collateral (the "Collateralization Ratio"). Meanwhile, algorithmic stablecoin protocols enable users to mint a stablecoin up to the Collateralization Ratio approved by the protocol's DAO for such deposited collateral.

The minting of stablecoins entails essentially the same process of borrowing; the main difference is that the stablecoin protocol creates the stablecoin, whereas the borrowing and lending protocols lend to other users. In each case, the protocols utilize Collateralization Ratios to establish how much a user can borrow based on deposited collateral. The algorithmic settlement mechanisms of these protocols (sometimes referred to as "liquidation mechanisms") then automatically execute if the value of cryptocurrency issued by the protocols relative to the value of the collateral falls below the required Collateralization Ratios. Such algorithms automatically liquidate the user's collateral and sell or exchange it for the borrowed asset.

To help illustrate this point, we can use an example of an algorithmic stablecoin protocol that requires users to deposit ether as collateral. The protocol requires a Collateralization Ratio of 150% (i.e., that the value of the collateral be worth at least 150% of the value the users intend to mint in the stablecoins of the protocol). While those stablecoins are outstanding, if the price of ether declines such that the value of users' collateral falls below the Collateralization Ratio for the protocol, the users' collateral is automatically liquidated, and the ether is sold to close out the loaned stablecoin that the users minted. All of this happens automatically and autonomously, ensuring that the protocols' collateral never falls below the value of the outstanding stablecoin.[36] These algorithmic settlement mechanisms utilized by borrowing and lending protocols and algorithmic stablecoin protocols are a fundamental building block of DeFi, and hundreds of DeFi protocols use similar mechanisms. As a result, blunt and broad

---

[35] *See* Miles Jennings, *In defence of stablecoins*, Financial Times (Aug. 7, 2022), *available* here.
[36] *See* Robert Leshner & Geoffrey Hayes, *Compound: The Money Market Protocol*, Compound (Feb. 2019), *available* here.

attacks on algorithmic settlement mechanisms like those that enable the functioning of algorithmic stablecoin protocols could destabilize the DeFi ecosystem. And that destabilization will likely result in substantial losses to users, drive innovation offshore, and jeopardize the United States' ability to influence the blockchain ecosystem.

Accordingly, R&D should be conducted as to the types of algorithmic settlement mechanisms that provide the greatest protection for consumers. For example, certain DeFi protocols utilize mechanisms that sell liquidated collateral automatically in order to extinguish the liabilities of the protocol. Others use manual auctions that rely on third-party participants to purchase the collateral. Investigation into the robustness and appropriateness of these mechanisms could significantly increase consumer protection among DeFi protocols and provide ample evidence that broad bans of algorithmic settlement mechanisms are unnecessary.

B. The Types of Collateral and Collateralization Ratios Utilized In DeFi Protocols Are Critical For Consumer Safety

Given the success of borrowing and lending protocols utilizing conservative Collateralization Ratios and over-collateralized stablecoins during heavily volatile periods, the focus of R&D should be on their relative safety to assess which collateral and Collateralization Ratios might be sufficient to permit safe public use of borrowing and lending protocols and algorithmic stablecoin protocols. For example, R&D could feasibly determine that only digital assets with a market capitalization in excess of a certain dollar threshold should be used as collateral to ensure that bad actors cannot easily manipulate the collateralized assets. Further, Collateralization Ratios above 125% have proven to be effective for highly liquid digital assets (e.g., bitcoin, ether, etc.) in the recent volatility and are worth further exploration.

R&D on types of collateral and Collateralization Requirements will also help undermine harmful attempts to broadly ban algorithmic settlement mechanisms, including those utilized by algorithmic stablecoin protocols. While we appreciate the government's interest in ensuring consumer protection in the DeFi ecosystem, we note that a ban of such mechanisms may hurt the international financial system for numerous reasons. For one, banning such mechanisms could substantially undermine the promises and benefits of DeFi, including financial inclusion. Second, stablecoins, both custodial and algorithmic, provide stability in countries where centralized monetary policy has failed.[37] And as more countries face growing inflation pressures, we expect stablecoin usage to increase.[38] In addition, because algorithms are key not only to DeFi but also to other aspects of the digital asset markets, a disproportionate regulatory

[37] Chainalysis Team, *Latin America's Key Crypto Adoption Drivers: Storing Value, Sending Remittances, and Seeking Alpha*, Chainalysis (Oct. 20, 2022), *available* here.

[38] The top five worst countries for inflation are Argentina (98.8%), Lebanon (124%), Syria (139%), Venezuela (156%), and Zimbabwe (230%). *See Inflation Rate / World*, Trading Economics, *available* here.

focus on algorithms as a source of instability could be perceived by industry as a threat to blockchain projects broadly. Engaging in appropriately focused R&D will help avoid these unintended results.

IV. Importance of Government Involvement in Blockchain R&D

We strongly agree with the policies outlined in President Biden's Executive Order on Digital Assets calling for the United States to maintain "technological leadership" in the digital asset space,[39] and we believe that prioritizing R&D in the blockchain ecosystem is essential to accomplishing that goal. We urge the OSTP to act expeditiously to account for the industry's national security importance to the United States.[40]

Specifically, many of our adversaries, including Russia and China, are developing government-backed blockchain protocols that, if exported and adopted at scale, like some current app-based products, could provide the associated foreign government with access to personally identifiable information, sensitive financial data, and data on shipping and cargo flows (for enterprise blockchains and, potentially, payment blockchains). In addition, American leadership in the economic sector and the dominance of the dollar could be threatened by the development of other national and regional central bank digital currency projects.[41] Without prompt R&D, we risk losing ground in the crypto space to other countries. For that reason, we reiterate our wholehearted support for the OSTP's efforts, and we welcome further discussion on how to keep the United States ahead of the crypto technology curve.

---

[39] Exec. Order No. 14067, 87 Fed. Reg. 14143 (Mar. 14, 2022), *available* here.

[40] *See* Faryar Shirzad, *National Security in the Age of Digital Innovation: The Critical Role of Crypto*, Coinbase (Jan. 20, 2023), *available* here.

[41] Georgia Quinn, *How Washington can protect U.S. dollar hegemony with stablecoins*, American Banker (Aug. 8, 2022), *available* here.

V. Conclusion

R&D is critical to the development of the blockchain ecosystem, as the technology rapidly becomes a key pillar of the global financial system and the Internet. We greatly appreciate the opportunity to provide comments on these matters, and we look forward to continuing engagement with the OSTP.

Respectfully submitted,

Miles Jennings, General Counsel and Head of Decentralization
a16z crypto

Michele R. Korver, Head of Regulatory
a16z crypto

Brian Quintenz, Head of Policy
a16z crypto

Tim Roughgarden, Head of Research
a16z crypto

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Acctual

From:	Mohamedeq Mohamed
To:	DARD-FTAC-RFI
Cc:	Atikh Bana
Subject:	RFI Response: Digital Assets R&D Agenda
Date:	Thursday, February 2, 2023 8:05:37 PM

Dear OSTP,

As you are aware, digital assets are rapidly changing the financial landscape, with stablecoins leading the way. These digital assets have the potential to revolutionize the way we think about money, with fast, low-cost, and secure transactions. The adoption of stablecoins and other digital assets is becoming increasingly widespread, making it more important than ever for businesses to understand and embrace this technology.

As a member of Acctual, a crypto sub-ledger organization, we are writing to share our insights and perspectives on the advancement of digital assets. The integration of our crypto sub-ledger with Accounts Payable and Accounts Receivable (AP/AR) sets us at the forefront of the future of B2B payments, specifically using stablecoins. The inclusion of Know Your Customer (KYC), Anti-Money Laundering (AML), and other security measures ensure that the transactions and accounting for digital assets are secure and compliant.

The growing popularity and importance of digital assets cannot be ignored. With the integration of stablecoins, the potential for digital assets to disrupt traditional financial systems and offer new solutions for businesses and consumers alike is immense. The use of digital assets as a means of payment and store of value provides increased efficiency and accessibility, particularly for those who are currently unbanked or underserved by traditional financial institutions.

The United States, as a leader in the financial industry, has a responsibility to stay ahead of the curve and ensure that the evolution of digital assets is done in a fair and secure manner for all global consumers and businesses. It is imperative that proper measures are put in place to protect the integrity and dignity of the US financial systems and businesses while providing a safe and secure environment for the growth and development of digital assets.

As a crypto sub-ledger organization, we understand the importance of instilling protections and ensuring that the evolution of digital assets is done in a responsible and secure manner. We are more than willing to contribute to the development and growth of digital assets by providing research and guidance for its adoption. Our goal is to be at the forefront of this evolution and help shape its future for the better.

If there is anything we can assist with or if you have any questions, please don't hesitate to reach out.

Best regards,
Atikh B. and Mohamedeq M.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

American Civil Liberties Union (ACLU)

Office of Science and Technology Policy
Executive Office of the President
[redacted]

March 3, 2023

Re: Comments of the American Civil Liberties Union to the White House Office of Science and Technology Policy regarding Digital Assets Research and Development [FR Doc. 2023–0153]

These comments are being submitted by the American Civil Liberties Union (ACLU). For more than 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. The ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual' s rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

The comments below were published on March 3, 2023 as an ACLU white paper, "Paths Toward an Acceptable Public Digital Currency."

Paths Toward an Acceptable Public Digital Currency
Serious discussions are underway inside the U.S. Federal Reserve and other central banks around the world on creating a new form of government-issued digital money. The Fed has already issued a policy paper and research report evaluating the idea, and in March, President Biden issued an executive order directing that the executive branch place "the highest priority on research and development" of such a "digital dollar."

There are good reasons to embrace the idea of a digital dollar (often called a "Central Bank Digital Currency," or CBDC, though such a currency could also be issued by the Treasury Department). There is clearly a high demand for digital monetary transactions in today's world, yet all the options for carrying out such transactions rely on private companies that have troubling records on privacy, freedom of expression, and accessibility — especially compared to the government currency that we already have: cash. Cash has a set of qualities that are good for freedom: It is universally accessible, universally accepted, relatively stable in value, and can be exchanged for goods and services without transaction fees. It can be used offline, and it lends itself to privacy, anonymity, free expression, and user control.

The companies that currently provide our electronic money, including the credit card oligopoly as well as payment networks such as Paypal and Venmo, spy on their customers' transactions. They frequently block transactions that they don't like, such as those related to sex or to political causes that are unpopular with the public — or with the government. And they are terrible when it comes to accessibility for people who are low-income or marginalized from the bureaucratic and technological structures that one must navigate to participate in digital transactions. The often exploitative fees they charge pose more barriers and suck dollars out of the economy for providing functions that could easily be provided for free by a true digital dollar.

Is cryptocurrency the answer? We share the values of those cryptocurrency and blockchain enthusiasts who embrace the technology because they believe money should be private and permissionless. But despite its enormous expansion as a speculative instrument, cryptocurrency has not become fully functional as an actual currency. While it has proven useful for some purposes such as making anonymous charitable contributions, vanishingly few retail purchases are being made with cryptocurrency. Built on the ideals of decentralization and disintermediation of legacy financial institutions, it has become centralized and institutionalized. It requires some tech savvy and can't be used without an internet connection, which doesn't work for people who lack consistent quality access. And cryptocurrency has not lived up to the hopes it would protect privacy.

We can't predict how these technologies will evolve and what implications such evolution may have for civil liberties. Tools have been developed that can make cryptocurrencies more "cash-like" in their privacy, and the government should accept those tools insofar as they apply to ordinary people and transactions and otherwise conform to the principles we lay out here for a CBDC. But whatever uses cryptocurrencies come to serve in our society, we don't believe that they will become a functional digital dollar anytime soon.

That brings us back to a CBDC as a possible means of achieving a better digital payment system. The biggest problem with a government digital dollar is the prospect that it would be even worse for privacy than the companies we have now. There is little doubt that law enforcement and national security interests within the government will push for a system design that gives them sweeping powers to monitor and investigate even the smallest financial transactions. Some are skeptical that our government will ever allow a privacy-protective CBDC to come into effect.

On the other hand, it's safe to say that most Americans would not want a currency system that creates a government record every time they give a friend money for beer or pay a kid to mow their lawn. There are good reasons to think that libertarians, civil libertarians, liberals, conservatives, and populists would all for their own reasons oppose such a system and insist that any CBDC offer robust privacy protections.

A menu of options

The balance that will be struck between the government's ability to oversee financial transactions and the civil liberties interests in a free and private currency will be worked out through the design choices that are made in the creation of a public digital currency. So those design choices — whether made by the Fed, the executive branch, or Congress — have enormous importance.

In September 2022, the White House issued a report outlining various policy and technical options for how a public digital currency might be designed. That report provides an excellent framework for analyzing the range of options in how a CBDC could be designed, and we make use of its framework in these comments.

The paper, which was produced by the White House's Office of Science and Technology Policy (OSTP), doesn't make recommendations for how a government digital currency should be structured; instead it offers a kind of menu of technical options that policymakers will need to choose from. Many of the options described in the report would spark fierce opposition from the ACLU and other privacy and civil liberties groups — and probably from Americans across the political spectrum. But among the "menu" listings there are also the makings of a digital currency system that would be entirely acceptable, and indeed could be an affirmative good for our nation and its people.

The White House paper does make *policy* recommendations, including three that address the biggest civil liberties concerns with a government digital currency:

1. **Preserving cash.** The report declares, "Use of the CBDC system should not be mandated. Offline capability should be incorporated, and the role of cash should be preserved." At the ACLU, we regard the preservation of physical cash as the starting point of any discussion of how currency and payments should work in the future.
2. **Privacy:** The report says that a CBDC "should maintain privacy and protect against arbitrary or unlawful surveillance." That's awfully weak, because surveillance doesn't have to be arbitrary or unlawful to be deeply problematic. More promisingly, the paper says that a CBDC should incorporate "privacy engineering best practices," including "privacy by design" and "dissociability," which means minimizing the links between data and identifiable people or devices. We also view this as vital — that anonymity of transactions, at least below a certain limit that meets the needs of regular people, should be built into the technological design of the system using the best available privacy technologies.
3. **Accessibility.** "All should be able to use the CBDC system," OSTP says, and it "should expand equitable access to the financial system." This is also a crucial policy goal for any public digital currency. Fixing the inaccessibility of the current financial system would be a major reason to implement a CBDC. It's also important to note that accessibility and privacy are linked; as the White House points out, a 2020 government study found that concern about privacy is one of the top reasons that unbanked households cite for why they don't have a bank account.

At the same time, however, the paper declares as a policy goal that a CBDC should "protect national security," "promote compliance" with Anti-Money Laundering (AML) and anti-terrorist financial-surveillance laws, and "mitigate illicit finance risks."

The trillion-dollar question is how the tensions and conflicts among the goals cited in this paper will be resolved in the design of a CBDC system. To what extent will the security agencies be permitted to use the transition from physical to digital dollars to expand their already too-broad visibility into Americans' financial lives? Physical cash allows for a great deal of privacy, a certain amount of which is used for illicit activity. The security agencies already have plentiful and overbroad powers to investigate people's finances — but would no doubt love to have new surveillance superpowers to try to reduce that illicit activity. The question is whether policymakers will bake surveillance into our digital financial system and toss out what remains of Americans' financial privacy in pursuit of that aim.

We recognize that the government has a legitimate interest in monitoring the transfers of large sums of money. Wealthy tax evaders or other criminals should not be offered new ways to send millions of dollars around the world undetected. What is needed is a system that protects the privacy of ordinary people while not hiding large transactions by wealthy people and companies. As far as we're concerned, the problem of how to build a CBDC *is* the problem of how to build that kind of a system.

Privacy-protecting cryptographic innovations must be at center of a CBDC

And privacy protections based on *policy* are not good enough. No one should support a CBDC system that generates centrally held usage data about every transaction and then purports to protect that data through a warrant requirement, as the OSTP paper seems to contemplate. Nor is the protection afforded by having data held by third-party intermediaries sufficient. Given uncertainties around how the courts will interpret the Fourth Amendment and the unreliability of lawmakers in protecting privacy, Americans need to be able to trust that the privacy of their past and future transactions won't be stripped away by some crisis, panic, or bad court ruling. We want a system that uses new and existing cryptographic techniques to make it, to the greatest extent possible, *technologically* impossible for the government (or any other party) to record ordinary transactions.

As we have discussed, one solution proposed in Congress would be a digital bearer instrument in which money is stored on a device with no party keeping track of balances on a centralized (or public) ledger. That would be the best, most cash-like option for digital money if the security questions around such a system could be addressed — not necessarily perfectly, but at least to the degree that would be reasonable given the privacy advantages such an architecture would bring.

In its menu of technology options, the OSTP paper does contemplate some limited offline options. And it discusses how transactions could be "tiered" to protect privacy, "with lower tiers facilitating a higher level of privacy in transactions than higher tiers." And, as the paper points out, transactions "could be limited to the lower tier with temporal restrictions on cumulative transfer amounts." That would stop somebody from trying to hide a million-dollar transfer simply by making a million one-dollar transfers, for example.

Even in a system not based on a pure bearer instrument, there are already a number of promising cryptographic technologies that could be used to protect people's privacy. For example, untraceable e-cash is an idea introduced 40 years ago by computer scientist and cryptographer

David Chaum that by now has many well-developed realizations. It could allow the Fed to keep a central accounting of people's balances as they transact, while making it impossible for the central bank to see how much each transaction is worth and who the parties are. Other techniques include those used by privacy-protecting cryptocurrencies such as Zcash, Monero, and MobileCoin that use zero-knowledge proofs to ensure that each transaction is valid, even while hiding the details.

Another technique that cryptographers have developed would make it mathematically impossible for the Fed to see data about transactions below a certain size, but allow the agency to see the details of larger ones, or even groups of transactions that reach a certain size within a certain period of time. These kinds of limits should be baked into the technology so they can't be changed on anybody's whim. As the White House says in its report, "This could help increase consumer trust that the CBDC system's rules will not be changed haphazardly, and this could also help protect the CBDC system from being abused during periods of high political volatility."

Overall, the field of privacy-protecting cryptography is advancing quickly with a great deal of creative research that promises to allow us to "have our cake and eat it too" when it comes to privacy and security. As a result, there is absolutely no justification for a CBDC system not to make maximal use of all the latest and greatest privacy-protecting technologies.

It's true that not all of the available techniques may yet be sufficiently stress-tested for security and for practicality in actual implementation — but such testing does not happen by itself, and the federal government is in an excellent position to make sure it happens by promoting public and transparent research in cooperation with academia and other stakeholders. Indeed, the White House paper declares that "It is important that the U.S. Government direct resources and the research community toward solving" open questions about CBDC design, and that it will be "vital to bring an all-of-government approach to bear on a digital assets R&D agenda." The White House moved toward such an approach in January when it announced the creation of a government committee pursuing a "National Digital Assets Research and Development Agenda" and solicited public comments on what the research priorities should be.

Other policy choices

As we and our allies have stated before, we should aim for a digital dollar that is as close to physical cash as possible in its accessibility and protection of privacy. That has implications for a number of the other items on the CBDC design-choice menu laid out by the White House in its report. Among them are:

- **Intermediaries.** Some visions for a CBDC involve the government spinning off various functions to private companies. This may make sense in some narrow areas, but the whole point of a CBDC is to extend the role of money as a *public good* into the digital arena, not to put big banks or other financial players at the center of a system. That would allow them to continue to suck fees out of the financial system to the detriment of economic efficiency and accessibility for low-income people, and undercut much of the very rationale for a CBDC. Putting private, profit-oriented financial players at the center of a CBDC system also risks replicating the terrible privacy regime that we have now with digital transactions. As with physical cash, transacting with digital dollars should not incur fees; it should be created and run as a public good.

- **Offline transactions.** It's vital that offline and peer-to-peer transactions be enabled to the greatest extent feasible. A fully offline digital bearer instrument would be the ideal, but if that does not prove feasible, then the greatest possible degree of offline functionality should be enabled. The less frequently an internet connection is required to settle balances, the better, because the United States is a big country, and many places and people have poor to non-existent internet connectivity. Nor is it a good idea to create a payment system that stops working when there's an Internet outage due to natural disaster or other causes.
- **Fungible vs. non-fungible units.** Fungible dollars are basically all the same, while non-fungible dollars could be differentiated from each other. That means, for example, that non-fungible digital dollars could be marked or categorized in ways that make them more controllable than cash. For example, the White House points out that "non-fungible units could enable the limiting of certain CBDC to be used toward more economically-beneficial uses, especially during times of recession," and certain digital dollars "could be marked as 'tainted' if they are used in illicit activity." This would allow the authorities granular control over how dollars are spent — blocking entities from accepting certain dollars, or providing that they can only be used to buy certain things, for example. Building non-fungible units is a bad idea. It's something that could never be done with cash, and (as the OSTP paper acknowledges) opens up wide avenues for centralized control and abuse.
- **Identification requirements.** Identification requirements should be minimized. If I'm buying and selling goods at a flea market or garage sale, I don't have to register with the government to accept cash. Unless someone is engaging in transfers of large amounts of money or the like, there is no reason to require every participant in a digital currency eco-system to rigorously identify themselves to a central ledger keeper. Where identification requirements are imposed, they should also make use of cryptographic privacy-protecting ID techniques that can satisfy some of the more reasonable administrative and security needs while protecting privacy to the greatest extent possible.
- **Transparency.** It's important that the software and hardware infrastructure behind a CBDC be transparent and subject to external, independent audits. As OSTP notes, an open-source approach "increases trust, security, reproducibility, and collaboration" and could reduce barriers to adoption, while "a degree of auditability will be important" as well as "the publication of data about the CBDC system using appropriate privacy-preserving approaches." Overall, as OSTP declares, transparency "is vital for people to believe the system is sufficiently safe, effective, and private for them to use."
- **Anti-money laundering rules**. A CBDC should be subject to the rules that apply to physical cash, and not the rules that apply to bank accounts. Under current law, cash transactions of $10,000 or more must be reported to the government by anyone "engaged in a trade or business," but cash is not otherwise generally subject to surveillance. Banks, however, are required to act like proxy police officers by "proactively monitoring and investigating suspicious activity" in their customers' accounts. And currently, "regulators are putting more pressure on financial institutions to know their customers in depth." Banks are also required to keep records of their customers' transactions in case the government wants to see them — and to carry out searches of that data for the

government about any individual that any law enforcement agency claims is engaged in terrorism or money laundering.

Conclusion

CBDC policymakers and architects need a clear and early vision of what a good government digital currency system would look like. That vision should center around creating a system that replicates, to the greatest extent possible, the advantages of cash when it comes to privacy and accessibility for ordinary people. The construction of a digital dollar could, if done right, significantly advance financial inclusion and privacy. But it would be an unprecedented and historic task, potentially shaping the U.S. financial system for decades or even centuries to come. As such, its design needs to very carefully balance the government's legitimate interest in stopping large-scale tax evasion and other financial crimes against the need to keep the tentacles of its surveillance powers out of the lives of ordinary people and ordinary transactions. Such a system should reach that balance by making maximal use of the latest cryptographic innovations for protecting privacy.

###

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

ACT | The App Association (App Association)

March 3, 2023

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
[redacted]

RE: Comments of ACT | The App Association to the Office of Science and Technology Policy regarding Digital Assets Research and Development (88 FR 5043)

ACT | The App Association (App Association) appreciates the opportunity to submit views to the Office of Science and Technology Policy (OSTP) to help identify priorities for research and development related to digital assets, including various underlying technologies such as blockchain, distributed ledgers, decentralized finance, smart contracts, and related issues such as cybersecurity and privacy (e.g., cryptographic foundations and quantum resistance), programmability, and sustainability as they relate to digital assets. Specifically, the App Association provides this input to address privacy-enhancing technologies (PETs), which are an important tool for unlocking the full potential of the data economy and can help ensure that innovation in emerging technologies runs concurrently with a respect for basic human rights, promotes equity in data processing activities, and increases trust in the digital economy writ large.

The App Association represents thousands of small business software application development companies and technology firms that create the technologies that drive internet of things (IoT) use cases across consumer and enterprise contexts. Today, the ecosystem the App Association represents—which we call the app economy—is valued at approximately $1.7 trillion and is responsible for 5.9 million American jobs.[1] Alongside the world's rapid embrace of mobile technology, our members create the innovative solutions that power IoT across modalities and segments of the economy. App Association members exist at the cutting edge of the research, development, and implementation of PETs in their products and services.

Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, ensuring that the

[1] The App Association, State of the App Economy 2020, January 2021, https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.

company’s business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. For this reason, we support the Administration’s goal of ensuring the United States leads the world in responsible data practices and technologies, including PETs, which are critical to our economic prosperity and national security, and to maintaining the core values behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

I. General Comments on Privacy Enhancing Technologies

PETs encompass a “broad set of technologies that protect privacy”, listing examples such as “secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic data generation tools.”[2] While there is no universally accepted taxonomy of PETs (or definition for the term, for that matter), existing efforts typically include categories of technologies that assist in the process of obtaining consent, data minimization, anti-tracking, encryption, anonymity, and control, among other categories, in addition to the technologies mentioned in OSTP’s past PETs RFI.[3] One strategy OSTP may consider when taking stock of the full spectrum of PETs for its analysis is to either bifurcate its research into business to business (B2B) and business to consumer (B2C) buckets, or to simply track the entire life-cycle of a given piece of data in various industry verticals, from collection, to processing by the first-party collector and subsequent processing by service providers or other third-parties. This would help ensure that OSTP takes all possible PETs into account, including those utilized by B2B and B2C developers.

In general, we encourage OSTP to take as broad a view of PETs as feasible as it takes on the responsibility of coordinating the national strategy to ensure that these tools benefit individuals and society. This would track similar work carried out by allied governments and existing efforts at the congressional level. For example, the Privacy Commissioner of Canada took an inclusive view of PETs in its report, “A Review of Tools and Techniques”, saying, “PETs are intended to allow users to protect their (informational) privacy by allowing them to decide, amongst other things, what information they are willing to share with third parties such as online service providers, under what circumstances that information will be shared, and what the third parties can

[2] OSTP RFI on Advancing Privacy Enhancing Technologies, “Background”, June 9, 2022. https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies

[3] See, e.g., Office of the Privacy Commissioner of Canada, ”Privacy Enhancing Technologies -- A Review of Tools and Techniques,” November 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/ pet_201711/#fn9

ENISA, “PETs controls matrix - A systematic approach for assessing online and mobile privacy tools”, December 2016, https://www.enisa.europa.eu/publications/pets-controls-matrix use that information for."[4] In the U.S., the Promoting Digital Privacy Technologies Act, S.224, also takes a broad lens, defining PETs as "any software solution, technical processes, or other technological means of enhancing the privacy and confidentiality of an individual's personal data in data or sets of data."[5]

II. Specific Research Opportunities to Advance Privacy Enhancing Technologies

The App Association serves as a leading resource in the privacy space for thought leadership and education for the global small business technology developer community.[6] We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and usable guidance to ease the burden of compliance.[7] Furthermore, through our Innovators Network Foundation Privacy Fellowship, we support thought-leadership that covers a wide range of privacy issues, including privacy enhancing technologies.[8]

We encourage OSTP to look to existing work from the Privacy Fellows and other leading academics on this topic as it conducts further research on PETs. For example, The Rise of Privacy Tech is an organization led by Privacy Fellow Lourdes Turrecha that serves as a leading conduit for startups in the privacy technology space to connect with funders, peers, and mentors in the industry and to catalyze privacy tech innovation. Recently, The Rise of Privacy Tech published its landscape analysis, "Defining the Privacy Tech Landscape", which included a full cataloguing of the different technologies that encompass privacy tech, including PETs (noting that PETs are a subset under the larger privacy tech umbrella).[9] Their investigation covered everything from key

[4] Office of the Privacy Commissioner of Canada, "Privacy Enhancing Technologies – A Review of Tools and Techniques", November 2017,"https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

[5] U.S. House of Representatives, "Promoting Digital Privacy Technologies Act", Sec. 2, February 4, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/224/text.

[6] ACT | The App Association, Innovators Network Foundation Announces Inaugural Privacy

Fellows (September 2019), available at: https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/.

[7] See e.g., ACT | The App Association, General Data Protection Regulation Guide (May 2018), available at: https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf; What is the California Consumer Privacy Act (January 2020), available at: https://actonline.org/wp-content/uploads/What-is-CCPA.pdf.

[8] ACT | The App Association, Innovators Network Foundation Announces Inaugural Privacy Fellows (September 2019), available at: https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/

[9] The Rise of Privacy Tech, "Defining the Privacy Tech Landscape, November 2021, https://www.riseofprivacytech.com/wp-content/uploads/2021/11/TROPT-Defining-the-Privacy-Tech-Landscape-2021-v1.0-1.pdf

definitions and categorizing the different facets of the privacy tech stack, to a business analysis on the present and future of the privacy tech market.

Another Privacy Fellow, Dr. Lorrie Cranor, directs Carnegie Mellon's CyLab Security & Privacy Institute, which also conducts research at the cutting edge of certain PETs. For example, Dr. Cranor's scholarship on "privacy nutrition labels" has informed the rollout of similar labels on both of the major app platforms in recent months.[10] Dr. Cranor's research team has also been at the forefront of developing Internet of Things security labels,[11] machine extractable opt-out choices,[12] and privacy enhancing plug-ins for app developers.[13]

III. Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs

App developers are already working to adopt and implement PETs in their products, services, and features in order to meet market demands. Here are a few examples of PETs that our members rely on every day:

- On-device processing. Apps utilize on-device processing for certain sensitive features to ensure that no external processing occurs and that the company cannot see or access the data. To share one key use-case, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log-in to apps using a scan of their face from the camera app. An app developer can choose integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third-party.[14]

---

[10] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. ACM Press. https://doi.org/10.1145/ 1572532.1572538

[11] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal and L. F. Cranor, "Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?," *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 519-536, doi: 10.1109/SP40001.2021.00112.

[12] Kumar et al., "Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text". In WWW '20: The 2020 Web Conference, April 20–24, 2020, Taipei. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/1122445.1122456/.

[13] C Tianshi Li, Yuvraj Agarwal, and Jason I. Hong, Coconut: An IDE Plugin for Developing Privacy-Friendly Apps, Proc. ACM Interact Mob, Wearable Ubiquitous Technol, 2, 4, Article 178, December 2018 https://doi.org/10.1145/3287056

[14] Apple, "About Face ID advanced technology", September 14, 2021, https://support.apple.com/en-us/HT208108

- Encryption. The App Association supports fully leveraging technical measures including end-to-end encryption to protect data broadly, enabling key segments of the economy to function—from banking to national security to healthcare—by safeguarding access to, and the integrity, of data from unwanted interlopers. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. The importance of encryption to the app economy has only heightened during the COVID-19 pandemic and the increasing desire to perform traditionally offline functions in the digital space due to social distancing mandates. That's why we've been strong supporters of NIST's efforts to support the development of encryption technologies, as well as their leadership in advancing risk-based scaled approaches to cybersecurity management in the NIST Cybersecurity Framework (which includes an emphasis on encryption as a technical protection mechanism), while opposing legislation seeking to undermine end-to-end encryption, such as the Lawful Access to Encrypted Data Act or the EARN IT Act.

- App Tracking Transparency. Even as federal lawmakers debate legislation that would put new guardrails around data sharing practices in the digital economy, app developers comply with a growing number of platform-level restrictions on certain types of data sharing with third-parties. For example, Apple's App Tracking Transparency (ATT) tool creates a simple solution to the opt-in/opt-out binary by presenting users with a just-in-time push notification asking if they want to permit apps to track them across third-party tracking that follows them outside of the app onto the open web or even other third-party apps. This type of engineering solution has so far evaded an easy resolution in the policy world, but has markedly improved user privacy outcomes along the way.[15]

- Privacy Labeling. Over the past few years, the app marketplace has seen the gradual introduction of the "privacy nutrition label" concept. The contemporary version of these labels (drawing from more than a decade of scholarship with researchers proposing similar concepts in various forms)[16] aims to perform a very simple function: make app developers' privacy practices more understandable to the average consumer. Initial research demonstrates that many app developers welcome privacy nutrition labels as a convenient, efficient, and user-friendly way for them to demonstrate their privacy practices and see it as a major improvement from the previous practice of directing users to lengthy privacy policies for similar information.[17] Though we believe the app platforms

[15] Estelle Laziuk, "iOS 14.5 Opt-in Rate - Daily Updates Since Launch", Flurry (May 25, 2021), available at https://www. flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

[16] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. ACM Press. https://doi.org/10.1145/ 1572532.1572538

[17] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In CHI

could do a better job of assisting developers in the creation and maintenance of the label, we believe the concept will help to maintain trust in the app ecosystem in the long-run.

IV. **Conclusion**

The App Association appreciates OSTP's consideration of the above views. We urge OSTP to contact the undersigned with any questions or ways that we can assist moving forward.

Sincerely,

[redacted]

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Regulatory Policy Associate

ACT | The App Association
[redacted]

Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3491102.3502012

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Americans for Financial Reform Education Fund (AFREF)

Demand Progress Education Fund (DPEF)

Office of Science and Technology Policy
[redacted]
Re: Request for Information; Digital Assets Research and Development, January 26, 2023

March 3, 2023

Dear Colleagues,

Thank you for the opportunity to submit comments regarding the administration's interest in establishing a National Digital Assets Research and Development Agenda. The agency's request for information (dated January 26, 2023) seeks data and analysis regarding information on the potential benefits, risks and impacts of using digital assets and blockchain-based technology in fields beyond the financial sector, as well as ways in which further research and development could amplify such supposed benefits or mitigate risks and harms.

Americans for Financial Reform Education Fund (AFREF) is a nonpartisan, nonprofit coalition of more than two hundred civil rights, community-based, consumer, labor, small business, investor, faith-based, civic groups, and individual experts. We fight for a fair and just financial system that contributes to shared prosperity for all families and communities.

Demand Progress Education Fund (DPEF) works to elevate regulators who care more about the wellbeing of everyday people than Wall Street's bottom line, and fights to ensure that Congress conducts oversight to hold the financial sector accountable. We oppose deregulation and consolidation that makes our financial system less sound, and push back against attempts by the finance and tech sectors to normalize exploitative products and systems.

Summary

Our organizations are highly skeptical of the overall use case for crypto assets in a financial services context, especially considering the high degree of risk and harm posed by these assets as they are currently used. At a fundamental level, these products appear to have little current use beyond speculative investment – which some argue is essentially a form of gambling.[1]

While other submissions will no doubt focus on the purported or potential benefits of blockchain technology, this submission largely focuses on some of the limitations blockchain technology itself. Moreover, in this submission we urge the government to interrogate further the fundamental premise of this inquiry – that blockchain based technology is worth developing at scale, given the limitations of the technology and its value relative to alternative approaches.

[1] https://www.cnbc.com/2023/02/16/billionaire-charlie-munger-cryptocurrency-is-crazy-stupid-gambling.html

We offer here three categories of fundamental limitations or flaws found with blockchain technology – a non-exhaustive list – and provide an overview of analysis and criticism regarding these limitations which we believe raises serious questions. Following from that we offer a few broad recommendations regarding research and development informed by this critique.

Lastly, with respect to use of blockchain technology to create a US central bank digital currency (CBDC), our submission ends by summarizing concerns and recommendations regarding such a proposal that we provided to the Federal Reserve last year in response to a request for information regarding the Federal Reserve White Paper, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation" (January 2022). In short, we raise concerns about the impacts a CBDC might have on consumer and privacy rights and protections, and urge the Fed to consider non-blockchain based alternative technology for a digital dollar and other digital payment and banking systems.[2]

Introduction

Much has been written by academics,[3] public interest organizations,[4] industry observers[5], current[6] and former regulators[7], and others about the systemic problems found in the crypto asset industry, particularly in the wake of the recent collapse of Terra, FTX, and several other platforms, whose failure has driven losses of more than $2 trillion in crypto market value[8] and continues to negatively affect surviving platforms and crypto investors.

Some proponents of investing in blockchain technology acknowledge these flaws, but argue (among other points) that:

1. Blockchain is a new technology, and further development of it will resolve at least some of the flaws or limitations that currently cause or contribute to the problems found in the crypto industry and elsewhere.

2. Blockchain's key innovation is decentralization, and the benefit that decentralization brings alone is worth the resources needed to further develop the technology so it is viable and scalable for the long term.

3. The real, or perhaps more versatile application of blockchain, can be derived from its use not as a system of finance, but as a system used for information management – in short, as a database.

We believe each of the arguments are, at the very least, contestable, and may be fundamentally difficult to defend, based both on observable practices within existing blockchain infrastructure, and upon structural analyses of blockchain from various fields, including computer science, economics, and mathematics.

---

[2] https://ourfinancialsecurity.org/wp-content/uploads/2022/05/5.20.22-digital-assets-CBDC-letter.pdf

[3] https://www.banking.senate.gov/download/allen-testimony-12-14-22

[4] https://ourfinancialsecurity.org/2021/10/letters-to-regulators-letter-to-treasury-opposing-a-bank-charter-for-stablecoin-issuers/

[5] https://www.nytimes.com/2022/03/31/style/ben-mckenzie-crypto.html

[6] https://www.reuters.com/technology/us-sec-chair-gensler-calls-congress-help-rein-crypto-wild-west-2021-08-03/

[7] https://www.linkedin.com/pulse/fraudulent-design-language-cryptocurrency-john-reed-stark/?published=t

[8] https://www.cnbc.com/2022/12/23/bitcoin-lost-over-60-percent-of-its-value-in-2022.html. Note: estimates of crypto market values, market capitalization, etc., vary and are not well defined.

Below we share some of the literature and analysis available that calls into question these arguments, which often form the basis of the rationale for the continued prioritization of investment in blockchain technology.

1. Blockchain Technology Is Not New

Blockchain proponents often argue that the technology is still in the "early days" of its development. This claim is used either offensively – to suggest that the technology offers significant unrealized potential benefits that will emerge in the near future – or defensively, to explain why the consistent failures of blockchain-based technology are not indicative of its enduring limitations but constitute "growing pains" that are a natural and necessary phase in the technology's development.

A relatively well-known essay by Molly White, a software programmer and noted critic of crypto assets and blockchain, entitled, "It's not still the early days" lays out the basics of a rebuttal to this argument.[9] In summary, White points out that Bitcoin was launched in 2009; Ethereum in 2015. Many first generation and second generation blockchain applications are anywhere from 7-13 years old. During that same time range, numerous other technological products and platforms (some new, some established) have been further developed and achieved stable, widespread use more rapidly. These products include things as varied as major social media platforms, online ride-sharing apps and platforms, new computer processors, new database programs, programming languages, operating systems, payment apps, and more.

While the nature of these innovations vary widely (and bring with them their own variety of benefits and negative externalities, some of which are profound in scope and are a core focus of our advocacy efforts), what they have in common is that arguably, they have all demonstrated their relative utility, scalability and viability in a relatively short period of time. In contrast, crypto and blockchain products have not demonstrated nearly the same levels of uptake within a similar time frame.

For example, in the payments sector, blockchain-based crypto assets struggle to demonstrate their usefulness as a mainstream method of payment (though anecdotal references to their usefulness in remittances or aid-based money transfers are ubiquitous.) Yet non-blockchain based digital payment systems have appeared to flourish more quickly and more broadly. Brazil's digital payment system Pix, introduced in 2020, now has more than 127 million Brazilians and more than 10 million companies as subscribers or users.[10] Africa's M-Pesa mobile phone payments service, introduced in 2007, has expanded to 10 countries, has 29.5 million active users and processes up to 614 million transactions per month.[11] These systems have their own unique weaknesses and risks they pose from a public interest standpoint (some of them significant), but from a technological and service delivery standpoint their use cases are much clearer and stronger than what blockchain-based technologies have been able to demonstrate.

White writes, "One only needs to look at Moore's law to see how this is pretty much built into the technology world, as once-impossible ideas are rapidly made possible by exponentially more processing power. And yet, we are to believe that as technology soared forward over the past decade, blockchain technologies spent that time tripping over their own feet?"

---

[9] https://blog.mollywhite.net/its-not-still-the-early-days/

[10] https://www.bloomberg.com/news/articles/2022-11-23/brazilians-choose-central-bank-s-payment-app-over-credit-cards?sref=f7rH2jWS

[11] https://africa.businessinsider.com/local/markets/m-pesa-kenyas-mobile-money-success-story-celebrates-15-years/srp9gne

Some trace the lineage of the building blocks of cryptocurrency and blockchain (distributed ledgers and encryption) even further back to the 1980s or 1990s, depending on where one starts in the chronology, with products such as eCash, eGold, BitGold.[12] Following this line of association, this area of technology has had an even longer head start, and yet has not scaled or progressed at comparable pace or level to other technological advancements.

Naturally, not all innovation or invention proceeds along a neat line of progression. It is theoretically possible that someone will develop a 'killer app' based on blockchain technology at some point.[13] However, the question remains, why prioritize development of a technology that has clear structural flaws which have impeded its development for arguably 30 years or more, especially when superior alternatives exist?

As Kai Stinchcombe, a tech writer and founder of financial services firm argues (referring to blockchain technology's utility in terms of data storage and distribution),

> "There are four additional problems with a blockchain-driven approach. First, you're relying on single-point encryption — your own private keys — *rather than a more sophisticated system* that might involve two-factor authorization, intrusion detection, volume limits, firewalls, remote IP tracking, and the ability to disconnect the system in an emergency. Second, price tradeoffs are entirely implausible — *the bitcoin blockchain has consumed almost a billion dollars' worth of electricity to hash an amount of data equivalent to about a sixth of what I get for my ten dollar a month Dropbox subscription*. Fourth [*sic*][14], systematically choosing where and how much to replicate data is an advantage in the long run — *the blockchain's defaults on data replication just aren't that smart.* And finally, Dropbox and Box.com and Google and Microsoft and Apple and Amazon and everyone else provide a set of valuable other features that you don't actually want to go develop on your own. Analogous to Visa, the problem isn't storing data, it's managing permissions, un-sharing what you shared before, getting an easy-to-view document history, syncing it on multiple devices, and so on.
>
> The same argument holds for proposed distributed computing and secure messaging applications. *Encrypting it, storing it forever, and replicating it across the entire network is just a ton of overhead relative to what you're actually trying to accomplish. There are excellent computing, messaging, and storage solutions out there that have all the encryption and replication anyone needs — actually better than blockchain based solutions* — and have plenty of other great features in addition (emphasis added)."[15]

---

[12] https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/#:~:text=The%20first%20cryptocurrency%20was%20eCash%2C%20created%20by%20David%20Chaum's%20company,very%20influential%20in%20Bitcoin's%20creation.

[13] Some argue that blockchain, or more specifically Bitcoin, is that 'killer app,' in terms of how it combines these technological precursors in modestly novel ways that have solved problems earlier models faced. The challenge with this argument is that even if one assumes Bitcoin may do one thing well - establish a 'censorship resistant' method of exchanging digital assets - the methods it uses to accomplish this - decentralized consensus mechanisms, etc. - generate massive negative externalities and may stunt the development of other ways in which blockchains might be used.

[14] The author actually makes three points in this excerpt but misnumbered the points in the original text.

[15] https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100; additionally the data used to calculate the electricity use in this example is circa 2017. It is generally understood that the electricity demands of PoW systems remain large and inefficient.

If the core elements of blockchain technology are not wholly "new" and by inference truly disruptive in nature, and the progression of the technology is slow relative to other tools with similar attributes developed in parallel that provide similar services with more real benefits and fewer challenges, and the technology itself has structural limitations (along with significant externalities and associated risks), it begs the question, is this an innovation worth prioritizing, given these limitations and the very real risks and harms that are present today as the technology is used? As software engineer Luke Plant (whose work is described further below) writes, "There are plenty of new technologies that turn out to be duds."[16]

2. Blockchain Platforms Are Not Truly Decentralized

Defenders of blockchain technology will sometimes acknowledge the real limitations of its design but suggest that blockchain's key innovation – decentralization – is worth "selecting" for. David Rosenthal, a well-known computer scientist and critic of blockchain technology,[17] has written extensively on this matter.[18] In one publication, Rosenthal points to the writings of Albert Wenger (drawing on Clayton Christensen), who, while attempting to defend blockchain technology, made a comparison between blockchain and PCs:

> "The canonical example here is the personal computer (PC). The first PCs were worse computers than every existing machine. They had less memory, less storage, slower CPUs, less software, couldn't multitask, etc. But they were better at one dimension: they were cheap. And for those who didn't have a computer at all, that mattered a great deal."
>
> ...
>
> A blockchain is a worse database. It is slower, requires way more storage, and compute, doesn't have customer support, etc. And yet it has one dimension along which it is radically different. No single entity or small group of entities controls it."[19]

Wenger goes on to say that a decentralized platform like blockchain could be the basis for an internet not controlled by centralized corporations (e.g., web3) and that if the technology is widely adopted economies of scale will emerge that will either solve or incentivize solutions to make such tech faster, safer, more efficient – all because the innovative value of decentralization provides enough utility to make all this worth it.

Rosenthal offers two critiques of this position. First, he notes that "the infrastructure of the internet (IP/DNS/HTTP and so on) is decentralized, but that hasn't stopped the actual internet everyone uses being centralized." Two, in large part, blockchains as they operate now are not actually decentralized. Three key data points Rosenthal raises help bear this out:

- Concentration of control of crypto mining operations amongst a few key mining pools;
- Concentration of crypto trading activity on one key platform (Binance); and
- Concentration of Bitcoin holders, with a very small portion of wallets holding a large percentage of Bitcoin in circulation.

---

[16] https://lukeplant.me.uk/blog/posts/the-technological-case-against-bitcoin-and-blockchain/#the-problem-with-technology
[17] https://en.wikipedia.org/wiki/David_S._H._Rosenthal
[18] https://blog.dshr.org/
[19] https://blog.dshr.org/2022/01/blockchain-gaslighting.html

The data supporting Rosenthal's points has not substantively changed since his writing in January 2022. As of January 2023, two mining pools controlled 51% of Bitcoin's hash rate (with similar levels of concentration found on other chains);[20] 66.7% of all crypto trading on centralized exchanges (which themselves constitute the bulk of all crypto trading) now occurs on Binance;[21] and as of July 2022 one analysis determined that .04% of BTC addresses (or wallets) held 62.25% of all Bitcoins issued.[22] Other sources have offered confirmation of this ongoing trend of centralization - for example, a recent Wall Street Journal article revealed how a group of roughly half a dozen coders "serve as stewards of Bitcoin Core, an open-source program that keeps the cryptocurrency's digital ledger up-to-date on thousands of computers that make up its network."[23]

Another recent study further demonstrates how existing blockchains are not nearly as decentralized as presented, are at risk as a result, and may face structural challenges in achieving "true" decentralization. Trail of Bits is a New York-based firm that provides security assessments and advisory services to major information technology companies. The firm was engaged by the Defense Advanced Research Project (DARPA) to investigate the extent to which blockchains are truly decentralized. Their study, published in July 2022, focused on Bitcoin and Ethereum (two largest and most popular crypto blockchain platforms).[24]

Their report found that, though the cryptographic tools used to secure blockchain's immutability were robust (a feature which helps promote decentralization), the platforms they surveyed were vulnerable to exploits that took advantage of their chain's other properties – their implementation approaches, networks and consensus protocols. A few examples among many:

- Every widely used blockchain has a privileged set of entities that can modify the semantics of a blockchain to potentially change past transactions.
- The number of entities sufficient to disrupt a blockchain is relatively low: four for Bitcoin, two for Ethereum, and less than a dozen for most PoS (Proof of Stake) networks.
- A dense, possibly non-scale free, subnetwork of Bitcoin nodes appears to be largely responsible for reaching consensus and communicating with miners – the vast majority of nodes do not meaningfully contribute to the health of the network.
- Bitcoin traffic is unencrypted - any third party on the network route between nodes (e.g., ISPs, Wi-Fi access point operators, or governments) can observe and choose to drop any messages they wish. Additionally, of all Bitcoin traffic, the researchers found that for extended periods of time, 60% of such traffic traverses just three ISPs.

The study identifies many more vulnerabilities. Taken as whole, the picture it paints is that not only do these flaws demonstrate that existing blockchains are vulnerable to "centralized" attacks or exploits, but that a) some of these flaws will be difficult to fix with simple technology, due to the incentive structures found within blockchain based consensus mechanisms, and b) these networks are at present time operating in de facto centralized manner.

---

[20] https://cryptoslate.com/behind-the-two-mining-pools-controlling-51-percent-of-the-global-hash-rate/
[21] https://cryptonews.com/news/binance-has-grabbed-two-thirds-of-all-crypto-trading-volume-what-happened-to-the-decentralization-of-finance.htm
[22] https://cointelegraph.com/news/hodlers-and-whales-who-owns-the-most-bitcoin-in-2022
[23] https://www.wsj.com/articles/bitcoin-core-maintainers-crypto-7b93804
[24] https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf

To be clear, in pointing out the lack of decentralization found in blockchain-based platforms and the barriers to such decentralization, we are not taking the position that decentralization via blockchain is necessarily a worthy goal.[25] Rather, we are taking blockchain proponents' arguments at face value: that decentralization is the key value-add provided by blockchain technology that is worth "selecting for" in spite of current and future drawbacks and challenges. If decentralization isn't actually meaningfully present in these systems, and a combination of technological and economic factors making achieving real decentralization difficult or impossible, or not worth the cost relative to other alternatives, then it raises the question of whether blockchain technology is worth developing relative to other approaches.

3. Permissionless Blockchains are Difficult to Disentangle from Financialization

Applications of blockchain technology outside the financial services sector theoretically rely less on the notional utility of "digital assets" created and stored on blockchains, and more on the utility of the underlying distributed database itself. As such, some argue that the threat/benefit profile of blockchains may be different from those found in the financial services, and thus observers should distinguish between and differentiate "crypto" from "blockchain".

Arguably, however, it can be difficult to divorce the use of distributed ledger technology from the practice of tokenizing data on such a database, and its subsequent monetization or use as a financial instrument.

UK-based software engineer Luke Plant, who has written an extensive analysis identifying the design flaws and limitations of blockchain technology, points out that, at least for permissionless (public) blockchains, "Note also that you can't remove the cryptocoin and keep the blockchain technology – a permissionless blockchain requires a speculative cryptocoin to power it, otherwise no-one will ever pay for it." Plant elaborates further by quoting David Rosenthal, who argues:

> "Because miners' opex and capex costs cannot be paid in the blockchain's cryptocurrency, exchanges are required to enable the rewards for mining to be converted into fiat currency to pay these costs. Someone needs to be on the other side of these sell orders. The only reason to be on the buy side of these orders is the belief that 'number go up'. Thus the exchanges need to attract speculators in order to perform their function. Thus a permissionless blockchain *requires* a cryptocurrency to function, and this cryptocurrency *requires speculation* to function."

There may be current or future applications of blockchain technology which are able either disprove this argument or find workarounds that don't negate the value of using a blockchain/DLT based platform (either by introducing a third party or making the platform insecure). And, as explored briefly below, some blockchain proponents argue that the financialization of various types of data is what "powers" certain blockchain operations and produces "value" from them.

But Plant and Rosenthal's point raises a serious challenge - if permissionless systems rely on decentralized consensus mechanisms to perform their core function(s), and those consensus mechanisms must rely on financial or economic incentives to work, the deployment of blockchain, even

[25] Other proposals exist to achieve decentralization in the context of information technology platforms. For example, Tim Berners Lee (widely credited with being a founder of the world wide web) has offered an approach he deems Web 3.0 - https://www.cnbc.com/2022/11/04/web-inventor-tim-berners-lee-wants-us-to-ignore-web3.html. We take no position at this time on the merits of this approach or otherwise. But, we share it to make the point that if 'decentralization' is a worthy aim, technologists can and should explore with a critical eye different pathways to achieve it. Yet the discourse on blockchain often already assumes that blockchain is 'the' path to decentralization and that developmental pathways to achieve it must flow from there.

for purposes primarily other than financial products and services, may nearly always include some element that relies on speculative financial activity.

For our organizations, that suggests the risks present in such speculative financial activities will often increase the risk profile of blockchain technology deployments, and increase the complexity of identifying appropriate regulatory and oversight mechanisms – all of which expend money, time, and resources that could otherwise be spent on alternative technologies that could achieve similar objectives.

Central Bank Digital Currencies (CBDCs)[26]

Proposals for a CBDC assume that a digital dollar built using blockchain technology and its associated institutional architecture may be able to address key financial inclusion issues, such as lack of access to bank accounts, the need for faster, more secure, and reliable payment systems, etc., and can do so while offering sufficient privacy and consumer protections for CDBC holders and users.

However, A CBDC (in general, or a poorly designed/deployed one) might: 1) Expose users to expansive surveillance activities and undue violations of privacy; 2) Undermine access to and availability of physical cash; 3) Push the Fed to take more of a role in the economy and financial markets than may be wise, either by buying more assets to offset CBDC liabilities, or by exercising more control over bank's debt and credit decisions, constraining banks' and consumers' access to credit; 4) Impact funding or support for the community reinvestment act (CRA) program, negatively impacting access to banking services for low income communities; and 5) Be used or abused to unfairly restrict people's use of public benefits, or to garnish wages to serve private or government debts.

For these reasons we have urged the Fed, and encourage your office, to reconsider the fundamental premises behind a CBDC and work with other agencies to make room for a more polycentric institutional and technological architecture, which may or may not incorporate blockchain-based tokens, if they prove to be as or more effective than other option and do not present comparatively higher risks.

Indeed, such architecture could incorporate both existing Fed systems and new innovative approaches that are not dependent on DLT technology. For example, we would support the acceleration of the Fed Now program, with consumer fraud protections incorporated, which would expand the availability of real-time payments as a first step. We would additionally see promise in the deployment of a privacy-protecting Fed Accounts system that would expand the capacity of the Fed to provide account-based deposit and payment systems, with low or no fee services, beyond commercial banking institutions to retail customers. Such a system could be coupled with proposals to implement a postal banking program where the post office, which already provides payments-based services such as money orders, could serve as a front-end point of contact for retail users.

Finally, we support proposals to create "e-cash" – offline, hardware-based digital cash, built using existing technology, and issued by the Fed, Treasury or some combination of agencies – that could serve the same function as physical cash, without the risks to privacy, consumer fraud and structural imbalances that a Fed-issued, blockchain based digital currency may present. Indeed, such systems already exist outside the US, where payment systems using SIM-card based hardware tied to mobile phone platforms are a popular means of making payments. Card and chip-based hardware already in

[26] For more extensive commentary from our organizations on CBDCs and digital dollar proposals, including a brief discussion of potential design principles for a CBDC, please refer to our May 2022 submission to the Federal Reserve - https://ourfinancialsecurity.org/wp-content/uploads/2022/05/5.20.22-digital-assets-CBDC-letter.pdf

use for commercial smartcards and U.S. military payments technology could be modified or altered to serve as digital cash, and there are many measures that could be employed to ensure the safety, security and authenticity of such digital cash using existing or modified technology to make such e-cash comparable to paper cash by these measures.

Despite the concerns listed above, we do believe it is worth exploring how a CBDC might be developed, for two reasons. First, within the framing we describe above, a comparative analysis of different approaches and modalities for a digital dollar could help better demonstrate either how heterogenous tools could complement one another, or how deployment of non-blockchain approaches could obviate the need for a blockchain-based digital dollar. Such an analysis might also identify the extent to which the risks posed by a CBDC could, or could not be mitigated, either by technological, policy or legal solutions. The danger in not fully mapping these scenarios is that the most ardent proponents of a CBDC may be tempted to engage in wishful or magical thinking about potential adverse consequences rather than seek clearly identify and take meaningful steps to prevent or mitigate them. OSTP and other agencies should instead conduct rigorous due diligence on any proposals before they are approved and deployed.

Second, we are deeply skeptical of the notion that privately created and circulated cryptocurrencies are a viable alternative to a CBDC/public digital dollar. Digital assets have flaws and vulnerabilities too numerous to name in full, but the concerns we and many others have about these assets' security, reliability, volatility, stability, and viability as payment systems should be enough to move federal agencies to keep private digital assets largely "off the table" as a realistic solution for financial inclusion. As such, exploration of a public digital dollar, either as a CBDC or not, may help ensure that federal agencies do not cede too much ground to this idea, and instead remain focused on ensuring the federal government is upholding its responsibility to provide a public currency and payments system that is equitable, reliable, efficient, safe and secure.

Recommendations

Our overarching recommendation for this research and development agenda is that, to the extent practical or feasible within the OSTP's mandate, it should be organized around concrete objectives first (those given in the initial request for information from the OSTP are good illustrative examples of objectives that might serve), and that a comparative analysis is then done from a more technology neutral or agnostic standpoint, to evaluate both blockchain-based and non-blockchain based technological solutions on equal footing.

We believe this reorientation could be a more fair and objective approach, and provide some compensation for a dynamic commonly identified by observers of this industry, who point out that blockchain is often a "solution in search of a problem."[27]

Additionally, the OSTP should strive to ensure that stakeholders, participants and evaluators of research initiated under this agenda are drawn from a diverse pool of individuals and entities whose perspectives and expertise can meaningfully represent different and independent viewpoints on the proposed merits, flaws, or limitations of blockchain technology.

[27] Letter in Support of Responsible Fintech Policy - https://concerned.tech/

In June 2022, a group of more than 1500 technologists, many with distinguished backgrounds in the fields of computer science and software engineering, signed and sent a letter to Congress, calling on policymakers to “take a critical, skeptical approach towards [crypto industry] claims” and to “take an [policymaking] approach that protects the public interest and ensure technology is deployed in genuine service to the needs of ordinary citizens.”

These technologists created and signed this letter due to concerns that policymakers were receiving a lopsided representation of technologists’ views regarding blockchain technology, which was at odds with their views on the matter:

> “By its very design, blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit. From its inception, this technology has been a solution in search of a problem and has now latched onto concepts such as financial inclusion and data transparency to justify its existence, despite far better solutions to these issues already in use. Despite more than thirteen years of development, it has severe limitations and design flaws that preclude almost all applications that deal with public customer data and regulated financial transactions and are not an improvement on existing non-blockchain solutions.”

Despite their conviction and depth of understanding, we suspect none of these signatories would argue their expertise here is utterly infallible, and we certainly hope proponents of blockchain technology believe the same about their own views and analysis. Scientific inquiry benefits from dissent and disagreement. We hope that the research initiatives spurred by the OSTP and its initiative here provide ample space for such discourse, and thank you once again for the opportunity to share our views on this subject.

Sincerely,

Mark Hays
Senior Policy Analyst
Americans for Financial Reform Education Fund
Demand Progress Education Fund

For any questions or comments about this submission,
Please contact submission author Mark Hays, Senior Policy Analyst with AFREF/DPEF,
[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Alliance for Innovation Regulation (AIR)

Submitted electronically

March 3, 2023

Dr. Arati Prabhakar
Director
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

RE: Request for Information on Digital Assets Research and Development (Federal Register Document Citation 88 FR 5043)

Dear Dr. Prabhakar:

On behalf of the Alliance for Innovation Regulation (AIR), a nonprofit of which I am CEO and Co-Founder, I appreciate the opportunity to submit this comment in response to the Office of Science and Technology Policy's (OSTP) Request for Information (RFI) on Digital Assets Research and Development.

AIR launched in 2019 to help governments get a better handle on the digital transformation of the financial system. Since then, we have quadrupled in size and are actively engaged with the innovation efforts of public-sector entities on three continents.[1] AIR's activities include consulting with regulators on how to strengthen their digital capabilities; partnering with agencies on hackathon-style competitions known as "TechSprints" to develop digital-focused solutions to regulatory problems; and advocating for a digital-native regulatory approach to address an increasingly digital-native economy.[2]

We are fully aware that the rapid development of digital assets and blockchain technologies is a double-edged sword. On the one hand, digital assets offer privacy protections and potentially lower transaction costs, among other benefits. Meanwhile, blockchains hold promise for improving formerly analog processes in multiple sectors, including the public sector; better analyzing data used to fight global corruption and other crimes; and expanding access for consumers to more efficient, safer and fairer tools.[3]

On the other hand, some digital assets are rife with risks, ranging from volatility in cryptocurrency prices and associated losses, to the ability of bad actors to use digital-asset technologies in fraud or illicit money-laundering schemes.[4] Some risks associated with blockchains include the inability at times to remove data from a permissionless blockchain and a lack of interoperability in certain cases.

Key Areas for Research

As previously discussed, digital-asset technologies present both risks and opportunities for financial services and other industries. While recent volatility in the crypto market is a cause for concern, government officials have policy options to bring necessary transparency and stability.

---

[1] "Three years ago, AIR didn't even have a logo. We've come a long way since," regulationinnovation.org/airs-third-anniversary/

[2] https://regulationinnovation.org/techsprints/

[3] https://www.weforum.org/platforms/shaping-the-future-of-blockchain-and-digital-assets

[4] "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets," International Monetary Fund, September 2022, https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022007.ashx

Furthermore, both digital assets and their underlying technologies show potential to have a positive impact on fighting financial crime, expanding financial inclusion and mitigating effects of climate change, among other things. To maximize the positive impact of digital-asset technologies, we recommend that the U.S. government's Research and Development (R&D) agenda zero in on the following topics for further study:

- Digital use cases that improve and expand financial inclusion;
- Potential benefits of central bank digital currencies for improving cross-border and digital payments;
- Broader use cases of distributed-ledger technologies in medicine, agriculture, supply-chain management, carbon capture and sequestration, and real estate;
- How an immutable blockchain with a history of every transaction could help identify financial activity related to corruption, money laundering, CSAM and other crimes; and
- Alternative "consensus-mechanism" technologies that are less energy-intensive and therefore leave a smaller carbon footprint.

Assessing Risks and Opportunities in Blockchain Technology for Regulators and Law Enforcement

AIR commends the OSTP for undertaking this effort to examine R&D opportunities pertaining to digital assets, part of the Biden Administration's recent Executive Order issued in March 2022. We believe that there are ample opportunities for the U.S. government and nations around the globe to employ beneficial uses of blockchain and other distributed-ledger technologies (DLT) while being vigilant about dangers associated with digital assets. Potential benefits include combating illicit financial crimes, expanding financial inclusion and monitoring efforts to mitigate climate change.

Perhaps most importantly, as blockchains and similar innovations enable the ongoing digital transformation of the private sector, it is also of utmost importance for regulators and other public-sector agencies to keep pace and to adopt these powerful kinds of technology for their own use. They must educate personnel about digital assets and other transformative technologies and explore how to replace their analog data analysis mechanisms with digital-native "Suptech" capabilities.

The gap between industry's digital capability and that of the government continues to widen, which exacerbates the risks posed by digital assets and other new products to consumers. An aggressive R&D agenda by OSTP and other government entities can help narrow that gap.

Additional Comments

Our additional comments for the RFI focus on how digital assets and related technologies could improve certain applications; how digital assets pose specific risks or harms; and opportunities to advance responsible innovation in the digital-assets ecosystem. Our responses generally pertain to the use of digital assets in the financial sphere.

A Holistic Approach to Managing Technologies Underlying Digital Assets

We believe an R&D agenda related to digital assets should aim to maximize the positive impact of blockchain and other distributed-ledger technologies while aggressively managing the risks. In many areas, the technological innovations that have enabled the growth of digital assets — and in some cases precipitated financial-stability and consumer-safety concerns — could also enable solutions to enduring global challenges.

The development of digital currencies could in the future lead to a broad-scale reduction in the cost of cross-border payments. This includes the establishment of Central Bank Digital Currencies (CBDC) around the world, which has the potential to enhance market efficiency. The creation of a U.S.-based CBDC, which the Federal Reserve and other government entities are exploring, could also preserve the U.S. Dollar's position as the world's reserve currency.[5] We applaud these efforts. In non-financial arenas, blockchain technology has proven beneficial in improving the registration of property titles,[6] the healthcare industry,[7] event ticketing[8] and other uses.

<u>We offer further detail in the following areas:</u>

- Recent failures of digital-asset companies have prompted some observers to sound the alarm about financial stability and consumer safety. Policymakers could mitigate that risk by clarifying protections for digital-asset customers and investors, and the regulatory guidelines for digital-asset firms.

- As criminals have used digital assets to stay hidden, law enforcement has used new technologies to their advantage, including in anti-money-laundering and cracking down on distributors of Child Sex Abuse Material (CSAM). Additionally, blockchain technology has emerged as a potential anti-corruption tool.

- While supporters of CBDCs point to financial-inclusion benefits, additional blockchain-related technologies utilized by non-governmental organizations and emerging markets also offer hope for reaching underbanked consumers. Digital-identity tools are required to reach the full potential of the benefits of digital assets. Various public- and private-sector initiatives are addressing this need and we applaud these efforts.

- Some consensus mechanisms that validate cryptocurrency transactions, such as Proof-of-Work (PoW) used by the Bitcoin network, are very energy-intensive and leave a sizable carbon footprint. Some private-sector solutions have aimed to mitigate this carbon impact.[9] Alternatives to PoW consensus mechanisms should be explored.

- A key element of ensuring responsible innovation in the digital-asset ecosystem is equipping regulators overseeing that innovation with the digital know-how, systems upgrades and human-capital improvements necessary to supervise the digital transformation of our financial markets.

---

[5] Digital currencies and the future of the monetary system, Remarks by Agustín Carstens, Bank for International Settlements, January 2021, https://www.bis.org/speeches/sp210127.pdf

[6] "How Blockchain and Cryptocurrency Are Influencing the Real Estate Market," Realtor Magazine, June 2022, https://www.nar.realtor/magazine/real-estate-news/technology/how-blockchain-and-cryptocurrency-are-influencing-the-real-estate.

[7] "Blockchain technology applications in healthcare: An overview," International Journal of Intelligent Networks, 2021, https://www.sciencedirect.com/science/article/pii/S266660302100021X.

[8] "How Mobile Blockchain Ticketing Is Changing The Events Industry," Forbes, March 2022, https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/18/how-mobile-blockchain-ticketing-is-changing-the-events-industry.

[9] "Consensus Mechanisms" described on Ethereum website: https://ethereum.org/en/developers/docs/consensus-mechanisms/

Financial Stability and Consumer Protection

The recent failures of the exchange FTX and other digital-asset-related firms in the wake of a dramatic drop in crypto-asset values last year revealed immediate consumer- and investor-protection concerns.[10] As the digital-asset sector grows and becomes more entwined with traditional finance, there is greater risk that volatility in these markets could spill over to broader financial markets, exacerbating investor and customer losses.

In order to foster responsible innovation of the digital-asset sector, policymakers should set out to create a legal framework that clarifies the regulatory status of crypto tokens, which regulatory agencies have appropriate jurisdiction over different aspects of the digital-asset industry, and how federal protections for crypto assets differ from those of more traditional bank deposits.

U.S. bank regulators, particularly the Federal Deposit Insurance Corporation, have acted appropriately to assert that funds stored with crypto exchanges do not enjoy the same type of FDIC backing afforded to traditional bank deposits.[11] Making this distinction clear and providing additional levels of transparency about how digital-asset firms reserve for crypto-assets they hold are key to ensuring a benchmark level of consumer and investor protection. We also applaud a recent joint statement by the U.S. bank regulators advising institutions to manage liquidity risks associated with providing services to digital-asset firms.[12]

Regulators and lawmakers should aim to develop a more formal policy framework to address consumer and investor protections for digital-asset users. One model for how the U.S. ultimately regulates crypto exchanges could be the framework developed by Japan, which established broad standards following earlier failures of crypto firms.[13] Most notably, the country's Financial Services Agency (FSA) requires crypto exchanges to keep a customer's fiat money and digital assets completely segregated from the exchange's own crypto-asset holdings.

Fighting Financial Crime

Unfortunately, criminals ranging from drug traffickers to distributors of CSAM have often resorted to hiding their financial transactions and laundering funds by utilizing crypto-assets to avoid scrutiny from banks' anti-money-laundering (AML) controls. The anonymity and pseudonymity afforded by digital-asset technology poses a significant money-laundering risk for authorities, similar to the difficulty law enforcement has in tracking physical cash. Monitoring onramps and offramps in a cryptocurrency transaction are key to combating money laundering and other crimes.

At the same time, blockchains can actually make it more difficult for criminals to hide financial activity, because a record of the transaction always remains in a DLT system.[14] Like cash, cryptocurrency is

---

[10] "What Went Wrong with FTX—and What's Next for Crypto?" Kellogg Insight, Kellogg School of Management, Northwestern University, https://insight.kellogg.northwestern.edu/article/ftx-collapse-future-crypto

[11] "Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies," FDIC Financial Institution Letter, https://www.fdic.gov/news/financial-institution-letters/2022/fil22035.htm

[12] https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-18.html

[13] "Japan Was the Safest Place to Be an FTX Customer," CoinDesk, December 2022, https://www.coindesk.com/consensus-magazine/2022/12/13/japan-was-the-safest-place-to-be-an-ftx-customer/

[14] "Why criminals can't hide behind Bitcoin," Science, March 2016, www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin

anonymous at the point of transaction, but unlike cash, it is readily traceable because all the transactions are visible on the associated blockchain. This makes it possible for the financial industry and law enforcement to detect patterns of possible crime and, after gaining appropriate legal permissions, to determine the identities of users. This identity information is collected by the crypto exchanges.

There are encouraging signs of progress with investigators being able to overcome tactics used by bad actors. New innovations offer hope that in some cases blockchain technologies can aid banks in establishing AML controls, and even help investigators catch criminals in the act.[15] For instance, my organization, AIR, held a TechSprint in 2020 on how crypto traceability could be used to thwart CSAM users.[16] During the event, one participating team actually identified a transaction occurring in real time, and referred it to law enforcement.

In another example, we partnered last year with the U.S. State and Treasury departments on the Anti-corruption Solutions through Emerging Technologies (ASET) TechSprint. The program, cited by the White House among government efforts to promote democracy around the globe, aims to accelerate solutions to thwart transactions related to corruption, such as bribery.[17] Among the prototypes is a proposal to use blockchain-enabled "smart contracts" to improve transparency in disaster relief contracts.

Other higher-profile cases included the seizure last year of $3.6 billion in bitcoin and arrest of a couple for allegedly trying to launder the funds. Prosecutors said they were able to trace the funds as they were hacked and then funneled through various accounts.[18] In another notable case, a blockchain analytics tool developed by Chainalysis aided government agencies in nabbing the largest distributor of online CSAM.[19]

Financial Inclusion, Digital Identity and Payments

Another area where blockchain technology shows promise is in helping more consumers access financial services. Proponents of CBDCs often cite broader financial inclusion as a goal, especially in emerging markets. However, blockchains may also help in other financial-inclusion efforts.

For example, blockchain-related solutions can provide consumers with digital identification options. A blockchain-based ID system can be used by private organizations to issue security credentials and other applications.[20] But it also could help overcome one of the hurdles to economic development for consumers in developing nations — particularly women — who often lack access to identity documents.[21] This hurdle compounds their difficulty in accessing financial services, since identity verification is required for a financial institution to onboard customers and comply with AML requirements.

---

[15] "Can blockchain turn the tide on financial crime compliance?" Deloitte Perspectives, https://www2.deloitte.com/mt/en/pages/financial-services/articles/mt-risk-article-can-blockchain-turn-the-tide-on-financial-crime-compliance.html

[16] https://regulationinnovation.org/crypto-techsprint/

[17] www.whitehouse.gov/briefing-room/statements-releases/2022/11/29/fact-sheet-summit-for-democracy-progress-in-the-year-of-action/

[18] "Feds arrest married couple, seize $3.6 billion in hacked bitcoin funds," Washington Post, February 2022, https://www.washingtonpost.com/national-security/2022/02/08/bitfinex-hack-bitcoin-arrests/

[19] "Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site," WIRED, https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

[20] https://www.ibm.com/blockchain-identity

[21] "Using Digital Solutions to Address Barriers to Female Entrepreneurship: A Toolkit," The World Bank, https://digitalforwomen.worldbank.org/sites/gender_toolkit/themes/barrier/pdf/Toolkit-v2.pdf

Many innovators have looked at ways to establish digital identity platforms — backed by blockchain technology — that consumers can access through a personal device. A well-known effort to bring underserved consumers into the financial services fold is India's Aadhaar project, which created a national biometric-based identification system, but the project has also led to privacy concerns.[22] More recently, researchers have worked on an upgraded version of the digital-identity framework that would incorporate blockchain-based technology.[23]

Another challenge is enabling financial-inclusion projects in the developing world to interact seamlessly with other payments rails, a concept known as payments interoperability. One development of note is Mojaloop, an open-source platform developed as a collaboration between private-sector companies and non-governmental organizations, which aims to achieve interoperability among payments ecosystems in emerging markets. The Mojaloop Foundation notes on its website that while its software "does not use blockchain," it "relies on the Interledger Protocol to operate, which is not a blockchain but uses some key concepts from blockchain technology, such as a decentralized design and cryptography-based security."[24]

Climate Change

Among the risks facing the digital-asset sphere is the enormous carbon footprint left by crypto miners through consensus mechanisms established in leading crypto systems. In crypto mining, validators receive financial rewards in bitcoin or other crypto as reward for solving computational problems. But this so-called PoW mechanism requires massive computing power and electricity resources.

Many throughout the industry and elsewhere have sought to establish alternative consensus mechanisms with a reduced impact on the energy grid. This includes the so-called "Proof-of-Stake" approach used by the Ethereum system that was adopted through the network's "merge" in 2022. Further investigation of alternative mechanisms to mitigate the carbon impact of the crypto sector would be an appropriate objective of an overall R&D agenda for digital assets.

Crypto technologies may also enable greater transparency and monitoring of carbon dioxide (CO_2) removal (CDR), as well as provide incentives to those that operate CDR systems. Today, the carbon credit market is broken because there is little transparency on how these offsets are being used and the amount of CO_2 being removed. Cryptocurrencies could be used to incent CDR by setting up competitions around the amount of CO_2 captured and sequestered.

Addressing Regulators' Digital Capability

To best understand and address the risks and opportunities of digital assets, U.S. government research efforts must also explore the digital capability of regulators overseeing financial services and other industries.

---

[22] What Happens When a Billion Identities Are Digitized? https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized

[23] "Researchers working on blockchain-based digital ID system to improve India's financial landscape," Biometricupdate.com, https://www.biometricupdate.com/202204/researchers-working-on-blockchain-based-digital-id-system-to-improve-indias-financial-landscape

[24] https://mojaloop.io/faq-items/does-mojaloop-utilize-blockchain/

The regulatory framework for cryptocurrencies and digital-asset technologies is still uncertain. But perhaps a bigger concern is the fact that federal regulatory agencies still largely operate through an analog lens — relying on legacy infrastructure, lacking the ability to catch threats in mountains of data and adopting change linearly — despite the exponential pace of digital transformation in the private sector. This gap puts them at an immediate disadvantage when trying to manage the risks and opportunities related to digital assets.

A key focus of federal R&D efforts should be how to strengthen human-capital resources across the regulatory agencies to ensure that the government can manage rapid digital change.[25] The first step toward addressing this is through education. We recommend that agencies and the government as a whole look into establishing teams of digital innovation specialists and offering training curricula on digital assets and other technologies as part of workforce development.

Conclusion

We applaud the White House for prioritizing a focus on digital assets through President Biden's executive order issued last year, and the Office of Science and Technology Policy for soliciting feedback on how to advance this effort through research and development.

Digital currencies, blockchains and other distributed-ledger technologies are increasingly part of the mainstream economy despite turmoil in the crypto market and remaining skepticism about their applicability for the consumer. Technology innovators, investors and an array of both startups and established companies are devoting a tremendous amount of resources to developing beneficial use cases for these technologies as well as solutions for addressing the related risks.

It is essential that the public sector be a part of this conversation to help foster prudent adoption of this technology for good. We at AIR are available as a continued resource to provide input to U.S. government officials as they develop the R&D agenda for digital assets.

Sincerely,

Jo Ann S. Barefoot

Jo Ann S. Barefoot
CEO and Cofounder
Alliance for Innovative Regulation (AIR)

[25] "Building a digital regulator: how the FCA is riding the innovation wave," https://www.fca.org.uk/news/speeches/building-digital-regulator-how-fca-riding-innovation-wave

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Aleo Systems Inc.

Aleo

March 3, 2023

BY ELECTRONIC SUBMISSION

Dr. Arati Prabhakar
Director, Office of Science and Technology Policy

Re: Request for Information; Digital Assets Research and Development (topics #1-6)

Dear Director Prabhakar,

Aleo Systems Inc. appreciates the opportunity to comment on the Office of Science and Technology Policy's Request for Information on "Digital Assets Research and Development." We are a venture-backed firm researching and developing advanced cryptographic techniques—specifically zero-knowledge proofs ("ZKPs")—that would permit applications on distributed systems to confirm facts without unnecessarily sharing and compromising the underlying data that proves those facts.[1]

This technology is critical to the future of the internet. In Part I, we explain that distributed systems—like the internet, and like blockchains—depend on the ability to exchange data confidentially, while commercial forces simultaneously work to limit anonymity. We then argue that the internet's data security problems, which are already considerable, would be made significantly worse by the design of first-generation blockchain technology.

In Part II, we get to Aleo's *raison d'être*: leveraging advanced cryptography to solve these problems. This technology can power the next generation of solutions for digital identity, provenance, authentication, private records, and data control in the age of an ever-sprawling "internet of things." These solutions can fundamentally upgrade the internet.

They also fall directly within OSTP's mandate to "kickstart research on next-generation cryptography, transaction programmability, cybersecurity, and privacy protections,"[2]—in addition to President Biden's directive that the OSTP explore ways to ensure U.S. leadership in technologies of the future, especially those critical to our economic prosperity and national security.[3] Having American companies lead the way means that we can build democratic values into how these systems work—precisely what happened with the internet, and precisely *why* the internet turned out to be so successful. It also means that more of the companies and jobs will be in the United States, allowing more oversight and potentially creating hundreds of billions of dollars of value. By their nature, these jobs will also be more distributed than the twentieth-century workforce, benefiting all states rather than a small handful.

[1] This comment uses the term "distributed systems" to refer to a network of unaffiliated nodes (like computers or mobile phones) that can nonetheless coordinate on activities like sending and receiving information. We use "blockchain" and "distributed ledger" interchangeably to refer to distributed (rather than centralized) ledger systems.
[2] *FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, THE WHITE HOUSE: STATEMENTS AND RELEASES (Sept. 16, 2022), https://perma.cc/BQ4B-2YRG.
[3] President Joseph R. Biden, Jr., *A Letter to Dr. Eric S. Lander, the President's Science Advisor and Director of the Office of Science and Technology Policy*, THE WHITE HOUSE: PRESS RELEASES (Jan. 15, 2021), https://perma.cc/9MDM-FYJD.

Part I – Privacy Enabled the Internet

The internet was a revolution in decentralized networking. It allowed individuals to connect their computers to a world wide web in order to exchange information. In its early days, many skeptics doubted the value of this technology and believed its apparent anonymity would more naturally facilitate crime and lawlessness than legitimate use cases.[4] But subsequent history told a very different story, one that provides valuable lessons that should inform policy with respect to blockchain technology today.

First, almost all of the internet's important use cases—email, messaging, banking, e-commerce—depend on the internet having a neutral infrastructure that facilitates the *confidential* exchange of sensitive personally identifiable information (PII) and other data. It's hard to believe users would have adopted email or messaging applications if they believed that the entire world could read the content of their messages. Indeed, many people use web browsers simply assuming they have privacy—as they might with a doctor, therapist, or close friend, asking questions they would not ask in public.[5]

At the same time, while the TCP/IP architecture of the internet appeared neutral and anonymous—and many first understood it that way—this did not mean that all activity on the internet would be anonymous. As Larry Lessig, Tim Wu, and others have pointed out, the industries built on the internet quickly found ways to label and organize information (which in turn permitted more local regulation of the internet than people first understood).[6] The practice of IP mapping, for instance, permits tracing IP addresses to particular geographic locations; the advertising industry, which benefits from location-specific advertising, monetized this technique soon after its discovery.[7] Moreover, e-commerce depends on "cookies"—little bits of data that, among other things, allow website operators to know that the person "checking out" is the same person who added certain items to a shopping cart.[8] It turned out the internet was a lot less anonymous than it looked.

In fact, the absence of data security ultimately held back innovation; this is why one of the most important policy developments for unlocking e-commerce was the government permitting the use of stronger encryption (which provides, for instance, more security when sharing payment information).[9] The key insight is that some amount of privacy is *necessary* to realize the internet's full possibilities, while complete anonymity limits the commercial potential of distributed technology.

There are two specific takeaways from this experience. First, concerns about anonymity—on the internet, and now on distributed ledgers—often underestimate the overwhelming commercial incentive to identify users, and thus in the long run are likely to be displaced by concerns about invasions and exploitation of privacy, as we now see with public policy concerns about the exploitation of user data.[10] Second, distributed systems thrive based on finding an "enabling" amount of privacy that permits: (1)

---

[4] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET xii, 13-14 (2006); *see id.* at xii ("In the 1990s, many believed that nations could not control the local effects of unwanted Internet communications that originated outside their borders, and thus could not enforce national laws related to speech, crime, copyright, and much more."); *id.* at 3 (co-founder at MIT's Media Lab asserting that the "internet cannot be regulated"); LAWRENCE LESSIG, CODE: VERSION 2.0, at 31 (2006).
[5] *See, e.g.*, Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, NY TIMES (Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol html.
[6] *See* LESSIG, *supra* note 4, at 38-83; *see generally* GOLDSMITH, WHO CONTROLS THE INTERNET.
[7] GOLDSMITH, *supra* note 4, at 7.
[8] LESSIG, *supra* note 4, at 48-49.
[9] *See, e.g.*, STEVEN LEVY, CRYPTO, at 312 (2002).
[10] *See, e.g.*, Statement of Chair Lina M. Khan Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022), https://perma.cc/AH3Z-SKFG.

data security; (2) individuals to control their data and retain the dignity of choosing with whom they share this information, just as they do in the physical world; (3) commercial activities that are easy and frictionless for users; and (4) the pursuit of public policy goals like limiting abusive material, preventing illicit finance, and deterring, detecting, and punishing crime.

Finally, it is important and humbling to note that almost none of the internet's most important and useful infrastructure, much less its applications, were predictable at inception. For example, in the 1980s, McKinsey famously advised AT&T that the size of the mobile phone market in 2000 would amount to 900,000 phones, noting that such devices would be absurdly heavy and suffer low battery lives, bad service, and expensive marginal costs; of course by the year 2000, 109 million people had mobile phones,[11] with 900,000 joining every three days.[12] It wasn't just McKinsey. Companies as sophisticated as Kodak failed to predict the integration of mobile phones and cameras. And few if any predicted the size of markets for user-generated content until those markets came to be, though now they seem obvious—much less the ability to have mobile-powered rideshare or grocery-delivery systems. These distributed systems, once created, incentivized innovation in unforeseeable ways, leading to massive investments in software as well as the hardware that enables them.

The internet's data security problem

The problems with internet data security almost go without saying. By one estimate, approximately "4,145 publicly disclosed breaches … exposed over 22 billion records in 2021."[13] In 2015, hackers stole the records of over 20 million people from the Office of Personnel Management, including fingerprint records for over 5 million people.[14] In 2017, hackers accessed the personal data of 143 million U.S. consumers—roughly 44% of the U.S. population—by breaching Equifax's servers.[15] IBM estimates that the average cost of a data breach is over $9 million, with stolen credentials on average costing more and taking 327 days to identify, to say nothing of how attackers may use that information to harm victims in the future.[16] These attacks amount to a serious tax on the U.S. economy.

The basic cause is the absence of data security. Consumers are often only as safe as the most negligent third parties in charge of their data. Even companies with advanced IT systems struggle to adopt basic cybersecurity measures, much less state-of-the-art practices. The overwhelming emphasis, however, has been on trying to drive the adoption of better practices. These efforts, while important, have failed to keep up. In the meantime, the distributed nature of the internet gives attackers more points of attack—a problem getting worse as more and more systems integrate to share more and more data. As a result, the expansion of cloud computing—a more distributed form of computing versus the *status quo ante* of storing and computing locally—may augur even more data breaches, because it means more data is shared. Indeed, IBM estimates that nearly half of all breaches occurred in cloud infrastructure.[17]

---

[11] Harry McCracken, *Shocker: In 1980, Motorola Had No Idea Where the Phone Market Would Be in 2000*, TIME MAGAZINE (Apr. 15, 2014), https://perma.cc/R9BZ-WB3Z.
[12] *Cutting the cord,* THE ECONOMIST: SPECIAL REPORT (Oct. 7, 1999), https://perma.cc/B4QS-TKY9.
[13] *Over 22 billion records exposed in 2022,* SECURITY MAGAZINE (Feb. 10, 2022), https://www.securitymagazine.com/articles/97046-over-22-billion-records-exposed-in-2021.
[14] *See Cybersecurity Resource Center,* OPM, https://perma.cc/9T28-68AM; *see also* Damian Paletta, *Government Personnel Cyber Breach Worse Than Previously Thought*, THE WALL STREET JOURNAL: ARTICLES (Sept. 23, 2015), at https://www.wsj.com/articles/government-personnel-cyber-breach-worse-than-previously-thought-1443025119.
[15] Colin Dwyer, *Hackers Accessed the Personal Data Of 143 Million People, Equifax Says,* NPR (Sept. 7, 2017), https://perma.cc/HJ8K-ZWSH.
[16] *Cost of a data breach 2022*, IBM: REPORTS, https://perma.cc/UY6W-XSQ3.
[17] *Ibid.*

But the internet's data privacy problems are much broader and deeper than concerns about criminal hacks. The reality is while we were initially concerned about the anonymity of the web, its infrastructure counter-intuitively supported a massive multi-hundred billion dollar data surveillance industry and the rise of surveillance-based capitalism.[18] Indeed, it turned out the internet as initially conceived was *too* open, and it was the addition of *more* privacy in the form of the HTTP over SSL ("https") that unlocked critical use cases like e-commerce.[19] Even now, and even after the addition of these technologies, headlines like the Cambridge Analytica scandal[20] demonstrate how third parties can leverage data for purposes of fraud, scams, election interference, and social engineering to dupe the vulnerable and to turn people against their fellow citizens, neighbors, and loved ones.

The first wave of policy responses—including GDPR—represent important pioneering efforts by policymakers to at least increase awareness of the contours of the problem. But largely these have created click-through regimes that probably very few internet users read. As the current Chair of the Federal Trade Commission Lina Khan recently suggested, these procedural protections are not enough.[21]

Blockchain technology 1.0

The internet permits decentralized and unaffiliated nodes (computers, phones, devices) to connect and exchange information. Blockchain technology takes the internet one step further and permits unaffiliated nodes to cooperate to maintain and update a ledger accurately and instantaneously, even though these nodes are self-interested and otherwise have no reason to trust each other.[22]

Current blockchain solutions accomplish this by essentially requiring each node to "yell the answer out loud"—in other words, all updates to the ledger are publicly announced in order to be recorded on an immutable ledger and are then accessible by anyone with an internet connection. In the context of financial applications, this is like requiring that all Venmo users use only the "public" setting (a social media feature that broadcasts the amount of the transaction and the participants to other Venmo users). The pseudonymity feature of blockchains like Bitcoin—which use your "public address" instead of your literal name or email address—provides little protection because it is a light lift for motivated observers to connect real life identities with public blockchain addresses (as firms are already doing). And once a user's wallet address has been linked to her real identity, observers can resurrect the entirety of that person's transactional history—a risk that does not exist in the traditional financial system. This endogenous transparency significantly limits the use cases for this technology. A financial system built on an open and transparent blockchain would be extremely concerning for individual autonomy, since purchases may say more about individuals and their identities than they would otherwise be willing (or even safe, in the case of some vulnerable groups) to share. Likewise, such a system would be unworkable for corporate data that constitutes trade secrets or that companies are not prepared to share more broadly.

---

[18] *See, e.g.*, *Last Week Tonight: Data Brokers*, YOUTUBE (April 11, 2022), https://www.youtube.com/watch?v=wqn3gR1WTcA.
[19] *See, e.g.*, *supra* note 9.
[20] Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, WIRED (March 17, 2019), https://perma.cc/MND2-6RAT.
[21] Statement of Chair Lina M. Khan, *supra* note 10 (asserting that process requirements sidestep "more fundamental questions about whether certain types of data collection and processing should be permitted in the first place").
[22] Distributed ledgers like Bitcoin and Ethereum use a native coin to incentivize nodes to do the work of verifying the accuracy of submissions to the ledger (otherwise those nodes wouldn't waste their time and energy to do so). As a result, this means the first use case for these ledgers is keeping track of these coins. But, as many have pointed out, there is no reason why similar algorithms couldn't use native coins to incentivize verification of non-financial applications (*i.e.*, to keep ledgers about something other Bitcoin or ETH account summaries).

The openness of these systems also limits non-financial applications. Distributed ledgers could, for example, be a more useful way to store electronic health records. In the status quo, if a healthcare patient moves or switches providers, the patient must arrange with their first doctor to transfer files to the second doctor—and risks losing medical records by failing to do so. This is because each healthcare provider functionally maintains a ledger for each patient on its own proprietary and functionally non-interoperable system (despite regulatory efforts to make these systems interoperable[23]).

In other words, the status quo gives healthcare providers physical and electronic ownership of their patients' records. A distributed ledger could turn that system on its head, making patients the owners of the records, while healthcare providers could serve as nodes that update records. In that system, the records travel with the patient even if they change healthcare providers. This would be a more convenient experience for patients, one that recognizes that their healthcare data belongs to them—and that healthcare providers merely update but do not own this data. Ironically, while this "decentralizes" data (returning it to the user), techniques like homomorphic encryption, multiparty computation, and differential privacy can make that data more broadly available for scientific analysis (and even the development of AI) *without* compromising privacy.[24]

The problem, however, is that the architecture of current blockchain technology means that each healthcare provider would "yell the answer out loud" and record that answer for all to see. Many would understandably not want this in the context of healthcare—or in many other contexts, as such records could consist of information that people or companies may not want to broadcast to others. Worse, if people adopt these systems without understanding the privacy implications—as happened with many applications on the internet—large swaths of consumer data would be available for exploitation. In that world, where it becomes too late for us to build our values into the code we use, the task for policymakers will be damage control.

Part II - Advanced Cryptography Can Provide Infrastructure-level Solutions

The data insecurity on current distributed infrastructure is staggering. The lowest-hanging fruit is information that companies store about their customers that they must store—even if they would rather not—to efficiently run their business. Take an early example: passwords. Originally many websites stored passwords on company servers. This was a risky practice because if hackers got access to those databases, they could access customer accounts. The clever and "enabling" solution was to stop storing the passwords and to instead store encrypted ("hashed") versions of their passwords (and over time, using more sophisticated techniques like "salting" to further protect customer data against increasingly sophisticated attack strategies like dictionary attacks).[25] This solution, while broadly implemented for passwords, has not been implemented for the overwhelming majority of data stored on servers.

More recently, the development of advanced cryptographic technique—such as ZKPs, homomorphic encryption, multi-party computation, and differential privacy—unlock an entirely new toolkit and design space for addressing these challenges. Aleo is particularly interested in the potential of ZKPs, which allow individuals and entities to prove that something is true—with overwhelming mathematical certainty—without sharing the underlying data.

A ZKP of a particular statement has three features. First, the proof must be "complete," meaning if someone provides the proof, we know with certainty that the particular underlying statement being

---

[23] *See, e.g.*, Promoting Interoperability Programs, CMS (Jan. 9, 2023), https://perma.cc/MBY2-ZYLE.
[24] *See, e.g.*, Understanding Differential Privacy, U.S. CENSUS BUREAU, https://perma.cc/C46F-XAKV.
[25] MIKE ROSULEK, THE JOY OF CRYPTOGRAPHY 204-205 (2021), https://joyofcryptography.com/pdf/chap11.pdf.

proven is true (*i.e.*, there is no further trust required). Second and related, it must be impossible for someone to provide a ZKP of a particular statement if that statement is false. Finally, the proof must be "zero knowledge," meaning the proof should not reveal anything about the statement other than the fact that the statement is true. One classic example demonstrates how these conditions may be satisfied. Imagine you want to "prove" that you know Waldo exists on a poster, but you don't want your counterpart (the "verifier") to know *where* Waldo is. You could hide the poster underneath a large piece of cardboard that has a cutout that is precisely the shape of Waldo, thereby allowing you to prove Waldo exists without providing any information on his whereabouts.[26]

Since ZKPs were first discovered in 1985,[27] researchers have devised techniques to reduce compute time and complexity, making ZKPs more practical to implement. Indeed, Aleo's team and advisors have been doing research at the cutting edge of this space for many years.[28] As this shift happens, below are just some of the potential applications for such a technology:

- **Identity Management.** Proving identity without needing to share an actual passport or driver's license. The process is similar to the existing workflow for creating and verifying passwords. The user takes the relevant information (*e.g.*, an email or passport) and posts it to an endpoint that creates a credential demonstrating something about that person's identity—that it has been verified according to exacting standards, that the person is over 18, or other salient characteristics about the user. That credential can then be leveraged wherever it is accepted. This system minimizes how the underlying data (email, passport, etc.) is shared so as to significantly reduce vulnerabilities, as well as the risk that irrelevant or inappropriate factors such as race or gender are considered by the individual or entity requesting the credentials. If implemented, this technology can save millions of users from data breaches where identifying material is exposed.[29]
- **Authentication and Provenance.** Beyond identity, this allows us to confirm the authenticity of data without necessarily stamping PII on files (*e.g.*, photographs) that are widely distributed. Computer scientists have already suggested this as a means of combating disinformation.[30]
- **Private records that third parties can update.** *E.g.*, Health records, as discussed above.
- **Data control.** Data control as the "internet of things" blossoms. The capacity for oversharing of raw data increases exponentially as consumers use more and more devices that share information.[31]

---

[26] Another common example is using a wristband to demonstrate age (rather than sharing date of birth each time). *See also Computer Scientist Explains One Concept in 5 Levels of Difficulty*, WIRED (Jan. 1, 2022), https://www.wired.com/video/watch/5-levels-zero-knowledge-proof; Matthew Green, *Zero Knowledge Proofs: An illustrated primer*, CRYPTOGRAPHY ENGINEERING: BLOG (Nov. 27, 2014), https://perma.cc/FHE7-PZ7S.

[27] Shafi Goldwasser et al., The Knowledge Complexity of Interactive Proof-Systems, *in* PROVIDING SOUND FOUNDATIONS FOR CRYPTOGRAPHY: ON THE WORK OF SHAFI GOLDWASSER AND SILVIO MICALI (Oded Goldreich ed., 2019). The authors subsequently won (along with two others) the Gödel Prize for this work, a prestigious prize for outstanding papers in the area of theoretical computer science.

[28] *See, e.g.*, Sean Bowe et al., ZEXE: Enabling Decentralized Private Computation, *in* 2020 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) (2020), https://ia.cr/2018/962 (multiple Aleo team members including co-founder and CTO Howard Wu demonstrating how to implement ZKPs in distributed systems).

[29] *See, e.g.*, Michael Rosenberg et al., zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure, *in* 2023 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) (forthcoming May 2023), https://eprint.iacr.org/2022/878.pdf.

[30] *See, e.g.*, Trisha Datta and Dan Boneh, *Using ZK Proofs to Fight Disinformation*, MEDIUM: DAN BONEH (Sept. 29, 2022), https://perma.cc/65X2-J289.

[31] *See, e.g.,* Sue Halpern, *Private Eyes*, NY BOOKS: THE NEW YORK REVIEW (March 9, 2023), https://www nybooks.com/articles/2023/03/09/private-eyes-the-fight-for-privacy-citron/ (explaining how Roomba's photographs of users' homes were lost in a data breach, including images of a customer using the toilet).

But that data can be encrypted and confirmed with ZKPs in order to protect against cyber-attacks, and yet still be made available for machine learning.

- **Proving without oversharing.** Proving things like financial health (*e.g.*, FICO scores) without needing to share bank statements or other highly sensitive specific information that can be abused, exploited, or negligently treated by the recipient.
- **Compliance tools.** ZKPs allow for greater access control and separation of responsibility in enterprise and governmental systems. They can also enable cross-validation of data to ensure accuracy and prevent fraud, trace provenance (*e.g.*, for weapons tracking), and enhance bank regulation techniques (*e.g.*, by programmatically updating new regulatory requirements or proving compliance with capital ratios and other solvency requirements in real time).
- **Secret ballot voting.** Voting in a secret ballot system where the ledger is not controlled by one entity so that third parties are more confident that the ledger has not been tampered with.
- **Digital Dollars.** The need for privacy here is apparent, and has been noted by the President's Executive Order on Ensuring Responsible development of Digital Assets,[32] the Federal Reserve, [33] the G7,[34] and the Digital Dollar Project. [35] ZKPs can allow for digital dollars in which privacy is guaranteed, while giving issuers or other intermediaries tools to comply with applicable regulations (e.g., a centralized issuer can KYC users and retain decryption keys called view keys that allow compliance and audit teams to identify users and suspicious transactions).
- **Diplomacy.** In 2016, the Princeton Plasma Physics Laboratory demonstrated a technique that could allow inspectors to confirm disarmament (*e.g.*, whether an object is indeed a nuclear weapon) without recording or revealing the internal workings of the weapon, which might be secret.[36]

The impact on semiconductors

The bipartisan CHIPS and Science Act of 2022 recognizes the national security and economic significance of the semiconductor industry.[37] In light of that, it's important to understand that advanced cryptography (including ZKPs) will require computations that can be optimized at the hardware level. This is because ZKPs will require repeating similar math at the software level—and repetition at the software level benefits from optimization at the hardware level. In this case, it will soon become possible to optimize and run these operations orders of magnitude faster using specialized hardware like field programmable gate arrays ("FPGAs") and application specific integrated circuits ("ASICs").

This means that the country that takes the lead in leveraging advanced cryptography will also have the expertise and the incentive to optimize hardware. Aleo is on the pioneering edge of this technology, and we believe it will create an entirely new multi-billion dollar industry. We have sponsored testnets that have yielded surprising and significant levels of progress in computation times. In addition,

---

[32] *Executive Order on Ensuring Responsible Development of Digital Assets,* THE WHITE HOUSE: PRESIDENTIAL ACTIONS (ISSUED MARCH 9, 2022), https://perma.cc/YC66-BYLA (mentioning privacy ten times).
[33] Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, FEDERAL RESERVE (Jan. 2022), https://perma.cc/D6BR-ZG8A ("[p]rotecting consumer privacy is critical").
[34] Rishi Sunak & Andrew Bailey, *Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)* (2021), https://perma.cc/E69B-E2YK.
[35] *Privacy Principles for a Digital Dollar,* DIGITAL DOLLAR PROJECT, https://perma.cc/GAW4-JD5N.
[36] John Greenwald, *PPPL and Princeton demonstrate novel technique that may have applicability to future nuclear disarmament talks,* PRINCETON PLASMA PHYSICS LAB'Y (Sept. 20, 2016), https://perma.cc/52SF-ZQYB.
[37] *FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China*, THE WHITE HOUSE: STATEMENTS AND RELEASES (Aug. 9, 2022), https://perma.cc/9GV2-F27C.

we helped create and sponsor Z-prize, an industry-wide effort that awarded millions of dollars to contestants who significantly improved the latency, throughput, and efficiency of computing ZKPs across multiple hardware platforms, including specialized hardware such as GPUs and FGPAs.[38]

Aleo plans to invest significant sums of money into this technology. If—and as—applications increase exponentially, it is our view that early winners can develop a significant lead, as the markets have witnessed with Intel on CPUs or Nvidia and AMD with GPUs. In other words, this technology is not amenable to a "wait and copy" strategy; as the history of semiconductors highlights, those who take the lead in specialized technology can often retain a formidable advantage.[39]

Support from the government

There are two areas where the government can act to help American companies innovate and take the lead in this race: inspiring demand and addressing regulatory uncertainty.

Inspiring demand. While compute times for ZKPs are significantly reducing,[40] there is still a "chicken and egg" problem with supply and demand; the supply of computing infrastructure for ZKPs is low because the demand is low. This is because there are few products to create demand, which in turn keeps the supply of computing infrastructure low. The introduction of demand signals will greatly increase investment in the space. To that end, and to stay on the cutting edge of data security, the government should explore pilot projects that leverage the technology. The Treasury Department and the Federal Reserve, in investigating a digital dollar, have already noted the importance of privacy and compliance with existing regulations.[41] As mentioned above, ZKPs allow for configurable levels of privacy—*i.e.*, the government could make privacy the default but retain the ability to view transactions when authorized (*e.g.*, with a warrant, or when required by applicable law like the Bank Secrecy Act).

There are myriad potential government use cases. The Social Security Administration could launch a pilot program on digital identity. The Census Bureau already leverages differential privacy to protect the privacy of participants;[42] it can and should explore using ZKPs to reduce data retention without losing the ability to conduct data analysis and may even be required to do so under its own disclosure avoidance regime.[43] The Office of Personnel Management could do the same with fingerprints and other information that it wishes to leverage but not necessarily store. These projects would spur even more innovation that could help ensure the United States is on the leading edge of applied cryptography.

Regulatory uncertainty. It's important to understand the role of the native tokens (such as Bitcoin or ETH) in distributed ledger systems. Distributed ledgers work because their algorithm incentivizes participation by rewarding that participation—specifically the work it takes to ensure the ledger's

---

[38] *See* Alex Pruden, *Announcing The Inaugural Zprize Competition Results*, ZPRIZE (Dec. 6, 2022), https://www.zprize.io/blog/announcing-zprize-results.
[39] CHRIS MILLER, CHIP WAR: THE FIGHT FOR THE WORLD'S MOST CRITICAL TECHNOLOGY (2022).
[40] Thanks in part to government efforts. *See, e.g.*, Dr. Joshua Baron, *Securing Information for Encrypted Verification and Evaluation (SIEVE)*, DARPA, https://perma.cc/4EXH-NF3U.
[41] *See, e.g.*, *The Future of Money and Payments*, DEP'T OF THE TREASURY (Sept. 2022), https://perma.cc/6K5T-GUC6.
[42] *Statistical Safeguards*, U.S. CENSUS BUREAU, https://www.census.gov/about/policies/privacy/statistical_safeguards.html.
[43] *See* 2020 Decennial Census: Processing the Count: Disclosure Avoidance Modernization, U.S. CENSUS BUREAU, https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html.

accuracy—with native digital tokens generated by that algorithm.[44] For instance, Bitcoin pays miners with Bitcoins, and Ethereum pays its validators with ETH. Nothing about ZKPs or other privacy enhancing technologies changes the need for these tokens as part of ensuring the accuracy and security of distributed ledgers. There are significant unresolved policy questions about the regulatory status of these tokens—specifically whether they are securities and must comply with a regulatory framework designed for wholly different types of assets—as well as how to adopt risk mitigation frameworks that comply with rules designed to prevent illicit finance.

The absence of a comprehensive regulatory framework around digital tokens has created substantial uncertainty for companies wishing to innovate in this space within the bounds of the law. In this environment, the concern is that the advantage goes to unscrupulous players or those who innovate abroad. Aleo believes the United States is the best place on earth for innovation, and that good regulations can protect everyone—the public, internet users, and even the companies that those rules regulate. That's why it's so important for these regulations to be adapted to what is unique about distributed ledger systems, so that regulations enable responsible innovation rather than ending risk by ending innovation.

The government does not need to compromise its longstanding public policy goals to promote this kind of innovation. The primary consequence of advanced cryptography will be enabling new, better, and more secure systems. At the same time, the same bad actors who try to use the internet for scams, frauds, illicit finance, or other malfeasance will not shy away from new technologies; just as we did with the internet, we need to identify ways to cabin, deter, and punish this behavior.

Applied cryptography can help. For instance, it can help promote data security**.** Right now, the absence of data security infrastructure on the internet has left thousands of honeypots for hackers and cybercriminals. ZKPs can secure vast swaths of this data without compromising functionality. More fundamentally, leveraging ZKPs as authentication can help reduce identity theft and identity-related crimes, which are mushrooming as "deep fake" technology becomes more prominent. Professor Danielle Citron and others have done tremendous work highlighting the enormous scale of abuses—ranging from revenge porn to fraud—taking place online right now.[45] No doubt this is a growing problem.[46]

Not all of those issues can be solved with technology, but at least some and perhaps many of them can. This is because cryptography allows us to demonstrate content is not authenticated (and thus likely faked)—or that it was shared without consent; integrating these capabilities with multiparty authentication (which can require the consent of those depicted) could create a world where platforms and providers can easily search for and remove non-consensual or faked material. These technological solutions, paired with other public policy responses, could help stem abusive practices.

Finally, it is important to understand distributed ledger technology in the context of distributed systems like the internet, even—and especially—for purposes of thinking about compliance. The notion that distributed ledgers can create an unaccountable, untraceable black box for criminal activities will—just like the notion that the internet would do the same—give way to the commercial need for identification and authentication, tools that can in turn be important instruments for law enforcement.

---

[44] Sina Kian, *What are cryptocurrencies good for?*, MEDIUM: SINA KIAN (Aug. 12, 2021), https://perma.cc/DPD6-WLQN.

[45] DANIELLE CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE (2022).

[46] Sami Quadri, *Former US ambassador says Russia is using 'deepfakes to impersonate him'*, EVENING STANDARD (Oct. 1, 2022) https://perma.cc/9HWP-6XCL.

In the meantime, ample avenues exist for managing risk on distributed ledgers. First, interactions on the base layer require procuring and spending that base layer's token (the cost of having a node process your transaction); the exchanges that allow users to purchase these coins can and should be made to KYC their customers. This alone would ensure that the overwhelming number of those holding tokens are subject to oversight—and the traces left by this activity will be difficult to obscure, especially at scale. Second, these systems all depend on nodes and validators for their security; insofar as these validators can be encouraged to domicile in the United States, they can play an important part in setting standards and preventing bad behavior. For instance, following a large theft of ETH tokens, many validators collectively decided to fork the blockchain and create a ledger in which the theft had never occurred, thus effectuating a technological version of "restitution" (restoration of funds to victims).[47] Third, the authentication potential of ZKPs can help upgrade outdated KYC practices and provide a greater check on bad actors. They can be updated and refreshed more frequently and, even with ZKPs, identity solutions can build in mechanisms for ensuring compliance.[48]

Finally, regulators can continue to achieve compliance at the application level.[49] Over the past ten years, public discussion has focused on the infrastructure layer because these systems—like Bitcoin and Ethereum—were new and exciting, and because many speculated on their value by purchasing their local coins. But the future of distributed systems depends not on their infrastructure, but on the applications their infrastructure enables. These applications will overwhelmingly be subject to regulations in their current form—and where they are not, it is incumbent on policymakers and the private sector to work together to enable new paradigms while addressing important public policy goals.

The history of distributed systems—whether telegram or the internet—has demonstrated that these systems are always more regulable than we think.[50] The best way to address the challenges of new technology is to invest in understanding them, so that we can understand how to achieve our public policy goals. Aleo is betting on the future of advanced cryptography, and betting that America will be and should be its home. We welcome any conversations on the best way to make that happen.

Respectfully submitted,

Sina Kian

Sina Kian
Chief Operating Officer & General Counsel, Aleo Systems, Inc.

Cc: Counsel to Aleo on this matter:
Wilmer Cutler Pickering Hale and Dorr LLP
Zachary Goldman, Esq.
Tiffany Smith, Esq.
Jason Raymond, Esq.

---

[47] Camila Russo, The Infinite Machine, ch. 21 (2020).
[48] *See, e.g.*, Lessig, *supra* note 4, at 70 (conceptualizing identity solution that "could radically increase privacy, as well as security, for all except those whose behavior can legitimately be tracked").
[49] *See generally* Miles Jennings, *Regulate Web3 Apps, Not Protocols*, A16zcrypto (Sept. 29, 2022), https://a16zcrypto.com/web3-regulation-apps-not-protocols/.
[50] *See, e.g.*, Goldsmith, *supra* note 4, at 124.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Aurum Digital Currency

Designing Money [Extended Abstract]

Leonard Adleman
University of Southern California
[redacted]

Rolfe R. Schmidt
[redacted]

1 Abstract

Money has existed in various forms for thousands of years. The ancient Lydians used coins of gold-alloy; the ancient Chinese, notes of paper. Today, the most important form of money is bank money (BM) issued by governments and stored in databases.

It is the transfer of BM, through the use of payment cards (e.g. debit cards, credit cards, gift cards), that underlies the bulk of Internet commerce. Recently, cryptographically based forms of money, such as Bitcoin, have arisen as an alternative to BM. Bitcoin, has made it clear that digital money can be designed to meet specific needs, and that the tools of computer science can endow money with remarkable properties.

We will argue that existing payment card systems are slow, costly, and a threat to privacy, and that Bitcoin does not meet the needs of governments. We will present a new form of money, Aurum, designed from first principles to be issued by governments and other trusted institutions.

Aurum is based on a simple but novel technological primitive we call "automatic replacement". With automatic replacement, each transaction results in the permanent destruction of the buyer's note, and the virtually instantaneous creation and delivery of a new note for the seller. We will argue that the use of automatic replacement can yield greater privacy that either Bitcoin or payment card systems.

We have implemented Aurum in prototype and simulated transactions at a rate of over 7000 per second (approximately the average transaction rate for the entire US economy). As reported below, each transaction was completed in milliseconds at a cost of less than one-thousandth of a cent.

We will describe how such a low cost high-speed form of digital money can lead to a new wave of innovation and be the basis for future economic growth.

2 The Origin of Government Money

In the West, the first government money appears to have been a Lydian coin issued in about 650 BC that bore the stamped likeness of a lion with sunburst, the symbol of the king [25]. The imprimatur of the state allowed Lydian coins, and the government money that followed, to supplant earlier forms. The success of government money in general, and the Lydian coin in particular, was based on trust; trust born from power. People could trust Lydian coins because the state had the power to guarantee their weight and metal content, to ensure that they were accepted throughout the realm, and to execute counterfeiters.

No sooner did government issued coins exist than states, such as Athens, began to manipulate them for social purposes [14]. Monetary policy had arrived. Governments have never relinquished their prerogative to use their money for what they deem to be good purposes, and it seems likely that they will resist innovations that might deprive them of that prerogative.

3 United States Physical Currency

In 1789, Article 1, Section 8 of the United States Constitution granted Congress the power to "coin money", thereby giving birth to the United States Dollar (USD). At that time, USD took the form of metal coins, but today it includes paper notes and BM. All forms of USD are governmentally regulated and issued by the Federal Reserve.

We still have notes and coins, which together we will refer to as United States Physical Currency (USPC). USPC has persisted because it has many desirable properties. It also has at least one undesirable property - mass; it cannot travel at the speed of light and cannot be used for digital commerce. This leads us to consider the problem of designing a form of government money that retains the desirable properties of USPC, but is digital. Let's review some of these properties:

- Privacy: Most often, when we spend USPC, we do not give our names or other private information. However, this privacy is not absolute. For example, the Government requires that businesses report the identity of individuals spending USD in any form in amounts of ten-thousand dollars or more.

  In general, the privacy conferred by a form of money is intimately related to the nature of the information, what we call the footprint, left by transactions. Often, when small amounts of USPC are used for common purchases, virtually no footprint is left. However, under other circumstances the footprint may be substantial. For example, when USPC is used in banks, the footprint may include hard-copy, digital and even video records that persist for a great deal of time. These records may contain information such as times, amounts, names, addresses, account numbers and even social security numbers.

- Security: Security has many aspects, but some of the most important are:

  - Resistant to counterfeiting. The Government combats counterfeiting by integrating physical features, such as water marks and 3D ribbons, into its notes, so that widely available methods of duplication and printing will produce copies of insufficient quality to be passed. The current approach is good, but not perfect. For example, it has been widely rumored that North Korea possesses presses on which it produces counterfeit one-hundred-dollar bills that defy detection [20].
  - Resistant to double spending. For USPC, controlling counterfeiting is sufficient to control double spending. We trust that once an individual spends a note, they no longer possess a passable copy, and cannot spend it again.
  - USPC is not secure against misplacement or theft. Once an individual loses possession of a note, no one, not even the Government, will replace it. This lack of security arises from our use of coins and notes as negotiable bearer instruments. If you possess it, you may spend it.

- Universality: USPC has many properties that facilitate its wide spread use. Among them:

  - Using USPC does not require special status: For example, the unbanked and underbanked, who may lack sufficient status to have a relationship with a financial institution, can use USPC.
  - Using USPC does not require special skills: The vast majority of individuals, including the illiterate, innumerate, and atechnical can use USPC.
  - Using USPC does not require special technology: notes and coins may be used in environments with minimal infrastructure; there is no need for computers or even pens.
  - Using USPC does not require significant time: For example, settlement is instantaneous. When a dollar bill is spent, the recipient immediately receives a dollar bill and may immediately spend it.
  - Using USPC does not require substantial expense: Neither buyer nor seller pays a processing fee when using a dollar bill. However, in considering expense, one should include the cost of maintaining the system. When existing notes become unfit, they are collected, destroyed, and replaced by new ones. In 2016 the Federal Reserve spent $660 Million to print new bills worth $216.5 Billion [18]. These notes are reused. From this, it seems reasonable to estimate the mean cost per transaction as less than 0.1% of transaction value.
  - Widely accepted: Because the US Government demands it, USPC may be used at many places to buy many types of goods and services, to satisfy debt, and to pay taxes.
  - Small denominations: A penny can be used to transfer what is viewed by many as a trivial amount of wealth. As a result, goods and services of small value can be bought and sold, and those of larger value may be priced with high precision.

- Governability: The Government regulates the USD to enact monetary policy. Government action, such as quantitative easing, changes the value of our USD. The Government also regulates USD in an effort to prevent financial crimes. For example, the Bank Secrecy Act requires that financial institutions report all USD transactions of ten-thousand dollars or more, and all "suspicious activity".

The Government has determined that it is worthwhile to sacrifice some privacy for the law enforcement and national security benefits of deterring money laundering in the service of crime or terrorism.

The hard learned lessons of the past have led to the laws and regulations that today govern the economic affairs of financial institutions, companies, and individuals. Whether you approve or not, we have left important decisions about our money and our economy to the political process.

4 Payment Cards

Banks store BM using database management technology. Transferring BM between account holders typically requires a distributed transaction involving the databases of multiple banks and third parties. Ultimately, the payer's account balance is reduced, the payee's account balance is increased, and the balances of the banks' accounts at central banks or clearing houses are adjusted to offset the change in liabilities. Institutions use various electronic funds transfer systems to transfer BM, but individuals typically use payment cards.

Today, the transfer of BM via payment cards is the primary means by which individuals make purchases over the Internet. Payment card systems have the following properties:

- Privacy: Card payments leave a large footprint. The card itself has your full name, physical signature, card number, expiration date, and card security code. The magstripe has similar information. When you use a card, the information is commonly stored together with a date and time of use, location of use, and a list of items purchased. All or part of this information is typically retained in the databases of merchants, banks and various third parties involved in the BM transfer. This footprint can lead to dramatic privacy breaches such as the one that occurred at Ashley Madison in 2015 [6]. There can be little doubt that concerns about privacy breaches diminish the customer base of sensitive sites, but they can also have a chilling effect on basic freedoms, for example, by inhibiting the purchase of books on controversial political topics.

- Security: The information on the card or the magstripe is sufficient for a criminal to use your card for purchases. The few technical barriers to criminal use seem meager. For example, when a signature is required, it can be forged, and the realities of the marketplace seldom allow for close scrutiny and detection. At some locations, such as gas stations and Internet sites, no signature is required. In 2013, the cost of fraudulent payment card use in the United States was 7.1 billion dollars[29].

  The payment industry has done an effective job of concealing this cost from purchasers by indemnifying them. This indemnification protects purchasers, but is paid for by merchants in the form of transaction fees, and ultimately manifests itself in the form of higher prices for consumers.

  The payment card industry has made significant efforts to improve both privacy and security, as is seen in the EMV standards [15]. These changes, however, are no panacea and significant challenges remain [5].

  Payment card footprints put merchants in the unenviable position of having to protect personal information that in many cases they don't need and would prefer not to have. Predictably, attempts by merchants to protect this information often fail. The direct costs and damage to merchant reputations can be substantial as the recent incidents at Target and Home Depot demonstrate [31].

  Because today's banking systems have grown organically, the resulting architecture is complex. This has created vulnerabilities even at the highest levels, as demonstrated by the recent theft of $81 million of Bangladesh Bank funds directly from their account at the Federal Reserve Bank of New York [8].

- Universality: Payment cards enjoy some of the universal properties of USPC. They require little in the way of special skills, are widely accepted, and can transfer small amounts. However:

  - Using payment cards does require special status: acquisition of bank accounts and payment cards requires economic status. This status barrier prevents the unbanked and underbanked from participating fully in today's economy and leads to significant social problems.

  - Using payment cards does require special technology: Online purchasers only require basic computing, but merchants may require special devices and communications technology.

  - Using payment cards does require significant time: Though this is not apparent to the purchaser, it is to the merchant. When you use your card, the merchant's account will be augmented, but the process can take days. During this settlement time the merchant cannot use the money that has been promised.
  - Using payment cards does require significant expense: In the case of credit cards, merchants pay interchange fees of close to 2% of the transaction [13]. Analogous fees for debit cards are approximately 0.79%[1]. Additional markups, sometimes significantly higher, are charged by acquiring banks. Merchants may need to purchase or lease special equipment.

    Consumers also pay. With credit cards, they can spend money they do not possess. If the debt they acquire is not paid promptly, it can lead to fees, penalties, and interest charges. Frequently, credit card debt is not paid promptly, and, in many cases, the burden becomes sufficiently great that bankruptcy results. The total credit card debt in the United States is over 700 billion dollars [26].

- Governability: Payment card transfer BM which is highly governable. For example, the Federal Reserve System was set up in 1913, in large part to facilitate United States monetary policy. Central banks have developed numerous tools for controlling the supply and flow of BM. BM is also governable for law enforcement purposes. For example, the Bank Secrecy Act rule [31 CFR 103.33(g)] – the "travel rule" – requires that US financial institutions pass identifying information with certain fund transmittals of three-thousand dollars or more. Because of the complex architecture of today's banking systems, such governance sometimes creates significant burdens for financial institutions, and the fragmented information that results can be difficult for law enforcement to obtain and analyze.

5 Bitcoin

The use of cryptography in the design of money began in 1985 with a prescient paper by Chaum[11]. Chaum described the tension between organizational and individual security and proposes systems to deal with the resulting problems. Among the proposals is a system for electronic cash which maintains a list of spent notes to prevent double spending. A similar approach is used in Aurum. See also [12, 10, 24].

Bitcoin was introduced in 2008 [23]. Among its most important properties are:

- Privacy: Paradoxically, though it appears that the designer(s) of Bitcoin placed a high value on privacy, it was not achieved. Bitcoin is not inherently private. On the contrary, it is quite transparent. The footprints of Bitcoin transactions are stored in the blockchain, which is large, permanent, and open for all to read. This has been used to glean significant information about Bitcoin users, as seen in [21, 22, 27, 9].

- Security: The system is designed to prevent double spending using a proof-of-work scheme. It was initially claimed that to compromise the system an attacker would need to hold 50% of the computing power of the bitcoin network [23]. It has since been shown that as little as 25% will suffice [17], and there is no proof that an even smaller percentage might not be sufficient. An examination of the miners at the instance of this writing shows that two colluding miners can execute a 25% attack and three colluding miners can execute a 50% attack. Perhaps this should be a concern. In any event, the security of Bitcoin is an open question.

- Universality: Bitcoin enjoys some of the universal properties of USPC. For the common user, it does not require special technology beyond basic computing, and it can be used to transfer small amounts. It does not require special status; it can be used by people without a relationship with a financial institution. In addition, Bitcoin can cross international borders easily and be used by virtually all people.

  - Few special skills are required: Bitcoin software is improving and lightweight applications make it easy for people to transact on the Bitcoin network. Those users operating full nodes need greater technical skills. Those acting as miners must be expert.
  - Using Bitcoin does require significant time: In practice many users accept "zero confirmation" bitcoin transactions which give an impression of real-time settlement. This practice leaves payees vulnerable to loss through double spending. Certainty of

  payment comes with inclusion in the blockchain. This takes about 10 minutes to get a one-block confirmation, and one hour for the recommended six-block confirmation.

  - Using Bitcoin does require substantial expense: Bitcoin users pay direct transaction fees and they pay for mining rewards through inflation. The site [2] monitors this cost in real time. Recently this cost has ranged between one and two percent of total transaction value. This is more expensive than debit cards and comparable to credit cards. In the future, when mining rewards are removed, the expenses incurred by miners will not disappear, and will have to be covered by transaction fees alone.

  - Bitcoin is not widely accepted: While bitcoin's acceptance has grown through time, it is currently accepted by few retailers. If Bitcoin obtains the imprimatur of a state this could change.

- Governability: Bitcoin was designed to prevent governability. It might be governable by the so called "core developers", but such governance would neither be democratic, nor wielded by an agent with a history of trustworthiness. In addition, any governance, whether by a state or not, appears to be antithetical to the underlying principles of many Bitcoin users. This lack of governance is likely to make governments reluctant to adopt Bitcoin and, in fact, resistant to it.

  Lack of governability not only makes it difficult for authorities to regulate the system, it also causes problems for Bitcoin itself, as seen in the recent block size debate[3]. Other blockchain based crypto-currencies such as Ethereum have been forced to improvise governance to overcome unanticipated crises [16].

6 Aurum

Our goal in designing Aurum was to produce a digital form of money that preserved the desirable properties of USPC. The resulting system had to be fast, inexpensive, and secure, while preserving privacy and enabling governability. We wanted the system to be composed from simple easily understood primitives so that its properties could be clearly seen and considered.

All forms of money must have a means of curtailing counterfeiting, but for digital forms of money, this problem is exacerbated because digital documents can be easily and perfectly copied.

To meet the counterfeiting challenge, Aurum uses *automatic replacement*. *Automatic replacement* is similar to the Federal Reserve process of removing physically unfit notes and replacing them with fresh ones from the Bureau of Engraving and Printing; however, *automatic replacement* takes advantage of modern technology and replaces Aurum notes on each transaction. When an Aurum note passes from a sender to a recipient, the sender's note is destroyed, and a new note is created for the recipient, who may immediately spend it.

In a typical implementation of the Aurum system we have:

- The Issuer: The agent responsible for governing the Aurum system. In particular, the Issuer may order the creation and distribution of notes. The issuer may be a government, but can be any institution. For example, private companies or commercial banks, can act as Issuers to create their own versions of Aurum. The acceptability of issued notes will depend on the power and trustworthiness of the Issuer.

  In what follows it will be convenient to use the US Government as an example. In that case, the natural choice for Issuer would be the Federal Reserve, and Aurum would be intended to be a new form of USD.

- The Authority: An Internet agent responsible for creating notes, destroying notes and overseeing the passage of notes between users. While the Authority must be controlled by the Issuer, it may be hosted by a third party. The Authority maintains:

  - A *destroyed list*. The destroyed list is used to prevent double spending.

  - A public-key, P_A, and a corresponding secret key, S_A, of the RSA public-key cryptosystem, or some other suitable system. P_A and S_A are used to prevent the illegal creation of passable notes (what we call *de novo* counterfeiting).

  In the prototype implementation described here, the Authority will also maintain:

  - A one-way hash function, H.

  - A note database, D.

All but S_A are, at all times, publicly accessible via the Internet.

- Note-content: A plain text digital document with a well defined syntax that contains a value in USD and a unique identifier such as a serial number. The note-content may contain other information, such as the date of issuance, but we will not explore this further here. Roughly speaking, a note-content is similar to a traditional check that has been filled out but not signed. A note-content has no value.

- Note: The result of applying S_A to a note-content; that is, a note is a note-content signed with the digital signature of the Authority. A note has the value in USD contained in its note-content.

A typical transaction would occur as follows:

1. An online shopper informs a web-based merchant that he would like to pay with Aurum.

2. The merchant generates a public key, P_M, and corresponding secret key, S_M (possibly chosen at random by the merchant for this transaction). The merchant sends the shopper an invoice which contains the amount owed in USD and P_M.

3. The shopper, using a digital wallet application, accepts or declines the invoice. In the case of acceptance, the shopper generates a public key, P_S, and corresponding secret key, S_S (possibly chosen at random by the shopper for this transaction). The shopper selects a set of notes of sufficient value. The shopper combines the selected notes, P_M, P_S, and the amount in USD owed the merchant into a single *automatic replacement* request and sends it to the Authority via a secure Internet channel.

4. The Authority executes an *automatic replacement*:

   - Authenticates the notes and their values by applying P_A and reading the resulting note-contents.
   - Confirms that the notes are not on the *destroyed list*.
   - Places the notes on the *destroyed list* (ensuring that they can never be respent).
   - Creates new notes, N_M for the merchant, and N_S for the shopper's change.
   - Encrypts N_M using P_M producing E_M, applies H to P_M producing A_M, places E_M at address A_M in D.
   - Encrypts N_S using P_S producing E_S, applies H to P_S producing A_S, places E_S at address A_S in D.

5. The merchant applies H to P_M producing A_M, and retrieves E_M from address A_M in D. The merchant decrypts E_M using S_M to obtain N_M.

6. The shopper applies H to P_S producing A_S, and retrieves E_S from address A_S in D. The merchant decrypts E_S using S_S to obtain N_S.

There are numerous variations on how to implement *automatic replacement*, but its effectiveness in stopping double spending requires that all parties share a consistent view of the *destroyed list*. This is accomplished by using well-known database techniques to assure that all *automatic replacements* are ACID (Atomic, Consistent, Isolated, Durable) [19]. In addition, our use of public keys, P_M and P_S, hash function H, and the database D is merely one possible way of providing a secure message delivery service.

6.1 Prototype

The performance demands of the Aurum system will be substantial. Combining data from [32, 7], the number of global payment transactions (cash transactions plus non-cash transactions) does not exceed 2.17 trillion per year or 68.8 thousand per second. In the United States the number of payment transactions does not exceed 247 billion per year, or 7,830 per second. To test the Aurum system's ability to meet these demands, we have built a prototype and deployed it on Amazon Web Services (AWS).

The prototype consists of three core programs: an *automatic replacement coordinator*, a *note destroyer*, and a *note creator*. These programs are written in C++ and rely on the CryptoPP library for all cryptographic operations. They implement an Aurum system using the 2048-bit RSA public-key cryptosystem. The prototype also includes a non-core program: a test client used to measure performance.

The *automatic replacement coordinator* is a stateless server that accepts *automatic replacement* requests from external clients over the Internet. When a request is received, it validates that the input notes are authentic and sufficient to cover the requested output notes. If this validation is successful, the *automatic replacement coordinator* orchestrates a distributed transaction over a private network using a modified two phase commit protocol (2PC) to ensure that *automatic replacements* are ACID. This transaction involves one or more *note destroyers* and one or more *note creators*.

The *note destroyer* maintains the *destroyed list* as a set of memory mapped files. There is one bit for each serial number, and all bits are initially set to zero. When a note is destroyed, the bit corresponding to its serial number is set to one. The *automatic replacement coordinator* cannot modify the *destroyed list* by direct action, and may only modify it though issuing *destroy* requests to the *note destroyer*. The *note destroyer* will cause an *automatic replacement* to fail if it attempts to destroy a note that has already been destroyed by either a pending or committed transaction.

The *note creator* creates new Aurum notes. It is the only program with access to the Authority's secret key, S_A. When called by the *automatic replacement coordinator* with a *create* request containing a list of note-contents, the *note creator* will create the corresponding notes. The *note creator* will cause an *automatic replacement* to fail if notes cannot be created for any reason.

We have also implemented a note database using a shared file system. This is not a core part of the Aurum system, it simply acts as a secure message delivery service. In practice we expect other messaging systems to be used as well.

When eight AWS `c4-4xlarge` instances and one AWS `t2-small` instance were used for one hour, the prototype processed 7,768 transactions per second, approximately the transaction rate of the United States. Amazon charged $6.82.

- The cost per transaction was approximately one forty-thousandth of a cent.
- The mean latency from a client's issuance of an *automatic replacement* request to its completion by the Authority was 16 ms. This should have a negligible impact on user experience.
- The energy use was negligible.

Further tests revealed that Aurum is readily scalable. The charge for running the prototype grew linearly with the transaction rate, while the cost per transaction and latency did not change.

In separate experiments we have successfully implemented a transaction signature scheme similar to those associated with EMV and standard Bitcoin transactions. It would be straight forward to implement a smart contract language scheme which would provide smart contracts without the need for blockchains. We have also built and tested a prototype user app for Android smart phones.

For those who wish to explore the Aurum system for research purposes, we plan to make prototype software available. For further details see [redacted]

In a production system, special purpose hardware should bring down costs and improve speeds. On the other hand, there will be costs associated with maintaining an important organization. To estimate these costs, we used Verisign, a publicly traded company with transaction processing needs similar to those that would be faced by Aurum, as a model. During the third quarter of 2015, Verisign's average daily Domain Name System query load was approximately 120 billion queries per day. During the same quarter, Verisign's total costs and expenses were $111,318,000[30]. Using this model, we estimate that the cost per transaction of a production Aurum system would be approximately one one-thousandth of a cent; orders of magnitude less than Bitcoin and payment cards.

A production Aurum system must survive in the Internet ecosystem. It will be the target of many attacks. It must use the tools that have been developed in academe and industry over the last several decades to resist them. A production system should be geographically distributed and Byzantine fault tolerant. Centralized governance does not mean centralized processing. The destroyed list should be widely distributed and public. Important private keys should be stored in secure locations and secret sharing techniques should be used to distribute them geographically and protect them from compromise [28].

6.2 Aurum Properties

- Privacy: No private information, such as names or account numbers, ever needs to be passed between sender and recipient, sender and Authority, or recipient and Authority. When the Aurum system is implemented as above, the footprint of a transaction consists of one bit in the *destroyed list*. The Aurum system can make failures like those that occurred at Ashley Madison, Target, and Home Depot a thing of the past.
- Security:
  - Resistant to counterfeiting: Under standard cryptographic assumptions, Aurum is secure against *de novo* counterfeiting. The presumed North Korean *de novo* counterfeiting of USPC should have no analogue for Aurum notes.

- Resistant to double spending: Automatic replacement protects Aurum from double spending and counterfeiting by the duplication of existing notes (what we call duplication counterfeiting).
- Like USPC, Aurum notes are negotiable bearer instruments and are not secure against misplacement or theft. No one will replace them. However, Aurum notes appear to have an advantage over USPC. At the option of the user, Aurum notes may be securely backed up, and if an original is misplaced, the back-up may be spent. Hence loss due to misplacement may be mitigated. Commercial banks might offer "online safe deposit boxes" that provide such backup as a service to Aurum users. Similarly, at the user's discretion, loss due to theft may be mitigated with the use of a transaction signature scheme.

- Universality:
  - Using Aurum notes does not require special status: Aurum notes will be usable by the unbanked and underbanked. No accounts or memberships are needed.
  - Few special skills are required: Simple apps make Aurum notes easy for both buyers and sellers to use. Those operating an Authority must be expert.
  - Using Aurum notes does not require special technology: A standard mobile device or personal computer is sufficient for both buyers and sellers.
  - Using Aurum notes does not require significant time: Settlement is immediate. Latency is measured in milliseconds.
  - Using Aurum notes does not require substantial expense: As indicated above, the cost of a transaction should not exceed one one-thousandth of a cent. Financial institutions that offer services such as indemnification or secure storage may charge additional fees. Private institutions that issue Aurum notes might also charge for their use.
  - The acceptance of Aurum notes will depend greatly on the trustworthiness and power of the Issuer.
  - Aurum notes can be denominated in arbitrarily small fractions of a cent.

- Governability: The Aurum system is designed to be governable. With regard to monetary policy, in the United States, the current system of executing policy through the Federal Reserve System is not inhibited by the Aurum system. In addition, the Government can modify monetary policy directly through the Authority. For example, by creating Aurum notes at its discretion.

  With regard to financial crimes, the Aurum system may offer some advantages. For example, the Bank Secrecy Act rule requiring that financial institutions report all USD transactions of ten-thousand dollars or more, can be implemented by requiring such institutions to send personal information consistent with their customer identification program (CIP) to the Authority with each such *automatic replacement* request. The Government requirement that trades and businesses file IRS Form 8300 for certain transactions can be implemented in a similar fashion. Thus the "on boarding" and "off boarding" of Aurum notes into and out of conventional institutions can be controlled as it is today. Because all associated information can be retained in the Authority, when due process provides access for law enforcement, the information may be readily obtained in a standard digital form suitable for analysis.

  So while the basic Aurum system is inherently private and produces extremely small footprints, it is flexible enough to increase those footprints and retain additional information when the political process dictates that it is in the best interest of a country to do so.

7 A World with Aurum

The Aurum system would lead to a more efficient economy and engender important economic innovations.

For example, the insignificant cost of Aurum transactions makes micropayments a reality. Even a transaction for one cent is practical. Anyone who produces digital content can now directly monetize it. There is no need to sell advertising, to force potential consumers to register, to fill out forms, remember passwords, pay subscription bills, endure advertising popups, or provide personal information.

It is reported [4] that the digital New York Times has "60 million unique visitors (U.S.) a month. One million of them pay [via digital subscription]; 59 million don't.". The digital subscribers provide about two-hundred million dollars in annual revenue (approximately one-eighth of the total revenues of the Times). But, if we assume that, on average, each of the 59 million non-subscribing visitors reads one article per day, and that each is willing to pay one cent per article via a non-intrusive one-click, then these visitors would add an additional two-hundred-fifteen million dollars to the annual revenue.

Inexpensive Aurum micro-payments will provide creative individuals the opportunity to enrich the world with their ideas. Budding novelists, musicians, graphic artists, bloggers, videographers, and a host of others may directly enter the market and sell their work for whatever the market will bear.

Banks and other financial institutions will have a new basis on which to create novel instruments or improve existing ones. For example, users may go to their bank website and download Aurum notes; eliminating the need for a trip to an ATM.

With Aurum notes, these innovations can be brought to fruition while retaining security, privacy, and governability.

8 Conclusion

We have proposed a simple new form of digital money, Aurum, that provides fast, inexpensive transactions, while preserving privacy and governability. Bitcoin has made it clear that the public is ready to consider new cryptography based forms of money. It seems likely that money in such forms issued by a trusted agent could gain wide acceptance. It may be the case that existing methods of digital payment, such as payment card systems, which have grown organically and been slow to take advantage of emerging technology, will find it difficult to compete.

The money considered in this paper can be thought of as objects in what we call an ownership system. At its most basic, an ownership system consists of a set of objects and a set of owners. At each moment, the ownership system records which owners own which objects. When the ownership of an object changes, the system must be updated accordingly.

USPC are objects which individuals may own. The USPC ownership system is highly distributed with each object owned by the individual who possesses it. There are ownership systems where money is no object. For example, automobiles are objects which individuals own and for which the ownership system is implemented by state governments in a highly centralized fashion. Stocks, bonds, and medical records provide other examples. Many existing ownership systems have arisen in an unsystematic manner and have acquired undesirable features. It does not have to be that way; as with money, the tools of computer science allow us to design ownership systems that meet prespecified requirements.

8.1 Acknowledgements

We thank Professor Bill Maurer, Professor Donald J. Patterson, Taylor Nelms, and Caitie Lustig of UC Irvine, and Jim Bidzos and Burt Kaliski of Verisign for their careful review of an earlier version of this paper and their suggestions which led to substantial improvements.

8.2 Disclosure

Leonard Adleman is a principle in the company Aurum. Patent pending.

References

[1] URL: `https://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm`.

[2] URL: `https://blockchain.info/charts/cost-per-transaction-percent`.

[3] URL: `https://en.bitcoin.it/wiki/Block_size_limit_controversy`.

[4] URL: `http://www.niemanlab.org/2015/08/newsonomics-10-numbers-on-the-new-york-times-1-million-digital-subscriber-milestone/`.

[5] Ross Anderson and Steven J. Murdoch. "EMV: Why Payment Systems Fail". In: *Commun. ACM* 57.6 (June 2014), pp. 24–28. ISSN: 0001-0782. DOI: `10.1145/2602321`. URL: `http://doi.acm.org/10.1145/2602321`.

[6] *Ashley Madison hack is not only real, it is worse than we thought*. 2015. URL: `http://arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/`.

[7] John Bagnall et al. *Consumer cash usage: A cross-country comparison with payment diary survey data*. Discussion Papers 13/2014. Deutsche Bundesbank, Research Centre, 2014. URL: `http://www.bostonfed.org/economic/wp/wp2014/wp1404.pdf`.

[8] *Bangladesh Bank hackers compromised SWIFT software, warning issued.* URL: `http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR`.

[9] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. "Deanonymisation of Clients in Bitcoin P2P Network". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* CCS '14. Scottsdale, Arizona, USA: ACM, 2014, pp. 15–29. ISBN: 978-1-4503-2957-6. DOI: `10.1145/2660267.2660379`. URL: `http://doi.acm.org/10.1145/2660267.2660379`.

[10] David Chaum. "Online Cash Checks". In: *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology.* EUROCRYPT '89. Houthalen, Belgium: Springer-Verlag New York, Inc., 1990, pp. 288–293. ISBN: 3-540-53433-4. URL: `http://dl.acm.org/citation.cfm?id=111563.111592`.

[11] David Chaum. "Security Without Identification: Transaction Systems to Make Big Brother Obsolete". In: *Commun. ACM* 28.10 (Oct. 1985), pp. 1030–1044. ISSN: 0001-0782. DOI: `10.1145/4372.4373`. URL: `http://doi.acm.org/10.1145/4372.4373`.

[12] David Chaum, Amos Fiat, and Moni Naor. "Untraceable Electronic Cash". In: *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology.* CRYPTO '88. London, UK, UK: Springer-Verlag, 1990, pp. 319–327. ISBN: 3-540-97196-3. URL: `http://dl.acm.org/citation.cfm?id=646753.704915`.

[13] Payments System Research Department. *Credit and Debit Card Interchange Fees Assessed to Merchants in the United States August 2015 Update.* Tech. rep. Federal Reserve Bank of Kansas City, 2015. URL: `https://www.kansascityfed.org/~/media/files/publicat/psr/dataset/us_if_august2015.pdf`.

[14] John Dryden. *Plutarch's Lives of Illustrious Men.* Ed. by Hugh Clough. The John C. Winston Co., 1908, p. 167.

[15] *EMVCo Specifications.* URL: `https://www.emvco.com/specifications.aspx`.

[16] *Ethereum Hard Fork No. 4 Has Arrived as DOS Attacks Intensify.* URL: `https://cointelegraph.com/news/ethereum-hard-fork-no-4-has-arrived-as-dos-attacks-intensify`.

[17] Ittay Eyal and Emin Gün Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable". In: *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers.* Ed. by Nicolas Christin and Reihaneh Safavi-Naini. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 436–454. ISBN: 978-3-662-45472-5. DOI: `10.1007/978-3-662-45472-5_28`. URL: `http://dx.doi.org/10.1007/978-3-662-45472-5_28`.

[18] *Federal Reserve System coin and Currency Data.* URL: `https://www.federalreserve.gov/paymentsystems/coin_data.htm`.

[19] Jim Gray. "The Transaction Concept: Virtues and Limitations (Invited Paper)". In: *Proceedings of the Seventh International Conference on Very Large Data Bases - Volume 7.* VLDB '81. Cannes, France: VLDB Endowment, 1981, pp. 144–154. URL: `http://dl.acm.org/citation.cfm?id=1286831.1286846`.

[20] *How the U.S. Could Pressure North Korea Tomorrow: Quit the $100 Bill.* URL: `http://business.time.com/2012/02/24/how-the-u-s-could-pressure-north-korea-tomorrow-quit-the-100-bill/`.

[21] Sarah Meiklejohn et al. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names". In: *Commun. ACM* 59.4 (Mar. 2016), pp. 86–93. ISSN: 0001-0782. DOI: `10.1145/2896384`. URL: `http://doi.acm.org/10.1145/2896384`.

[22] M. Möser, R. Böhme, and D. Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: *eCrime Researchers Summit (eCRS), 2013.* 2013, pp. 1–14. DOI: `10.1109/eCRS.2013.6805780`.

[23] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: *Consulted* 1 (2008), p. 2012.

[24] Tatsuaki Okamoto and Kazuo Ohta. "Universal Electronic Cash". In: *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology.* CRYPTO '91. London, UK, UK: Springer-Verlag, 1992, pp. 324–337. ISBN: 3-540-55188-3. URL: `http://dl.acm.org/citation.cfm?id=646756.705374`.

[25] Andrew Ramage and P. T. Craddock. Archaeological Exploration of Sardis, Harvard University Art Museums, in association with the British Museum Press, 2000, pp. 17–18.

[26] Research and Statistics Group Microeconomic Studies. *Quarterly Report on Household Debt and Credit*. Tech. rep. Federal Reserve Bank of New York, 2016. URL: `https://www.newyorkfed.org/medialibrary/interactives/householdcredit/data/pdf/HHDC_2016Q1.pdf`.

[27] Dorit Ron and Adi Shamir. "How Did Dread Pirate Roberts Acquire and Protect his Bitcoin Wealth?" In: *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers*. Ed. by Rainer Böhme et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 3–15. ISBN: 978-3-662-44774-1. DOI: `10.1007/978-3-662-44774-1_1`. URL: `http://dx.doi.org/10.1007/978-3-662-44774-1_1`.

[28] Adi Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[29] *The US Sees More Money Lost To Credit Card Fraud Than The Rest Of The World Combined*. 2014. URL: `http://www.businessinsider.com/the-us-accounts-for-over-half-of-global-payment-card-fraud-sai-2014-3`.

[30] *Verisign, Inc Quarterly Report Q3 2015*. 2015. URL: `http://files.shareholder.com/downloads/VRSN/1869027888x0xS1014473-15-73/1014473/filing.pdf`.

[31] N Eric Weiss and Rena S Miller. "The Target and Other Financial Data Breaches: Frequently Asked Questions". In: *Congressional Research Service, Prepared for Members and Committees of Congress February*. Vol. 4. 2015, p. 2015.

[32] *World Payments Report 2015*. 2016. URL: `https://www.worldpaymentsreport.com/reports/noncash`.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Ava Labs, Inc. ("Ava Labs")

Ava Labs.
1177 Avenue of the Americas, 5th Floor
New York, NY 10036

March 2, 2023

Office of Science and Technology Policy
Attn: Rachel Wallace
Eisenhower Executive Office Building
[redacted]

To whom it may concern:

Ava Labs, Inc. ("Ava Labs") appreciates the opportunity to comment on the Request for Information (the "RFI") propounded by the Office of Science and Technology Policy ("OSTP). We provide information below in response to certain requests in the RFI. We strongly believe that OSTP can play a critical role in helping the US government understand blockchain technology and tokenization and charting a productive course for both the public and private sectors.

The Avalanche public blockchain network is an internet-based distributed ledger and computing platform composed of many different and evolving components contributed by a wide variety of participants. Avalanche continues to grow and change through the efforts of its community.

I am the founder and CEO of Ava Labs, a team making it simple for both individuals and institutions to deploy high-performance blockchain applications on the Avalanche public blockchain.

Previously, I was a Professor of Computer Science at Cornell University, where my research focused on operating systems, networking, and distributed systems. During this time, I was Co-Director of the Initiative for Cryptocurrencies and Smart Contracts (IC3), which aims to move blockchain-based applications from whiteboards and proofs-of-concept to tomorrow's fast and reliable financial systems.

In 2003, I pioneered the first currency that used Proof-of-Work (PoW) to mint coins, called Karma [1]. In 2013, I published research on selfish mining in what has become the one of the most-cited research papers in blockchains and digital assets after the Bitcoin whitepaper [2]. I have characterized the scale and centralization of existing cryptocurrencies [3], as well as proposed leading protocols to improve on-chain and off-chain scaling [4].

In 2018, I led a group of researchers at Cornell as we discovered, validated, and introduced the Avalanche family of consensus protocols to the field of distributed systems [5]. Avalanche is the first novel consensus protocol since Nakamoto Consensus in 2008, and just the third ever. These protocols are now the engine enabling the Avalanche public blockchain to surpass finality, scalability, and security thresholds previously considered unachievable.

1. *KARMA : A Secure Economic Framework for Peer-to-Peer Resource Sharing* *https://www.cs.cornell.edu/people/egs/papers/karma.pdf*
2. *Majority is not Enough: Bitcoin Mining is Vulnerable* *https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf*
3. *Decentralization in Bitcoin and Ethereum Networks* *https://arxiv.org/abs/1801.03998*
4. *Bitcoin-NG: A Scalable Blockchain Protocol* *https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf*
5. *Avalanche: Scalable and Probabilistic Leaderless BFT Consensus through Metastability* *https://assets.website-files.com/5d80307810123f5ffbb34d6e/6009805681b416f34dcae012_Avalanche%20Consensus%20Whitepaper.pdf*

We now turn to responses to certain requests in the RFI.

Request 1: *Goals, sectors, or applications that could be improved with digital assets and related technologies.*

a. *Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered.*

Response: Blockchains create new and improved infrastructure for the entire internet by solving several key problems in computer science: (a) how to have a distributed group of computers operated by unaffiliated parties agree on a common dataset, (b) how to create unique digital representations of assets, items and things, whether they are natively digital or not, (c) how to establish ownership of those digitally unique things, and (d) how to transfer ownership of those digitally unique things.

Tokenization is the process of creating these digitally unique representations of assets, items and things on a blockchain. Think of a token as the piece of paper that memorializes the bundle of rights created by the digitally unique representation. A token can be a digital representation of anything, not just so-called cryptocurrencies. The possibilities created by this ability to create digitally unique representations are as endless as the possibilities created by a blank sheet of paper.

This link discusses tokenization and provides a sensible classification system for tokens.

In the first decade of public blockchains, we saw promise and potential outpace the technical foundations. Now, entering the second decade of blockchains and thanks to breakthroughs in the core consensus algorithms powering these systems, the technical foundation is now mature.

Blockchains are empowering reliable and secure applications at global scale, supporting billions of dollars of asset movement daily without the environmental toll found in early blockchain systems.

More information about Avalanche consensus, the mechanism by which validator nodes on Avalanche blockchains agree on a common dataset is available here.

Whereas traditional assets and applications are confined to siloed databases, new programmable assets and applications – such as those found on blockchains – are operating on transparent, interoperable networks. In these systems, all functions of an application are encoded in logic that puts individuals in control, rather than under the control of a central authority.

This video has a fuller discussion of the points mentioned above.

The technology has also reached the point where compliance can be encoded in the system's logic, ensuring that no participant can go astray of what is allowed by relevant conventions, rules or regulations (including, say, satisfying compliance mandates across multiple agencies or authorities and differentiated by jurisdiction). This extends to implementing restrictions on transfers, investor count, flowback, KYC/AML, OFAC accreditation, and more.

Beyond the positive impact blockchain is already making in financial use cases like asset management, cross-border remittances, and payments there is a host of consumer-forward use cases that can improve the security and integrity of industries like supply chain management, insurance and underwriting, social media, healthcare data, and public record infrastructure.

For example, Deloitte is accelerating disaster recovery by using the Avalanche blockchain to help state and local governments easily demonstrate their eligibility for federal emergency funding. Whereas the audit of FEMA relief for Hurricane Katrina took almost a decade to complete - with future relief recorded on blockchain, audits can be more prompt, efficient, and accurate.

The Lemonade Foundation is provisioning insurance to thousands of subsistence farmers in Kenya who are most at risk of climate change-driven disasters using the Avalanche blockchain. Before blockchain, the costs of insuring small farmers where premiums are less than $10 a year was not feasible.

Subnetworks ("subnets") are a key driver for this customization. Subnets are entirely separate chains of the Avalanche blockchain consisting of validators who reach consensus for the fully customizable blockchain. These subnets can house just one application all the way up to a full-fledged virtual machine. This is effectively running a separate blockchain within the Avalanche network ecosystem.

These subnets allow for specialized applications to run on Avalanche blockchain technology, with the flexibility to be as open or permissioned as the creator desires. These specialized applications can do anything a smart contract can do, including tokenization of any asset, item or thing, with the benefit of writing directly to a blockchain. It also allows the creators to include custom requirements in order to participate or use the subnet's application - including but not limited to hardware requirements, completion of KYC, holding of a specified number of tokens, and any other features the launch team believes are necessary or appropriate. Subnets also allow the original Avalanche network to continue to scale while keeping the network from becoming congested. Any application running on its own Avalanche blockchain subnet is able to avoid bottlenecks caused by heightened activity from other applications and activities elsewhere on the network. Since Avalanche is able to scale infinitely, even if the Avalanche network gained billions of users - subnets would be able to handle the load.

Subnets are described in more detail in various places in the Avalanche white paper, available here.

Request 5: *Opportunities to advance responsible innovation in the broader digital assets ecosystem.*

b. Information about opportunities for the United States to advance responsible innovation in the broader digital assets ecosystem, in areas that are adjacent to R&D.

c. This may include programs that could support increased education and workforce training related to digital assets, standards setting efforts that could help advance democratic values in the use and governance of digital assets, and supply chain opportunities to maintain access to the necessary hardware for emerging digital assets.

Response: When considering innovation and regulation, the starting point should focus on the fact that tokens are not one undifferentiated asset class. For instance, Bitcoin is nothing like NBA Top Shots. It is critical to understand the technology and the uniqueness of different digital assets and classify tokens sensibly, based on its primary functions and features.

Regulations and policies should take an approach consistent with existing methodologies, where the nature of the asset and the risks associated with that asset type are the starting point for crafting appropriate legislation. In the same vein, intermediaries should be regulated based on their activities and associated risks, but there are various types of activities and actors who are not subject to regulation in the Web 2 world and should not be subject to regulation simply because they engage in activities in the Web 3 world because they are simply software creators or publishers and other types of technology providers not intermediating transactions, providing custody of tokens or functioning as a fiduciary. This includes personal wallets, miners and validators, providers of APIs and block explorers, various types of software providers, and anything that is decentralized (defined as no single point of failure, no single source of truth and no authority responsible for or capable of changing data).

There is a balance to be struck between cohesive policies and alignment that regulations cannot be "one size fits all." As such, regulation should be tailored to each use-case in blockchain, wherein a particular sector should meet the requirements set out for that sector. It is also critical that the regulatory structures acknowledge the non-financial uses of blockchain technology and avoid regulating them as if they were financial instruments.

The European Union (EU) and its member nations have adopted this type of approach with the Markets in Crypto-Assets Regulation, which will pass shortly and begin being implemented next year. The recognition of different asset types, the recognition that not all tokens are financial instruments, and the technology neutral approach evidenced by the fact that regulated financial instruments on blockchain continue to be regulated as financial instruments and not crypto-assets, evidences an attention to the nature of each crypto-asset that is missing in the US and many other jurisdictions.

Our Owl Explain initiative provides various resources on these topics, including the Tree of Web3 Wisdom, which is a list of principles for policy makers. You can find the website here.

Request 6: *Other information that should inform the R&D Agenda.*

d. *Information about any other topic, not covered above, that respondents believe is important to inform the development of the National Digital Assets R&D Agenda.*

Response: We note that the European Union has three programs that may be of interest to OSTP in formulating an R&D Agenda:

1. The European Blockchain Services Infrastructure is designing and deploying a blockchain that European governments can use to deliver services to their citizens. A link to information can be found here.
2. Europe's DLT Pilot is exploring the use of blockchain for the clearance and settlement of transactions in financial instruments. A link to information can be found here.
3. Europe's Blockchain Sandbox Regime allows blockchain-based businesses to participate in special programs in conjunction with regulators to allow for experimentation with new types of services for consumers of all types. A link to information can be found here.

* * *

Blockchain and tokenization are revolutionizing the infrastructure of the internet. We are still at the early stages of that revolution. With sensible regulation that recognizes the nature of the asset, the nature of the activities, and the associated risks, the US can be a leader in these areas as it is in so many other areas of technology. Moreover, with policies and programs that incentivize good actors and appropriate R&D, that leadership role will span across the breadth of the internet. Ava Labs will continue to work to support these twin goals. The Avalanche network with its cutting-edge technology will facilitate improved infrastructure for the internet.

Respectfully submitted,

[redacted]

Dr. Emin Gün Sirer

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Bain Capital Crypto

Bain Capital Crypto baincapitalcrypto.com

[redacted]

March 3, 2023

Ms. Rachel Wallace
Deputy General Counsel
White House Office of Science and Technology Policy (OSTP)
[redacted]

Submitted via email to DARD-FTAC-RFI@nitrd.gov

Re: Request for Information: Digital Assets Research and Development Agenda

Dear Ms. Wallace:

Bain Capital Crypto, L.P.[1] ("Bain Capital Crypto") appreciates the opportunity to respond to the Office of Science and Technology Policy request for information[2] ("RFI") on "National Digital Assets Research and Development Agenda." We are a venture capital fund adviser launched in 2021 whose managed funds invest exclusively in the crypto ecosystem. Our team of investors, researchers, and regulatory experts support projects building blockchain-based infrastructure and applications from the seed through growth stage with a highly technical and collaborative approach. We believe that crypto represents one of the most interesting and important technological developments since the advent of the Internet and that a sensible regulatory framework is needed to realize its promise of a more open, community-driven, resilient, and decentralized economy.

Bain Capital Crypto's team includes researchers who conduct cutting-edge work on digital assets and blockchain-based technology and we work collaboratively with research partners and our portfolio companies to support the innovative products and services they are building based on such technology. Our research team is headed by Guillermo Angeris,[3] who completed his PhD in electrical engineering at Stanford University, where he focused on applications of optimization in applied physics. Guillermo has also written some of the foundational, highly-cited literature in the space of automated market makers, commonly used in decentralized exchanges. Theo Diamandis[4] is a research partner at the fund and a 4th year PhD student at MIT, where he works

---

[1] See Bain Capital Crypto, www.baincapitalcrypto.com.
[2] Digital Assets Research & Development Agenda, Request for Information, 88 Fed. Reg. 5043 (Jan. 25, 2023), https://www.regulations.gov/document/OSTP-2023-0001-0001.
[3] See Guillermo Angeris, Head of Research, Bain Capital Crypto, https://scholar.google.com/citations?user=6vXh2O4AAAAJ&hl=en&oi=ao.
[4] See Theo Diamandis, Research Partner, Bain Capital Crypto, https://scholar.google.com/citations?hl=en&user=91muemoAAAAJ&view_op=list_works&sortby=pubdate.

on algorithms for mathematical optimization. Theo has written a number of papers on topics like how to allocate scarce computational resources of nodes and validators, along with work on algorithms for optimal trade execution across automated market makers.

Below we share some of the topics that either our research team is working on in a general capacity, or that our portfolio companies are exploring, often in collaboration with our team. Our submission broadly corresponds to topic nos. 1, 4 and 6, as enumerated in the RFI. We believe these are just some of the areas that merit further research and investment by both the public and private sectors.

Zero Knowledge Protocols

Zero knowledge proofs ("ZKPs") provide cryptographic proofs that a party executed a certain computation correctly.[5] The "zero knowledge" part means that the verifying party does not need to know all of the inputs to verify the correctness of the computation. ZKPs usually have the property that verifying the proof is much faster than performing the computation in the first place. Within the digital assets space, ZKPs are being used to provide simple certificates that can be easily verified by all participants. This is in comparison to many current blockchains, such as Ethereum, where all parties need to re-execute every transaction ever included in the chain to verify the chain's correctness. Using ZKPs, parties only need to check proofs, which is far less expensive than re-computing the result of each transaction.

ZKPs have many other potentially interesting applications. For example, ZKPs can enable verification of machine learning models' output,[6] certifying that the predictions given are indeed a result of a particular machine learning model. They may help to combat misinformation, including "deepfakes," by guaranteeing the provenance of edited or artificially-generated images, which will become increasingly important as artificially-generated content becomes increasingly prevalent.[7] Finally, ZKPs may present innovative solutions to identity verification; for example, someone can prove they have a particular credit score without revealing their history, or that they are eligible to open an account on a financial platform without handing over sensitive personal information that gets stored in multiple databases and becomes a target for hackers and identity thieves. This application of ZKPs could present an alternative form of compliance that is more privacy-preserving, cost-effective, secure, and portable than existing KYC and AML regulatory regimes, something we discussed at greater length in a previous comment letter to the U.S. Department of the Treasury.[8] Several of our portfolio companies are also working on developing hardware accelerators for ZKPs, which will be needed as the complexity of ZK applications increases, and software for ZKPs, making it easier for developers to write and

---

[5] Boaz Barak, *Zero knowledge proofs*, An Intensive Introduction to Cryptography, https://intensecrypto.org/public/index.html.
[6] Daniel Kang, Tatsunori Hashimoto, Ion Stoica & Yi Sun, *Scaling up Trustless DNN Inference with Zero-Knowledge Proofs*, arXiv (Oct. 17, 2022), https://arxiv.org/abs/2210.08674.
[7] Daniel Kang, Tatsunori Hashimoto, Ion Stoica & Yi Sun, *ZK-IMG: Attested Images via Zero-Knowledge Proofs to Fight Disinformation*, arXiv (last revised on Nov. 10, 2022), https://arxiv.org/abs/2211.04775.
[8] Bain Capital Crypto Comment Letter re: Ensuring Responsible Development of Digital Assets (Nov. 3, 2022), https://www.regulations.gov/comment/TREAS-DO-2022-0018-0073.

use ZK technology. Additionally, we are working on better mathematical abstractions to accelerate further development of ZK protocols and constructions.

Optimal Resource Allocation

Blockchains, at their core, are shared compute platforms.[9] They must allocate a finite amount of non-fungible resources (such as computation, bandwidth, or storage) among competing parties, who are in contention for these resources. Our research has defined a general framework for this 'resource allocation' problem, which we believe has applications not only for blockchains but also for more general problems of this form.[10] For example, this mechanism may be applied to cloud computing, where a similar problem (contention over limited resources) happens over short time scales as servers are dynamically launched and spun down, in reaction to demand for compute. Similar mechanisms may also be applied to other markets such as those for distributed energy generation and consumption, among others.

Derivatives Without Counterparty Risk

Constant function market makers (CFMMs) are a novel type of automated market maker pioneered in the digital assets space.[11] CFMMs are the primary mechanism used for decentralized exchanges—they are, by far, the dominant source of on-chain trading volume and liquidity. Some of our published research shows that these CFMMs can serve as reliable mechanisms for price discovery, even when the traded tokens have relatively little liquidity.[12] Our research[13] has also shown that CFMMs can replicate a large class of financial derivatives without counterparty risk.[14] This property has the potential to decrease systemic risk and improve capital efficiency in the modern financial ecosystem, leading to more resilient financial markets. In fact, their robustness comes with strong theoretical guarantees.[15] We, and a number of our portfolio companies, continue to research the implications of these properties.

---

[9] Tim Roughgarden, *Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559*, arXiv (Dec. 1, 2020), https://arxiv.org/abs/2012.00854.
[10] Theo Diamandis, Alex Evans, Tarun Chitra & Guillermo Angeris, *Dynamic Pricing for Non-fungible Resources: Designing Multidimensional Blockchain Fee Markets*, arXiv (last revised on Nov. 3, 2022), https://arxiv.org/abs/2208.07919.
[11] Guillermo Angeris and Tarun Chitra, *Improved Price Oracles: Constant Function Market Makers*, at 80-91, In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, Association for Computing Machinery (Oct. 26, 2020), https://doi.org/10.1145/3419614.3423251.
[12] *Id.*
[13] Guillermo Angeris, Alex Evans & Tarun Chitra, *Replicating Market Makers*, arXiv (Mar. 26, 2022), https://arxiv.org/abs/2103.14769.
[14] Guillermo Angeris, Alex Evans & Tarun Chitra, *Replicating Monotonic Payoffs Without Oracles*, arXiv (Nov. 26, 2021), https://arxiv.org/abs/2111.13740.
[15] Guillermo Angeris, Akshay Agrawal, Alex Evans, Tarun Chitra & Stephen Boyd, *Constant Function Market Makers: Multi-Asset Trades via Convex Optimization*, arXiv (July 26, 2021), https://arxiv.org/abs/2107.12484.

Improved Exchange Design

Blockchains have facilitated experimentation with novel exchange designs for a variety of assets, opening up a dramatically larger design space. Since certain mechanisms are more or less efficient for certain classes of assets, a natural question is then, "what properties could we want out of an exchange?". Our research in exchange design is exploring a number of additional desiderata in the exchange space.[16] Others, including Ramseyer et al. are also actively exploring this design space.[17] Some examples include exchanges where large institutions may buy and sell assets without fear of being front-run by high-frequency traders, mechanisms for trading baskets of assets simultaneously (also explored by Budish et al.[18]), and mechanisms that enable users to express their preferences on semi-fungible goods. We believe these exchange designs can improve the efficiency of commodity markets, such as metals exchanges. We have additional work on optimal trade execution, where a party can request a trade between two assets; any other party can then execute the trade and provide an easily-checkable certificate that the trade was performed optimally.[19] We have also been exploring batched exchanges[20] and auctions as a means to provide better execution for end users.

We appreciate the opportunity to provide information on some of the important research areas in the blockchain and digital assets space and are encouraged that the public sector is taking an interest in further exploring this technology and its potential use cases, like many other governments around the world are already doing. The United States has been at the forefront of this technology since its earliest days, and U.S.-based companies have been category-defining in everything from blockchain protocols to decentralized finance; from NFTs to stablecoins. The U.S. must capitalize on its first-mover advantage by supporting both private and public sector investment in this technology. We would be happy to provide more detailed information on any

---

[16] *Supra* note 15, *Constant Function Market Makers: Multi-Asset Trades via Convex Optimization*; *Supra* note 11, *Improved Price Oracles*; Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, Charlie Noyes & Tarun Chitra, *An analysis of Uniswap markets*, arXiv (last revised on Feb. 9, 2021), https://arxiv.org/abs/1911.03380; Alex Evans, Guillermo Angeris & Tarun Chitra, *Optimal Fees for Geometric Mean Market Makers*, arXiv (Apr. 1, 2021), https://arxiv.org/abs/2104.00446; Guillermo Angeris, Alex Evans & Tarun Chitra, *When does the tail wag the dog? Curvature and market making*, arXiv (Dec. 15, 2020), https://arxiv.org/abs/2012.08040.

[17] Geoffrey Ramseyer, Mohak Goyal, Ashish Goel & David Mazières, *Batch Exchanges with Constant Function Market Makers: Axioms, Equilibria, and Computation*, arXiv (last revised on Jan. 31, 2023), https://arxiv.org/abs/2210.04929.

[18] Eric B. Budish, Peter Cramton, Albert S. Kyle & Jeongmin Lee, *Flow Trading*, University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2022-82 (June 23, 2022), https://ssrn.com/abstract=4145013 or http://dx.doi.org/10.2139/ssrn.4145013.

[19] Guillermo Angeris, Alex Evans, Tarun Chitra & Stephen Boyd, *Optimal Routing for Constant Function Market Makers*, at 115–128, In Proceedings of the 23rd ACM Conference on Economics and Computation, Association for Computing Machinery (July 13, 2022), https://doi.org/10.1145/3490486.3538336.

[20] Nicholas A. G Johnson, Theo Diamandis, Alex Evans, Henry de Valence & Guillermo Angeris, *Concave Pro-rata Games*, arXiv (Feb. 4, 2023), https://arxiv.org/abs/2302.02126.

of the items listed above. In particular, our research team can be reached at [redacted] or [redacted]

Sincerely,

[redacted]

Guillermo Angeris
Head of Research

[redacted]

Theo Diamandis
Research Partner

[redacted]

Tuongvy Le
Partner and Head of Regulatory & Policy

Bain Capital Crypto

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Bankless Consulting

Bankless Consulting Response to The White House Office of Science and Technology Policy Request for Information on Digital Assets Research and Development

March 2, 2023

For additional information about this response, please contact:

Chuck Cummings, Bankless Consulting Co-Founder
[redacted]

Introduction and Overarching Recommendations

14 years after the introduction of Bitcoin, digital assets are on the cusp of moving from a niche market to the centerpiece of the Fourth Industrial Revolution. Many jurisdictions, including such economic powers as the European Union, Hong Kong and the United Arab Emirates, are embracing digital assets and creating comprehensive regulatory frameworks that seek to balance innovation with consumer and investor protections. The U.S must similarly engage with this new opportunity to retain its status as a global leader and magnet for economic and intellectual capital.

Responsible American innovation in digital assets requires the federal government to provide clear legal and regulatory guidance. To help American society realize the potential of digital assets, Bankless Consulting recommends three overarching research and development topics for this working group:

1. Creating more efficient capital markets.
2. Increasing Americans' wealth through disintermediation.
3. Incentivizing innovation that benefits the American people.

As we recommend to our clients, we are sure the federal government can approach digital assets with an aspirational view of the opportunities, while being vigilant of the risks associated with increased adoption of digital assets.

Response to RFI Topics #1, #4, and #5

Digital Assets Can Help Ordinary Citizens and Enhance American Competitiveness

Digital assets:

- Enable the disintermediation of rent-seeking actors who take advantage of consumers
- Improve the efficiency and transparency of capital markets
- Enhance overall well-being by incentivizing desirable behaviors
- Preserve and enhance American competitiveness and economic dynamism by lowering barriers to innovation.

Research should be directed to understanding how and in which industries disintermediation can benefit ordinary citizens

One of the most valuable aspects of blockchain technology is the capability for trustless and transparent data storage and exchange, which removes the need for oversight by intermediaries. These third parties are rent-seeking by nature, and the cost of their involvement is typically borne directly by ordinary consumers.[1] Research is needed to discover scenarios where direct peer-to-peer transfers of tokenized assets could eliminate this rent-extracting transactional layer, thereby directly benefiting customers through a reduction in costs. Examples of industries ripe for disintermediation are real estate, insurance, retail finance, and ticketing. There are many more consumer-facing service industries where cost savings produced through the use of blockchain could instead reside in Americans' bank accounts.

Research is needed to understand how blockchain-based marketplaces can augment traditional capital markets

Tokenized securities and blockchain technology represent the future of digitized capital markets because they are more capital efficient and more transparent.[2]

Blockchain-based marketplaces are more capital efficient because they allow for sizable volumes of assets to be housed and transacted on chain, with significantly lower overhead (fewer employees, fewer offices, etc.) than legacy marketplaces.

Furthermore, digital asset marketplaces are inherently transparent because the underlying technology is a decentralized public ledger, a database of transactions viewable by all. Recent frauds in the digital asset space (FTX, etc.) are the result of private actors taking custody of investors' assets and obscuring malfeasance. These are akin to traditional financial frauds perpetrated by bad actors, and should not be conflated with activity in truly decentralized blockchain-based marketplaces. In such markets, investors can obtain information on digital asset transactions by directly querying the blockchain — a level of transparency and scrutiny which serves to reduce the likelihood that fraudulent actions can occur unnoticed.

Research is needed to understand how best to use digital assets to promote desirable behaviors and outcomes in citizen populations

Research in the field of behavioral economics suggests that well-being (including better educational, financial, and health outcomes) can be generated through "choice architecture", i.e. thoughtful implementation of incentives and disincentives.[3]

---

[1] One study found that rent-seeking reduced US incomes by 45%. Leeson, Peter T. (2009). *The Invisible Hook: The Hidden Economics of Pirates*. Princeton University Press. p. 191. ISBN 9780691150093.
[2] A recent article published by NASDAQ summarizes this view: https://www.nasdaq.com/articles/tokenization%3A-the-fabric-of-our-financial-future
[3] Thaler, Richard H. and Sunstein, Cass R. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press. ISBN 978-0-14-311526-7.

Digital assets are a powerful mechanism for implementing choice architecture. Research is needed to examine how public and private sector actors can leverage digital assets to provide incentives for citizens to live longer, healthier, and better lives.

A few examples are illustrative:

1. Many Americans are not saving enough to fund their retirement. Digital assets can be used not just to reward individuals for enrolling in savings plans, but also to enact beneficial savings mechanisms, such as automatic deposit of a person's assets into savings accounts at regular intervals.
2. Many citizens have struggled to upgrade their vocational skills to compete in the new economy. One solution could be issuing digital education credits — effectively vouchers — which can be redeemed at accredited educational institutions for skills-based training.
3. Digital assets could be issued to people who donate blood or organs, or who participate in anti-smoking programs, thus reducing the strain on the healthcare system, tracking the success of health promotion initiatives, and improving health outcomes across the nation.

Research is needed to determine how different agencies across the U.S. government, as well as private-sector actors, can employ digital assets to incentivize individuals and organizations to choose beneficial behavior.

Research is needed to determine how to streamline processes for compliant capital formation

The U.S. economy owes much of its competitiveness to the venture capital industry, which funds promising new ideas by investing in emerging industries and companies. This has enhanced capital formation across many industries, including blockchain itself. However, the traditional venture capital model is currently limited to a small number of accredited investors, largely located in the wealthiest metropolitan centers, who are therefore unable to effectively reach entrepreneurs in the majority of communities across the U.S.

Digital assets offer new opportunities for funding — and crowdfunding — ideas which might not otherwise make it to market. Imagine an entrepreneur in Kansas who, unable to afford to travel to Silicon Valley to meet with investors, decides instead to conduct — in a compliant manner — a small offering of tokenized shares in their company on a regulated blockchain-based platform. This efficient access to capital enables them to raise sufficient capital to build a working version of their product.

Digital assets represent the future of crowdfunding and promise to unlock a new era of U.S. dynamism, but only if a thoughtful, comprehensive regulatory framework provides certainty to founders who need clarity to embark on risky ventures. In the interest of preserving and enhancing national competitiveness, research is required to understand how digital assets can reduce barriers to capital formation and thereby benefit startup founders, investors, and consumers. Particular attention should be paid to ways in which digital assets provide opportunities to streamline startup fundraising, for example, by reducing the cost of hiring intermediaries such as lawyers and accountants.

Digital assets should not be viewed as strictly financial assets, but rather as highly versatile and adaptable tools to promote a more dynamic and healthy economy, with the overarching goal of preserving and enhancing American competitiveness.

Responsive to RFI Topics #1, #4, and #5

Improving Capital Efficiency By Bringing Real-World Assets On Chain

Blockchain technology enables the fast, secure, and inexpensive exchange of digital assets. Pioneers in the digital asset space are beginning to bring traditional asset classes on chain, including equities, bonds, real estate, invoices, car titles, and royalty payments. Bringing traditional assets on chain can increase capital efficiency and lift the American economy, but research is needed into methods and standards for the integration of real-world assets with blockchain.

Creating frameworks for bringing real-world assets on chain can increase capital efficiency

Capital efficiency drives resource allocation. Taking real estate as an example, there are currently trillions of dollars locked in this asset class that cannot easily be sold or borrowed against. Many of these investments are illiquid, sometimes for a decade or more.

Under current regulations controlling real estate syndications, investors are unable to sell their stake in a project without the entire ownership of the company changing hands or an internal swap amongst investors. Tokenized ownership of real estate positions enables the creation of marketplaces where investors could act independently to sell their positions in these projects to both internal and external investors. This creates secondary markets for digitized real estate assets that can help drive investment into the development of manufacturing facilities, green energy production, and affordable housing.

The Tax Cuts and Jobs Act of 2017 created “opportunity zones" where various incentives were used to direct the flow of capital investment into underserved areas. Using a similar methodology in conjunction with tokenized real world asset markets could enable the creation of pools of opportunity zone assets that can attract new capital. These investment pools can be thought of as a blockchain-enabled “Real Estate Investment Trust” (REIT) where government-backed projects can be tokenized and incentivized to attract capital through an increased rate of return.

Invoice financing is another sector of the economy where the blockchain can improve capital efficiency. It is a common practice for companies to take out short-term loans on money owed to them, providing them with access to the capital needed to fulfill incoming orders, make payroll, pay rent, and otherwise continue operations. Typically, businesses have 30 - 120 days to pay for goods after delivery. To help businesses bridge the gap between order and payment, banks and other institutions lend capital against accounts receivable, often at high interest rates, especially for a small or medium size enterprise (SME). SME financing can have rates higher than 15%, while large companies can access capital at the much lower prime rate. The difference in these rates is not commensurate with default rates, as the SME industry has a default rate of less than 2% on loans of this kind.

Because of these high interest rates and low risk of default, there is an opportunity to bring these assets on chain, into the liquid world of decentralized finance. Fees collected by lenders in the tokenized real-world asset space are between 4%-10%, while borrowers can obtain capital with interest rates as low as 5%.

We recommend researching how the first debt markets of this kind are operating in conjunction with U.S. banks such as Block Tower and Hudson Valley Bank, who have partnered with MakerDAO to offer credit facilities across their mortgage and invoicing portfolios.

Research into methods and standards for tokenizing and fractionalizing real-world assets should be prioritized

Traditional companies, blockchain-based businesses, retail investors, and consumers would all benefit from research into standardizing the practice of bringing real-world asset classes on chain, including how best to fractionalize the ownership of real-world digital assets.

Once the real-world asset is on chain as a digital asset, the sale or collateralization is much cheaper and more efficient than is possible using the tools of traditional finance. However, current legal restrictions and lack of blockchain-specific regulations make the process of moving proof of ownership to a blockchain cumbersome and expensive.

Tokenizing and fractionalizing these real-world assets enables the average citizen to gain access to financial instruments that have previously been closed to non-accredited investors. Providing predictable methods for fractionalizing ownership of traditional financial assets would both democratize and create more efficient capital markets, while also providing greater liquidity to those markets.

The United States has the potential to become a world leader in digital asset ownership rights and maintain its leadership as the global financial hub. To ensure the United States retains its position as the world's dominant economy, research into the legalities of company formation, recognition of digital ownership rights, and new ways to create or facilitate the onboarding of current title mechanisms onto the blockchain is needed.

The potential for bringing real world assets on chain is yet to be realized. With experimentation underway in a variety of fields, current use cases include:

- Title ownership and transfers (e.g. houses, cars, boats)
- Real estate fractionalized ownership
- Real estate secondary markets
- Treasury bills
- Bonds
- Equities (synthetic assets)
- Debt financing (collateralized debt positions)
- Royalty payments
- Real estate investment trusts (entire portfolios)
- Art
- Commodities
- Intellectual property rights

The opportunity afforded by bringing real-world assets on chain is nascent and unprecedented. By focusing R&D money into standards for fractionalized ownership of tokenized assets and best practice for bringing real-world assets on chain, the government can help accelerate innovation in traditional finance and the broader digital asset ecosystem.

Responsive to RFI Topics #1, #2, #4, and #5

Creating Opportunities For DAOs to Drive Social Impact and Economic Innovation

R&D should be prioritized for cooperative internet-based entities, commonly called DAOs

Thousands of Americans are using the internet to coordinate actions in novel ways, many of which are administered by ownership of digital assets. Early adopters of blockchain technology see the possibilities for social good resulting from these innovations in human coordination. DAOs are a paradigm shift and this burgeoning pocket of our economy is poorly defined and largely unregulated. Through R&D, the federal government can bring legitimacy to this organizational structure and unlock tremendous good for American society.

Rules and regulations for DAOs should encourage Americans to leverage the internet and digital assets in ways that most benefit American society. The established legal and regulatory frameworks for governing corporations, LLCs, 501(c)3's, and other legal entities — designed before the internet transformed America's economy and society — do not adequately govern DAOs, as they largely fail to protect founders and contributors from potential liability, nor do they provide the tax advantages of more established legal entities.

The internet is global. Public blockchain technology is decentralized and distributed globally. With R&D of internet-based entities like DAOs, the United States could explore new ways to realize the benefits of a global economy and the Fourth Industrial Revolution[4].

Continuing a trend of responsible American innovation on the internet

Digital assets, made possible by cryptography and decentralized ledger technology, have added a financial dimension to internet-based groups.The World Economic Forum defines DAOs as "entities that use blockchains, digital assets and related technologies to direct resources, coordinate activities and make decisions"[5].

---

[4] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir
[5] https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organizations_Beyond_the_Hype_2022.pdf

People are forming DAOs when doing so serves their interests better than a C corporation, B corporation, LLC, or 501(c)3 nonprofit organization. There are many reasons why Americans elect to form a DAO rather than make use of an existing U.S. legal entity structure. DAOs are:

- **Digital native**: For people who have grown up with the internet, it feels as natural to form an organization on the internet as one in a state-based legal jurisdiction.
- **Efficient**: DAOs remove the friction of establishing a state-based legal entity. They leverage the internet to promulgate information quickly. As a result, people with a common mission can begin pooling their resources into a DAO in a matter of minutes.
- **International**: People in any country with an open internet connection can contribute to a DAO. U.S.-based companies will find it increasingly difficult to compete with the broad expertise harnessed by DAOs with contributors domiciled in countries all over the world.
- **Transparent**: All actions involving digital assets on a public blockchain can be independently verified.

By providing clear rules and regulations relating to DAOs, the U.S. can continue to lead the world in responsible technological innovation.

Goals, sectors, and applications that DAOs can improve

Many DAO leaders are advancing a cause that is not commercial, providing us with early glimpses of how this technology can be used for social good. Current and potential examples of DAOs working to make a social impact include:

- **Immediate mission**: A DAO was created to provide direct aid in the form of digital assets to the Ukrainian government as the Russian invasion began.
- **Long-term mission:** Endowments and trusts can be composed of digital assets and be digitally governed by a rotating cadre of contributors to the DAO's treasury.
- **Public goods:** A group of citizens can pool digital assets to purchase a first edition United States Constitution in order to guarantee public access to the document forever.
- **Intellectual property:** A group of teachers in a DAO can share curricula and other educational resources with each other and distribute any revenue generated from their collective value creation.
- **Professional guild**: A group of software engineers formed a DAO to govern the collective value of their professional network and expertise.

- **Historic preservation:** A historical society's members can contribute digital assets to a DAO for the purpose of renovating a historical building which has fallen out of line with municipal code and is at risk of being closed or demolished.
- **Cultural property:** The fans of a sports team can combine their digital assets to buy the team so that the owner doesn't sell it to a different city.
- **Land conservation:** A group of people can pool their digital assets to conserve wilderness and protect it from commercial development.
- **Storytelling:** Filmmakers are building a DAO to crowdsource information from historians, journalists, and regular citizens to fact-check a television series about Ukraine in the 21st century.
- **Sourcing truth:** A doctor is building a DAO to incentivize the crowdsourcing of truthful information in critical industries such as healthcare and public policy.
- **Research:** A biotech DAO is coordinating scientists outside of biotech hotspots like Boston or Paris to double the number of life-saving therapeutics available to patients.
- **Dissemination:** A community of organizational scientists, strategists, and researchers are building the world's first decentralized, community-reviewed publication for the social sciences.
- **Data property rights:** A social media app is forming a DAO so that app users can collectively govern what the company can do with their data.
- **Political engagement**: Advocates for a cause or a candidate can pool their digital assets to influence electoral politics.
- **Global philanthropy**: A group of American donors can use a DAO to decide how to disburse funding to grantees all over the world.

Goals, sectors, or applications where DAOs introduce risks or harms

Americans are choosing to form and contribute to DAOs even though they are not formally recognized by most jurisdictions in the United States. DAOs represent a new form of social and economic organization. However, the legal status of DAOs is currently unclear, and DAO participants are often exposed to potential personal liability.

Even in jurisdictions where DAOs have limited recognition, such as Wyoming, the law often imposes serious constraints and has a chilling effect on social experimentation. Because they operate in a legal gray area, DAO members and leaders are taking a number of risks, regulatory and otherwise. DAOs fail to protect Americans contributing to them in a number of ways that the federal government should help address. Here are a few examples. Again, this list is not comprehensive.

- **Not-for-profit status**: How can DAOs organized around charitable causes obtain tax-exempt status and be able to issue receipts to donors?
- **Fiduciary duties**: What duties do DAO managers or administrative persons owe to members of the DAO?
- **Deposit insurance**: What protections need to exist for people contributing their digital assets to a DAO?
- **Employment law:** What differentiates employees, contractors, and other types of contributors to a DAO?
- **Workplace protections**: Where do DAO contributors turn if their rights are violated?
- **Intellectual property**: When does a DAO own the IP and when do contributors own the IP?
- **Paying taxes:** What taxes do DAOs owe? What taxes do their contributors owe?
- **International law**: What are the implications of having non-US members contribute to DAOs?
- **Custody of property**: What rights or claims do DAO members have over the digital assets under custody in the DAO?
- **Contracts**: When are blockchain-based smart contracts legally binding? How can DAOs form contracts with U.S.-based legal entities?
- **Arbitration and dispute resolution**: Is self-imposed arbitration of conflicts between DAO members legally valid? What minimum standards should apply to such arbitration proceedings?

Many of the world's largest economies are beginning to create comprehensive regulatory frameworks for these internet-native organizations. To compete in the burgeoning internet-based marketplace for global talent, the United States must provide better clarity for people working in internet-based organizations.

Appendix

About Bankless Consulting

Founded in 2022, Bankless Consulting is a digital assets technology consultancy.

Our consultants are passionate about using blockchain-enabled technology to help small businesses, social impact organizations, and individuals. In our first year, we helped launch many mission-driven companies and projects. We have also advised several businesses and nonprofits on how to use web3 to gain a competitive advantage.

Our vision is a future where we enable businesses and consumers to embrace digital assets, while encouraging our clients to engage in this economic transformation with confidence, authority, and authenticity.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Banking Innovation Through Technology (BITT)

[redacted]
Bitt: Banking Innovation Through Technology

Submitted via email to: DARD-FTAC-RFI@nitrd.gov

March 3rd, 2023,

Office of Science and Technology Policy
Executive Office of the President
[redacted]

Comments on Request for Information; Digital Assets Research and Development

We at Bitt thank the Office of Science and Technology Policy ("OSTP") for the opportunity to comment and help identify priorities for a U.S. national digital assets research and development ("R&D") agenda.

Our perspective on digital assets is informed by Bitt's experience in designing, developing, and deploying digital currency solutions in the stablecoin and central bank digital currency ("CBDC") markets. We are the supplier to the world's largest democratic CBDC offering, the e-Naira, in Nigeria. We have deployed CBDC and stablecoin platforms on our Digital Currency Management System ("DCMS") in Ukraine, Belize, and the Eastern Caribbean, and are currently engaged in negotiations to deploy with multiple central banks and monetary authorities in Europe, Africa, central Asia, and the Pacific Far East. Our team provides expert advisory input and participation in several global standards-setting groups, including the OECD, WEF, IMF, ITU, and World Bank.

In terms of the digital assets R&D agenda, we applaud the priority and urgency of the policy goals of E.O. 14067, and fully support the digital asset design parameters set forth in OSTP's Technical Evaluation for a U.S. CBDC. As a digital asset pioneer, we designed our DCMS from the ground up to enable personal privacy, security, and financial inclusion: these three holistic values are built into our company mandate.

Beyond the engineering design challenge, we have worked closely with our central bank clients to roll-out their digital asset platforms in the real world in ways that embody these paramount democratic values of privacy, security, and financial inclusion.

Sincerely,

Simon Chantry
Co-Founder and Chief Information Officer
[redacted]

James Shinn
Executive Director
[redacted]

I. Comments on *Request for Information; Digital Assets Research and Development*

From RFI: *Privacy-enhancing technologies: Privacy-enhancing technologies ("PETs") refer to a broad set of technologies that protect privacy, which are within the scope for this RFI. We are particularly interested in privacy-preserving data sharing and analytics technologies, which describes the set of techniques and approaches that enable data sharing and analysis among participating parties while maintaining disassociability and confidentiality. Such technologies include, but are not limited to, secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic data generation tools.*

Some financial institutions and individuals worry about new privacy risks associated with CBDCs, like state surveillance. However, CBDCs and stablecoins can be designed in a way that lowers the costs associated with KYC and AML compliance, both within the United States and abroad, while also protecting the privacy of the individual in a similar way other digital payments currently function. There are a variety of privacy-enhancing technologies that can protect user information, including both Personal Identifying Information ("PII") and transaction data. For example, we designed the Bitt DCMS to be a flexible and configurable platform to enable privacy-preserving functions at the transaction network and architecture levels.

At the architecture level, role-based access controls are implemented and configured to the requirements of the system operator (central bank for CBDC; regulated financial institution for a stablecoin), ensuring that only specified users with adequate permissions can access the underlying transaction network (in the case of a private transaction network or ledger). In terms of privacy considerations, several private transaction networks offer robust privacy enhancing features, ranging from true cash-like privacy, where only the two counterparties to a transaction are aware that it took place, to public ledger data availability restricted only by the architectural and governance related access controls, as mentioned above. Tiering via wallets can also be integrated to enable functionalities for different privacy needs within a possible solution.

On the cash-like privacy end of the spectrum, technologies such as Chaumian blind signatures, and RSA accumulators, zero knowledge proofs, and homomorphic encryption offer highly effective privacy preserving techniques that protect the identity of the counterparties transacting, as well as the amounts transacted. There are both DLT-based and non DLT-based solutions that leverage the aforementioned privacy enhancing technologies that could be used to mint, issue, and circulate CBDCs and stablecoins, with configurable degrees of disclosure, leading to robust privacy enhancement.

Public Transaction Network Considerations:

If a public ledger with inherent privacy preserving functions is being utilized (such as Monero or ZCash), then transaction data is protected at the transaction network level. If a public ledger without inherent privacy preserving functions is being utilized (such as Bitcoin or Ethereum), then transaction data can be protected by using "layer 2" solutions such as lightning network or Nightfall on Polygon (or zk-rollup solution), respectively.

Other transaction networks offer plain-text records of account balances and state changes as users transact in CBDCs, placing significant importance on the access control features in the middleware or architectural layer between the network and applications. Transaction history can also be segregated at the network level based on the intermediaries involved in the counterparties' transactions (transaction channels on Hyperledger) or can be truncated following a set amount of time (chain-snipping on Corda and others).

KYC and Identity Considerations

In all cases, the KYC requirements for utilizing the CBDC or stablecoin solution can have a significant impact on user privacy preservation and protection. Intermediaries who store and accumulate KYC data carry significant risk for themselves and their users. Solutions exist to address this risk across many digital asset platforms, both public and private. Bitt has experimented with several digital identity solutions to enhance privacy and enable users to own their own data. The following is an overview of how verifiable credentials could be implemented with the DCMS for a CBDC or stablecoin deployment. This added functionality would allow central banks to manage inflation through the accurate and reliable economic profiling of transactions which require clean, authentic data and metadata collection at point of capture, rather than depending on inaccurate and outdated private data or under-sampled and inaccurate surveys.

Even though current legacy financial infrastructure allows for the gathering of metadata via the wisdom of the crowds, private data brokers, and user-generated content like social media: these methods have succeeded in creating new modes of business and have failed in creating reliable, long-term authentic data streams that can be used for public and monetary policy. Legacy infrastructure in effect has succeeded in privatizing and siloing metadata into the hands of private corporations like PayPal, Visa, Mastercard, Venmo, Stripe, and the like. Data streams captured by these corporations become strategic assets and thus these corporations are incentivized to hoard the data and keep it from the public or public policy makers; leaving policy makers with coarse-grained, high level aggregate data extrapolated from market observation and GDP figures.

Our solution, allowing central banks to utilize CBDCs via verifiable credentials with rich authentic transaction tagging, would solve this problem and provide new possibilities for public policy enabling novel monetary policy rollout, and allow for the creation and enforcement of a new internet identity infrastructure that is currently required in order to decrease costs, strengthen institutions, and take back privacy from entrenched private interests. This identity infrastructure allows for quantum secure, private, and regulatorily compliant payment transaction data capture. Core Web3 identity technologies, including key event receipt infrastructure (“KERI”), a secure identity overlay for the internet, authentic chained data containers, and application of verifiable credentials using modern graph database semantics, provide all needed facilities to ensure end-to-end authenticity of payment data using central bank authorized monetary payment infrastructure.

Furthermore, this technology stack provides for reliable, authentic tagging of payment transactions with geolocation data, market segment classification, jurisdictional annotations for law enforcement, and even product-level tagging while simultaneously allowing a decoupling of the tags from individual payments so that payer privacy is preserved all while enabling groundbreaking economic profiling capabilities. Each tag of a payment transaction is an extension of an existing credential and thus is authentic and verifiable, since each core credential is linked to an individual person’s identity. This identity uses the W3C standard for Decentralized Identifiers (“DIDs”), another core Web3 technology.

To summarize, privacy enhancing technologies can be implemented through digital asset platforms that bring essential identity and data protection features to retail, enterprise, and government users, while providing a path to data providence for all users. Lack of privacy in payment systems poses substantial risks, including the ability for those with access to reverse engineer transaction patterns and behavior, which could lead to several risks, including:

- Economic: the ability to reverse engineer and disrupt a value chain; and
- Personal: the ability to determine personal holdings for the purpose of extortion or theft; the ability to tailor pricing to an individual based on their past commercial behavior.

Numerous examples exist for both categories, clearly pointing to the requirement of a robust identity solution to preserve user privacy while providing appropriate anonymized data that will enable advancement in economic analyses and monetary policy.

Privacy enhancing technologies related to digital assets counteract risks to financial stability and prudent regulations. Moreover, the regulation of the digital asset market must build on current regulatory regimes, from the longer-term transition from cash to CBDCs, to replacing current centralized asset trading markets with DeFi solutions, in markets like equities, fixed income, mortgages, derivates, etc.

From RFI: *Goals, sectors, or applications that could be improved with digital assets and related technologies: Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered. This includes explanations of the current limitations in how those goals, sectors, and applications are currently advanced with limited use of digital assets and related technologies, and how increased or better use of digital assets could provide a specific advantage over existing approaches in advancing these objectives. Where relevant, respondents are encouraged to justify how digital assets provide unique value for advancing that goal, sector, or application compared to the use of traditional databases or other technologies (e.g., as outlined in National Institute of Standards and Technology Internal Report 8202, Figure 6).*

Bitt is a leader and important partner in developing efficient, equitable, and targeted monetary and fiscal policies using programmable CBDCs. There are numerous digital asset use cases that have been validated over the past few years in many markets, while others have yet to unfold. For example, USD stablecoins have not only serviced exponential growth in the DeFi space but have also provided a flight to safety for citizens in countries experiencing inflation, or dangerous living conditions that require them to store their wealth digitally outside of the banking system as they seek refuge in another country. With the proper design of an American CBDC, a digital USD could fulfill these same use cases and more by providing holders with access to risk free central bank money in digital form in times of need.

Another large opportunity that has yet to be realized is the use of CBDCs in public payments including public procurement, social transfers, relief funding, and other such programs. The use of CBDCs alongside complimentary Public Finance Management solutions could significantly improve the efficacy of funds, ensuring that a higher percentage is used in the approved manner, and not lost to corruption, leakage, or unnecessary intermediary actors.

Reports from the IMF, World Bank, and UNDP address issues related to poor efficacy, fraud and corruption in public payments, particularly in the context of social protection programs and other forms of public expenditure. Experts have noted that one of the challenges of implementing public payment programs is the risk of fraud and leakage, alongside the importance of effective targeting and delivery mechanisms to reduce the risk of fraud and ensure that payments reach their intended beneficiaries. Fraud and corruption are risks associated with cash transfer programs, particularly in settings with weak governance and enforcement mechanisms. Effective monitoring and evaluation systems are required, as well as strong institutional frameworks, to mitigate the risk of fraud and corruption. Overall, we see a significant opportunity for technological solutions to provide ransparency, accountability, and effective governance mechanisms to prevent fraud and ensure that payments reach their intended beneficiaries.

In addition to these reports, the IMF, World Bank, and UNDP have all developed policies and programs aimed at promoting transparency, accountability, and good governance in public expenditures that could be greatly improved by digital assets and associated assurance solutions. These solutions could help increase transparency and accountability, strengthen institutional frameworks, and provide legal and regulatory enforcement mechanisms to prevent and punish fraud and corruption, and ensure higher efficacy of public payment programs.

In response to Figure 6 within the NIST internal report 8202, DLT technology is much better suited for a CBDC than a possible legacy system; a well designed CBDC will require all of the uses highlighted in the figure:

- CBDCs require a shared consistent data storage in order to ensure transparency and integrity.
- CBDCs need more than one entity to contribute data, from the central bank to the consumer.
- CDBCs require data records that once needed are never updated, deleted, or destroyed.
- CBDCs require that sensitive identifiers will not be written to the data store in order to ensure privacy regulations are respected.
- CBDCs require entities with write access to have differentiated controls in order to maintain financial and monetary integrity.
- CBDC's require a tamperproof log of all writes to the data store.

From RFI: *Goals, sectors, or applications where digital assets introduces risks or harms: Information about goals, sectors, or applications where digital assets might introduce risks or harms, and examples of where risks or harms are already being manifested. This includes explanations of direct or indirect impacts on users of digital assets, communities or sectors in which digital assets might circulate or be integrated into services, and non-users (e.g., communities, environment) that may be exposed to risks or harms of digital assets (e.g., ransomware attacks, higher electricity costs, pollution). Where relevant, respondents are encouraged to justify how digital assets are introducing new risks or harms in advancing the underlying goal, sector, or application compared to the use of traditional databases or other technologies.*

The chief broader macro risk involved in the advancement of CBDCs stems from other countries gaining a substantial lead on the US in researching, testing, piloting, and deploying their own CBDCs prior to material progress being made on a digital USD. While there are many factors that play into the demand for a particular currency, given the rapidly evolving international financial technology ecosystem, a uniquely designed CBDC could gain significant market share in a short period of time provided it possessed certain technological and policy related characteristics. Such a scenario could be considered an issue of national security. The US stands to maintain dollar strength by testing a digital USD in diverse contexts and use cases in which it could provide benefits – both domestically and internationally. There is a demand for a digital USD given the substantial increase in market cap of the major USD stablecoins over the past few years.

From RFI: *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets: This might include information about R&D that helps companies build more environmentally-sustainable digital assets, assist law enforcement in countering illicit financial activity using digital assets, and enable regulators to protect consumers from fraud. This includes opportunities to innovate for equity and privacy with R&D that could help underserved communities harness the benefits of digital assets while being protected from their risks, such as via improvements to digital assets to allow them to better remain accessible, reliable, and secure even when connectivity and end-user device quality are limited.*

Existing research into the efficacy of social transfer and relief payments, such as those administered by USAID for countries in need of support, could be bolstered by further considering the use of CBDCs alongside extensive public finance management solutions to further drive accountability and transparency into how funds are spent and the outcomes they bring. Such a solution could also enable consumer protection and provide opportunities for underserved communities to make full use of funding while experimenting with cutting edge technologies that could enable new business models and enable financial inclusion.

Consumers are at risk of fraud when using digital assets, particularly given the lack of regulation and oversight in the industry. The federal government could support research on new technologies and solutions to protect consumers from fraud, such as through funding for blockchain-based identity verification systems or the development of more secure digital asset management solutions. Such efforts could be woven into a US CBDC research program to ensure a wholistic approach, leveraging both public and private DLT platforms.

The lack of clear regulatory frameworks and oversight mechanisms for digital assets has been a major challenge for industry participants and regulators alike. The federal government could support research on new approaches to regulating digital assets, such as through funding for policy analysis and development, or the development of new regulatory frameworks and oversight mechanisms.

From RFI: *R&D that should be prioritized for digital assets: Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present. This includes topics for technical research, topics for research in the social sciences and across disciplinary boundaries, and opportunities for hardware and software development. This also includes information about emerging areas that could enable new opportunities to leverage digital assets, as well as information about technical limitations of digital assets and the associated business models and governance arrangements they often rely upon. Respondents are encouraged to, where relevant, describe how the discussed R&D topic could be useful in helping a potential U.S. CBDC system align with the Policy Objectives for a U.S. CBDC System. Respondents are also encouraged to share how the discussed R&D topic could help advance U.S. competitiveness and leadership in the world.*

Ultimately, we believe that R&D should be focused and prioritized to determine how best to develop technology, frameworks and policy recommendations that advance the six key priorities identified in the Executive Order 14067.

Consumer And Investor Protection:

Within this section, we would like to reemphasize the point that testing, and research should be dedicated to implementing a CBDC that is deployed with privacy of the user at the center of design in a way that protects the individual, while fulfilling law enforcement requirements related to KYC/AML compliance, ant-corruption, and CTF. CBDC's allow for increases in privacy and increases in transparencies that will not only protect consumers, but also decrease risks for investors. Tests have shown that CBDCs could provide improvements on current privacy practices, given that there are no profit maximization incentives connected to privacy abuse. Opportunities exist to provide selective identification disclosures instead of wholesale copies of PII being shared across various stakeholders and institutions. Furthermore, there are opportunities to increase access to credit due to enhanced verification practices and provable financial activities. We can build a world in which governments and institutions have increased transparency of where capital flows within society, ensure that capital is allocated in areas and places that it was meant to be allocated, all the while ensuring consumers continue enjoying the privacy protections and anonymity that they enjoy today via current digital and cash-based payment methods.

Promoting Financial Stability

Research should focus on the impact a USD CBDC could have on monetary policy, disintermediation, and the roles of different players within the greater monetary system. The Federal Reserve, as well as Treasury, needs to test and evaluate the impact that CBDC may have on the monetary transmission mechanism, how targeted it could be, and its potential impact on behavior within different actors in the financial ecosystem. Testing should also focus on the efficacy of the two-tiered model recommended for CBDC's and the necessary stopgaps needed to prevent possible disintermediation, in addition to other technical solutions to mitigate the financial stability risk such as that proposed by the Regulated Liability Network.

Testing should also be focused on possible new mechanisms dedicated to improving management of the economy: testing of CBDC tools to fight inflation (such as indexing of real time price levels of goods or the use of CBDC's to program different interest rates for different economic sectors), financial inclusion (government benefits), and utilities (smart grid payment integration).

Countering Illicit Finance

Testing should focus on creating a properly designed CBDC that enhances KYC, AML, and CFT regulation with increased visibility and identity verification of illicit actors. One of the founding principles of our company was to find a solution to more stringent KYC, AML, and CFT regulations which caused banks to cut corresponding banking relationships with countries all throughout the Caribbean. Our solution, within the ECCB, was created to reconnect all countries within the ECCU to international financial flows while adhering to all applicable laws and regulations placed by the United States. Current CBDC frameworks are helping in this manner via harmonization of AML/KYC regulations across G20 cross-border payments; final design and harmonization, however, is still to be decided as central banks around the world research best practices and protocols. The United States needs to focus research within this space in order to maintain leadership in the design of CBDCs and illicit risks that may come.

U.S. leadership in the global financial system and economic competitiveness

We recommend that research and development of a US CBDC increases in intensity in the coming years, or the United States runs the risk of losing leadership in the global financial system. A United States CBDC will increasingly be a key national security factor and its need will only intensify in the coming years as competition with other private and public digital currencies continues to increase. It is increasingly clear that one of China's main goals in creating a CBDC is primarily to increase the speed and ease of international payments denominated in the renminbi in order to increase adoption of China's national currency as a form of international payment at the expense of the USD and Euro[1]. Current USD-based international payments are slow, expensive, and cumbersome for both US-based and international players. CBDC based projects stemming from Chinese competition in the Middle East have already moved countries away from paying in USD and towards other currencies. We expect movement in this area to continue to be away from the USD in the years to come unless the United States takes greater leadership in the space.

Financial Inclusion

Research within financial inclusion should be dedicated to exploring the mechanisms in which a CBDC could alleviate the more than 7 million American households[2] which remain unbanked. Increased research, such as the one spearheaded by MIT's Digital Currency Initiative *CBDC Expanding Financial Inclusion or Deepening the Divide* is needed not just at the federal level but also at the state level given the variety of reasons and geographies in which financial inequality exists within the United States. Research should focus on systems design research on the technical trade-offs of key CDBC design decisions (such as programmability of payments), on the roles of public, private, and civil societies have within a hypothetical USD CBDC, and public opinion on a CBDC implementation and education.

Responsible Innovation

Research on responsible innovation should focus on investigating platform design in order to increase competitiveness of the United States payment systems. Once architecture, roles, and decision-making frameworks of all players are agreed, testing should continue with sector-by-sector use cases such as supply chain and CBDC integration, health care system integration, and government aid payment trials with efficacy and decreased corruption as key goals.

[1] Greene, R. *Beijing's global ambitions for central bank digital currencies are growing clearer*. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2021/10/06/beijing-s-global-ambitions-for-central-bank-digital-currencies-are-growing-clearer-pub-85503

[2] *How america banks: Household use of banking and financial services*. (2019). Retrieved from https://www.fdic.gov/analysis/household-survey/2019execsum.pdf

From RFI: *Opportunities to advance responsible innovation in the broader digital assets ecosystem: Information about opportunities for the United States to advance responsible innovation in the broader digital assets ecosystem, in areas that are adjacent to R&D. This may include programs that could support increased education and workforce training related to digital assets, standards setting efforts that could help advance democratic values in the use and governance of digital assets, and supply chain opportunities to maintain access to the necessary hardware for emerging digital assets.*

Bitt's extensive experience in deploying national digital currency solutions with central banks and financial institutions worldwide have provided us with deep insight regarding challenges, strategies, and opportunities in rolling out novel financial technologies. For example, integration with existing systems including core banking, RTGS, ACH, and other legacy financial networks poses a set of challenges and opportunities for new use cases and functionality. Generally, connection points in systems have unique potential vulnerabilities that require extensive and comprehensive testing to ensure outcomes are within appropriate and acceptable boundaries.

In addition to legacy financial systems, other complimentary systems such as telecommunications, identity, accounting, and others provide opportunities for enhanced functionality and efficiency gains, while reducing settlement costs and times. For each potential connection point, research should be conducted in order to fully determine the primary and secondary effects of an implementation in order to identify and mitigate risk, determine stakeholders required, and explicitly define technical and functional requirements. Furthermore, critical financial services for enabling financial inclusion – such as remittance processors – should be tested in conjunction with CBDCs and stablecoins to determine the added benefits that could be realized by end users, who are often marginalized people seeking to support their families abroad.

Education plays a key role in advancing technical elements of financial technology as well as critical financial literacy skills for people of all ages. In a rapidly evolving financial technology ecosystem, education is a critical component in advancing equity goals throughout our society to ensure that individuals and enterprises alike are aware of:

- Financial tools, products, and services that could empower their economic efforts,
- Opportunities to innovate and contribute valuable products and services in market,
- The risks associated with participating in the digital asset ecosystem,
- Regulations, guidelines, and safeguards for fostering responsible innovation.

The establishment of CBDC standards is a critical effort required to align democratic nations worldwide. While some efforts have been made to quantify and depict the design decisions present in CBDC systems – including Bitt's CBDC Mindmap, and the Atlantic Council's paper "Missing Key: The challenge of cybersecurity and central bank digital currency" there are no go-to standards for central banks to reference in their CBDC design decision making process. Monetary authorities require referenceable decision-making framework in order to quantify the risks and tradeoffs associated with each identifiable design decision for their CBDC. CBDCs will become critical financial infrastructure in the coming years, and as such will require explicit requirements for deployment, access, maintenance, operations, and upgrades. While EO 14028 provides some relevant guidance for the management of critical software, additional CBDC-specific elements are required to comprehensively address the responsibilities of stakeholders involved in the management of CBDC platforms.

Appendix

Bitt's Mindmap: https://www.bitt.com/solutions/mindmap

When embarking on the journey of creating and deploying a CBDC, central banks face many decisions that will influence the nature of their national digital currency with respect to technology, governance, security, management, regulation, and more. Bitt's Mindmap represents a high-level framework to serve as a reference when preparing the formal considerations that are necessary in developing and deploying a CBDC.

Considerations follow a first principles approach and are divided into two main categories: CBDC Transaction Network, and CBDC Stakeholder Tools. The CBDC transaction network comprises the core ledger, a database that houses the balances of all wallets or accounts and continuously updates as transactions occur. The transaction network can be deployed in many configurations, each of which having unique software and hardware considerations. Stakeholder-specific functionality is considered in the applications section, and calls into question the variety of CBDC actions that each stakeholder group should be able to achieve on such a network, as well as corresponding accountability and data protection measures.

While such functionality is technically executed in a Business Process Manager, such as the Bitt Numa, it is useful to consider the corresponding applications and their stakeholder group in order to derive adequate governance and control mechanisms.

Furthermore, it is assumed that a percentage of these functions can be achieved via APIs through which stakeholders can integrate their existing tools and applications. Whether the system is centralized, distributed, or decentralized, all stakeholders will connect to the CBDC transaction network via APIs, each requiring the consideration of multiple factors pertaining to access and functionality.

Management of the network, on the other end, is considered in the context of who develops, hosts, and maintains the network, including governance considerations for upgrades and/or changes to the network, integrations, and other network-level changes. In addition, the management of the physical hardware on which all CBDC software resides is called into question, with considerations raised to ensure continuous operations.

This mindmap is not exhaustive and is meant to provide the basis on which to begin your CBDC development and deployment journey. Should you have any feedback, comments, questions, or additions, please reach out to centralbankbitt.com.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Blockchain Association

Blockchain Association
[redacted]

March 3, 2023

The White House
Office of Science and Technology Policy
[redacted]

Re: Request For Information; Digital Assets Research and Development, Document Number 2023-01534

To Whom It May Concern,

Blockchain Association (the "Association") submits this letter in response to the Office of Science and Technology Policy's ("OSTP") Request For Information ("RFI") titled "Request for Information; Digital Assets Research and Development."[1]

Blockchain Association is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for the digital asset economy. The Association endeavors to achieve regulatory clarity and educate policymakers, courts, and the public about how blockchain technology can pave the way for a more secure, competitive, and consumer-friendly digital marketplace. The Association represents nearly 100 member companies reflecting the wide range of the dynamic blockchain industry, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting public blockchain ecosystems.

Blockchain technology offers the opportunity to solve many systemic issues affecting the legacy financial system and our increasingly digital lives. Since 2009, Bitcoin — the world's first crypto network — has allowed individuals to quickly and cheaply transact with each other without relying on intermediaries like banks or payment processors. Blockchain technology, which powers Bitcoin and other crypto networks, has sparked a paradigmatic shift in the way people interact with each other online. For Americans to realize the benefits of blockchain technology, U.S. policymakers must ensure that American entrepreneurs, developers, and other builders may freely innovate here at home.

[1] Request for Information; Digital Assets Research and Development, 88 Fed. Reg. 5043 (Jan. 26, 2023), https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development.

Not only has blockchain technology offered new ways for Americans to interact online, it has helped to secure the dollar's status as the global reserve currency. The United States has a unique opportunity to use blockchain technology to spread the dollar and strengthen our economy by supporting dollar-denominated stablecoins. However, if the United States were to encourage adoption of a Central Bank Digital Currency ("CBDC"), rather than a privately-issued stablecoin, it could thwart goals to align the technology's potential with American values unless such a CBDC network were open-source, permissionless, and privacy-preserving. If a CBDC program does not embody these core characteristics, the United States risks violating Americans' constitutional rights and raising national security concerns by mirroring China's surveillance state. Instead, U.S. policymakers should welcome privately-issued stablecoins and focus on enacting narrowly-tailored legislation that aims to regulate centralized stablecoin issuers.

It is crucial for policymakers to understand the unique characteristics of blockchain technology and why it solves many of the problems rooted in our legacy financial system. Thus, it is necessary that data provided to Congress and regulators be peer-reviewed, technology-neutral, and impartial. This should help ensure that any regulation or legislation targeted toward blockchain technology or digital assets requisitely factors in its unique characteristics and reflects the latest understanding of the technology and its use cases.

Due to blockchain networks' unique characteristics, regulators and legislators ought to focus their efforts on mitigating risks posed by custodial intermediaries and establishing standards for disclosures, audits, and reserves, rather than restricting access to decentralized services, including decentralized finance ("DeFi"). This focus derives both from actual risk and available information. Many of the risks posed by custodial intermediaries are well understood and have been evident in high profile cases, while the most well-respected DeFi services use software rules to mitigate or eliminate these risks and have not failed even during market uncertainty.

Finally, it is particularly important that industry experts have the opportunity to provide robust and accurate information to lawmakers to help them avoid creating legislation with unintended consequences. It is all too easy for legislators to make knee jerk reactions to recent market events, but this would do more harm than good. Sweeping actions against the larger industry could have a chilling effect on crypto innovation, sending this promising technology overseas. As with other industries, the focus should be on punishing bad actors, deterring future misconduct, and creating pathways forward for good actors: this is essential to creating a regulatory landscape in which innovation can thrive in the United States.

* * *

Public Blockchains Solve Decades-Long Problems in the Legacy Finance and Information Technology Industries by Removing the Main Source of Risk and Abuse: Intermediaries.

During the depths of the 2008 financial crisis, an anonymous author published a whitepaper to a mailing list for cryptography researchers.[2] The paper described a distributed ledger technology that would allow for the transfer of value without an intermediary, or a "peer-to-peer electronic cash system," which the author termed "Bitcoin." This major breakthrough in the world of cryptography and computing solved the Byzantine Generals problem, which in game theory describes the difficulty decentralized parties have reaching consensus without relying on a trusted central party. The underlying technology would come to be known as "blockchain."

The Bitcoin network allows anyone anywhere in the world to send and receive value using nothing more than a computer and an internet connection. Before the advent of Bitcoin and blockchain technology, reliance on financial intermediaries, like banks, was necessary to make payments over the internet. For most traditional online payments today, multiple intermediaries are involved in a single transaction and act as gatekeepers, making electronic payment slow and expensive. These intermediaries have a history of exposing Americans' sensitive financial information to corrupt institutions, being vulnerable to cyber attacks, discriminating against underserved communities, and exploiting their own customers in the pursuit of profit.[3]

Current financial regulations are designed to protect against risks posed by these intermediaries. Cryptocurrencies and blockchain technology, however, mitigate traditional finance risks by replacing centralized intermediaries with a decentralized ledger that allows anyone to send payments across the world almost instantly, without needing permission, and at almost no cost. Government agencies and individuals can leverage a blockchain's transparency for enhanced analysis and use it as an investigation tool. It is a common misconception that cryptocurrency is completely anonymous and untraceable; rather, the transparency provided by many cryptocurrencies' public ledgers is much greater than that of other traditional forms of value transfer. The open and permanent record of the blockchain natively solves regulatory problems that previously could only be solved by imposing compliance obligations on trusted third parties.

Unlike the legacy banking system, which is dominated by large, private financial institutions, crypto networks are public payments infrastructure: digital cash for the digital era. And although digital cash was the first use case for crypto networks, it is far from the last. American innovators,

---

[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org (Oct. 31, 2008), https://bitcoin.org/bitcoin.pdf.

[3] *Terrorism and Cryptocurrency: Industry Perspectives Before the H. Subcomm. on Intel. and Counterterrorism*, 117th Cong. (2022) (statement of Kristin Smith, Executive Director, Blockchain Association), https://theblockchainassociation.org/wp-content/uploads/2023/02/Intelligence-and-Counterterrorism-Subcommittee-Hearing-Written-Testimony.pdf.

entrepreneurs, and developers are now building applications with blockchain technology, constructing the next iteration of the internet — sometimes referred to as "Web3."[4]

"Web1" refers to the early internet of the 1990s, when users could only do basic tasks like read static web pages or send emails. "Web2" refers to the internet we have today, with all its interactive applications and services, including social media. But just like the banking system, Web2 is dominated by a few large companies, or "tech giants," which wield outsized power and influence for their own profit at the expense of the American public. While today's internet has opened enormous benefits for the American economy, the vast wealth created has been captured by a small number of corporations.

Web3 — born from and built on crypto networks — is the solution to this imbalance of power. Web3 not only allows individuals to own their data and content,[5] but it also allows them to possess digital goods and property. The implications of this span a wide-range of applications including digital identity solutions, supply chain management, real estate, and healthcare.[6] Importantly, these applications run largely on decentralized networks, without incumbent entities capturing value in the form of excessive fees or targeted advertising. Individuals and small business owners[7] stand the most to gain. This revolutionary shift in our digital future will increase equity, lower barriers to entry, and enhance democratic values.

For the United States to realize the full benefits of Web3 and ensure we remain the global leader in this space, American entrepreneurs must have the freedom to innovate.

Reliance on Peer-Reviewed Reports and Impartial Data is Crucial for OSTP to Maintain Accuracy and Integrity in its Reporting.

On September 8, 2022, OSTP published a report on the climate and energy implications of crypto assets in the United States.[8] The Association appreciates OSTP's request in the RFI for feedback on this report. In response to OSTP's request, the Association wishes to respectfully

---

[4] Thomas Stackpole, *What is Web3?*, Harv. Bus. Rev.: Big Idea Series (May 10, 2022), https://hbr.org/2022/05/what-is-web3.

[5] Unstoppable Domains, *Control Your Personal Data in Web3 with Web3 Domains*, Unstoppable Domains: Blog Posts (Jun. 27, 2022), https://unstoppabledomains.com/blog/categories/web3-domains/article/control-your-personal-data-in-web3.

[6] Forbes Tech. Council, *15 Industries That Could Significantly Benefit From Blockchain Technology*, Forbes (Jun. 10, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/06/10/15-industries-that-could-significantly-benefit-from-blockchain-technology/?sh=45e7de777af2.

[7] Shai Bernstein & Christian Catalini, *How Digital Currencies Can Help Small Businesses*, Harv. Bus. Rev. (May 25, 2022), https://hbr.org/2022/05/how-digital-currencies-can-help-small-businesses.

[8] Off. Sci. and Tech. Pol'y, *Climate and Energy Implications of Crypto-Assets in the United States*, White House Office of Science and Technology Policy Report (Sept. 8, 2022) [hereinafter *OSTP Report*], https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

emphasize the importance of relying on peer-reviewed evidence and impartial research when drafting future reports.

While it is true that specific consensus mechanisms of certain crypto networks require significant energy consumption by design, the research cited in the report contained several flawed assumptions and narrowly-defined data sets. In several instances, the report relies on research paid for by special-interest groups diametrically opposed to crypto adoption. For example, the report states that "over the next decade, Texas may see an additional 25 GW of new electricity demand from crypto-asset mining, equivalent to a third of existing peak electricity demand in Texas."[9] However, this projection is not in line with observed demand within the industry.[10]

The report also compares global crypto network measurements with U.S. domestic energy consumption patterns.[11] This method fails to consider the outsized share of existing green energy infrastructure and later-generation mining rigs in the United States with respect to other nations.

Further, the data used in much of the research cited was from a narrow period of 2019 to 2022.[12] This timeframe represented the most recent wave of massive adoption and peak usage rates. Using projection models based on these samples likely exaggerates future adoption rates and consumption.[13] During previous cycles of rapid digital currency adoption, for example in 2017, energy consumption projections from Bitcoin mining were similarly overestimated and inflated.[14] The publishers of this data also cited additional problems with their methodology as it pertains to the selection of mining equipment in the sample, stating that their approach "may have periodically overstated Bitcoin's total power demand for a variety of reasons."[15]

---

[9] *Id.* at 5.

[10] Christopher Bendiksen, *A Closer Look at the Environmental Impact of Bitcoin Mining*, CoinShares (Mar. 30, 2021), https://coinshares.com/research/closer-look-environmental-impact-of-bitcoin-mining.

[11] *Compare OSTP Report*, *supra* note 8, at 15 n.80 (citing Alex De Vries, *Bitcoin Energy Consumption Index*, Digiconomist, https://digiconomist.net/bitcoin-energy-consumption (last visited Feb. 28, 2023)) *with OSTP Report*, *supra* note 8, at 15 n.81 (citing U.S. Energy Info. Admin., *Documentation of the National Energy Modeling System (NEMS) Modules*, U.S. Dep't. Energy, https://www.eia.gov/outlooks/aeo/nems/documentation (last visited Feb. 28, 2023)).

[12] *Id*. at 9 n.28 (citing Cambridge Bitcoin Electricity Consumption Index, *Bitcoin Mining Map Visualization*, https://ccaf.io/cbeci/mining_map (last visited Feb. 28, 2023)).

[13] *Id.* at 17 n.102 (citing Naureen S. Malik, *Crypto Miners' Electricity Use in Texas Would Equal Another Houston*, Bloomberg (Apr. 27, 2022), https://www.bloomberg.com/news/articles/2022-04-27/crypto-miners-in-texas-will-need-more-power-than-houston).

[14] Tom DiChristopher, *No, bitcoin isn't likely to consume all the world's electricity in 2020*, CNBC, (Dec. 21, 2017), https://www.cnbc.com/2017/12/21/no-bitcoin-is-likely-not-going-to-consume-all-the-worlds-energy-in-2020.html

[15] *Cambridge Bitcoin Electricity Consumption - Methodology*, Cambridge Center for Alternative Finance, https://ccaf.io/cbeci/index/methodology (last visited Feb. 28, 2023).

We urge the OSTP to ensure that recommended policies remain neutral with respect to underlying technologies. For example, recommendations to explore executive or legislative action to "eliminate the use of high energy intensity consensus mechanisms for crypto-asset mining" would discriminate against certain types of data centers (i.e., those that perform certain computations) over others that consume similar amounts of energy.[16]

The Association does not question the important work of combating climate change, a critical component of our nation's and the world's environmental, economic, and national security. However, the Association emphasizes the importance of considering peer-reviewed evidence, impartial academic research, and transparent industry data to support future initiatives.

The Advantages of a CBDC are Unclear.

As technology allows for the digitization of money, policy decisions carry with them the potential to either positively or negatively impact privacy, security, and the preservation of Americans' constitutional rights. In particular, the question of how best to implement digital cash in our society largely revolves around the choice between using privately-issued stablecoins or CBDCs.

Stablecoins, like other digital assets, run on decentralized public blockchains, meaning anyone can use them without having to rely on a trusted third party. The public nature of these networks means they are more secure, since a successful cyber attack requires hacking thousands of computers running shared code versus one single centralized database; more accessible, since they can be used by anyone with access to the internet; and more resilient, since decentralized networks suffer virtually no outages compared to systems with single points of failure.

For many reasons, a CBDC is the wrong way to maintain U.S. dollar dominance in the digital era.

First, to strengthen the dollar's dominance as the global reserve currency, our main priority should be to spread dollars far and wide—to make them available to anyone and everyone around the world. Privately-issued stablecoins have already made a huge impact in global crypto markets: they have added to the competition in the payments landscape by serving as a faster, cheaper, and more flexible means of sending dollar-denominated payments internationally, in addition to providing a means of accessing the value of fiat currencies without leaving the crypto ecosystem. Stablecoins have already achieved much of what a CBDC would do, particularly because dollar denominated stablecoins are the preferred stablecoin of many users. Rather than reinvent the wheel, the U.S. should support the growth of existing stablecoins.

Second, we should seek to maximize the contribution of our vibrant and experienced private sector, not sideline it in favor of a centrally-planned government project. While other nations like China might give their central governments total control over emerging industries and

---

[16] *OSTP Report*, *supra* note 8, at 7.

technologies, that is decidedly not the American way. As former Vice Chair for Supervision of the Federal Reserve, Randal Quarles, explained, "A global U.S. dollar stablecoin network could encourage the use of the dollar by making cross-border payments faster and cheaper, and it potentially could be deployed much faster and with fewer downsides than a CBDC." Issuing a CBDC instead of supporting the development of private stablecoins would cause entrepreneurs and other members of the private sector to bring their innovations to countries other than the United States, causing us to miss out on the opportunity to become a leader in this space.

CBDCs also present major concerns for users: CBDCs can easily grant state actors a so-called "God's eye view" of the entire economy, tracking purchases and gleaning intimate personal details of its users. Rather than running on permissionless public blockchains, CBDCs are managed by a single central authority with the power to surveil, censor, and exclude users. A financial system subject to total command and control by the government would jeopardize Americans' fundamental rights to financial freedom and privacy.

These issues have come to the forefront in recent years, as the combination of cybersecurity breaches and surveillance capitalism have revealed a dire need for data privacy protection. This is not just a minor concern, it is an issue of constitutional import. Except in limited cases, the Fourth Amendment requires the government to obtain a warrant before it can search a person's financial records. The fundamental right to privacy is a prized American civil liberty and an essential feature of a functioning free society. This is what separates a nation like ours, which respects its citizens' autonomy and dignity, from one like the People's Republic of China, which has exploited technology to create a dystopian surveillance state. Look no further than China to see what a censored version of the internet, and financial networks, will inevitably become. The U.S. adoption of a CBDC could similarly threaten or bring real harm to everyday Americans.

If Congress Were to Authorize the Creation of a CBDC, It Must Be Open-Source, Permissionless, and Privacy-Preserving.

Should Congress ever empower the Federal Reserve to issue a CBDC, it must retain the design properties of cash with three principles on which cash-based commerce functions:

1. Open-Source – The underlying network on which the CBDC is issued should be open-source so anyone can build on it, innovate with it, and incorporate CBDCs into their businesses and personal accounts.

2. Permissionless – Anyone must be able to create an account and use CBDCs without having to seek approval and risk being cut out from the economy due to political, economic, social, or other reasons.

3. Privacy-Preserving – American citizens are legally able to exchange cash for goods and services without needing permission from a centralized authority. This must remain the case in a world where CBDCs exist at a global scale. Peer-to-peer commerce is the

essence of American capitalism and it is what allows our economy and our democracy to function in a free and fair way.

By contrast, consider again what is today playing out in China, where the government has fully embraced the digital yuan, its version of a CBDC.[17] It is obvious why the Chinese Communist Party has moved so quickly to implement a CBDC: it represents a once-in-a-century opportunity to expand its influence abroad by requiring foreign trade and investments to be conducted with the digital yuan through its CBDC network, while also providing a vast financial surveillance tool, giving it full access and control over the finances of Chinese citizens. In other words, CBDCs are a win-win for the Chinese ruling party's ambitions.[18]

The Association finds that the true strength of the American dollar lies in it being backed by the United States itself and the democratic values it upholds abroad. These include freedom of speech and assembly, fundamental rights to privacy and property, and the opportunity to pursue a prosperous future. The dollar's comparative advantage over other currencies backed by authoritarian and manipulative governments would be best exercised through well-regulated, privately-issued U.S. dollar-backed stablecoins.[19] This strategy would serve the national interest by both fully embracing the efficiencies of emerging technology, while removing the risk of eroding core American values.

Our Recommendations for the Path Forward on Responsible Innovation.

The Association appreciates the work of OSTP in gathering information on crypto networks and digital assets. Understanding the nuances of decentralized networks and what sets blockchain apart from previous generations of computing technology is prerequisite to successful regulatory steps by Congress and government agencies.[20]

Regulating any new technology should require a broad understanding of the unique characteristics that distinguish it from others: automobiles require different rules than horse-drawn carriages; electric light bulbs require different rules than gas lanterns; email

[17] Jamie Crawley, *China Targets Blockchain Breakthroughs With Beijing Research Center: Report*, CoinDesk (Feb. 10, 2023), https://www.coindesk.com/policy/2023/02/10/china-targets-blockchain-breakthroughs-with-beijing-research-center-report/.
[18] Jennifer Conrad, *China's Digital Yuan Works Just Like Cash—With Added Surveillance*, Wired (Nov. 8, 2022), https://www.wired.com/story/chinas-digital-yuan-ecny-works-just-like-cash-surveillance/.
[19] *Toomey Outlines Stablecoin Principles to Guide Future Legislation Before the S. Committee on Banking, Housing, and Urban Development*, 117th Cong. (2021), https://www.banking.senate.gov/newsroom/minority/toomey-outlines-stablecoin-principles-to-guide-future-legislation; Josh Gottheimer, *Release: Gottheimer Announces 'Stablecoin Innovation and Protection Act,' Critical New Cryptocurrency Legislation*, Josh Gottheimer: New Jersey's Fifth District (Feb. 15, 2022), https://gottheimer.house.gov/posts/release-gottheimer-announces-stablecoin-innovation-and-protection-act-critical-new-cryptocurrency-legislation.
[20] Jake Chervinsky & Kristin Smith, *How Congress Can Get Crypto Legislation Right*, The Information (Jan. 11, 2023), https://www.theinformation.com/articles/how-congress-can-get-crypto-legislation-right.

protocols require different rules than regular mail through the U.S. Postal Service. The same gap in perspective has hindered attempts to regulate decentralized networks built on public blockchains, which require rules that fit the technology rather than analog financial infrastructure.

There are several specific issues for which fit-for-purpose regulations can allow for blockchain and crypto innovation to flourish in the United States, while mitigating risks to consumers and financial stability.

First, legislators ought to capitalize on the broad industry and bipartisan Congressional support for centralized stablecoin regulation. Although there is broad support, there are a few general principles worth highlighting for this regulation. Regulation of stablecoins should be narrowly tailored and harmonized within the United States and across jurisdictions globally. Any framework for stablecoins should seek to maintain and promote the international competitiveness of the United States and the dollar. Regulation should protect the privacy, security, and confidentiality of individuals utilizing stablecoins, including allowing customers to opt out of sharing any information with third parties, and financial surveillance requirements under the Bank Secrecy Act should be modernized, including for existing financial institutions, in light of emerging technologies like stablecoins.

Second, stablecoin issuers should be subject to operational requirements, including: disclosures regarding assets held in reserves backing the stablecoin; clear policies regarding creation and redemption of stablecoins; and routine audits or attestations by registered public accounting firms. The reserves of stablecoin issuers should be limited to specified, high-quality, liquid assets that do not pose an unreasonable risk to the soundness of said reserves, and stablecoin issuance should not be limited to insured depository institutions. In addition, commercial entities should be eligible to issue stablecoins, provided they choose one of the stated regimes. Finally, non-interest bearing stablecoins should not be regulated like securities.

A second issue ripe for further consideration is tailored regulation of spot markets. Legislation and regulatory actions addressing spot market exchanges should focus on the risks posed by custodial intermediaries. These actions should establish standards around disclosures, audits, and reserves, and ensure that decentralized protocols can continue to operate in a decentralized manner. Lawmakers should not simply restrict access to the nascent and vibrant world of DeFi, particularly because DeFi technology natively solves regulatory problems that previously could only be solved by imposing compliance obligations on trusted third parties—such risks were introduced by intermediaries and are mitigated and/or eliminated by disintermediation. Such measures would greatly benefit both American consumers and entrepreneurs without having an undue chilling effect on innovation.

Third, there are some broad principles that could aid regulators as they approach the space. Regulators should focus initially on business models within the industry that they understand. These tend to be similar to traditional financial institutions in their models and practices.

Authorities, including law enforcement and federal investigators, should continue to pursue any and all bad actors who may be operating in the space, focusing on persons or entities who seek to exploit Americans for nefarious purposes. Lastly, regulators should regularly engage with partners within industry who stand ready to assist authorities in protecting and safeguarding our citizens using cutting-edge products and services.

The Association urges OSTP and other government entities to continue to gather input from industry experts. This process can help strengthen regulatory proposals and sync them with reality. Regulators should not implement reactionary measures to recent market events without understanding the implications. Ungrounded efforts like these are what ultimately led to a provision in the 2021 Bipartisan Infrastructure Bill[21] that imposed tax reporting requirements[22] on a potentially massive number of users in the crypto space, even where compliance would be impossible due to the nature of the technology.[23] It is imperative to balance the desire to mitigate risk with the enormous opportunities stemming from American innovation. The Association implores Federal agencies and Congress to take the required time necessary to get regulations right.

Conclusion.

The Association reiterates its broad support for implementing a well-researched regulatory framework that balances all considerations outlined above. Industry leaders appreciate the opportunity to directly contribute to information-gathering activities and fully endorse these important and open processes. The Association offers its members and staff as a resource for any further questions, concerns, or detailed information on the contents of this submission.

Respectfully submitted,

[redacted]

Kristin Smith
Chief Executive Officer

[redacted]

Jake Chervinsky
Chief Policy Officer

---

[21] H.R. 3684, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/house-bill/3684.

[22] Kelly Makena, *Controversial crypto rules remain in infrastructure bill after House vote*, The Verge (Aug. 25, 2021), https://www.theverge.com/2021/8/25/22641375/cryptocurrency-infrastructure-irs-tax-developers-miners-bitcoin.

[23] Abraham Sutherland, *Research Report on Tax Code 6050I and Digital Assets*, Proof of Stake Alliance (Sept. 17, 2021), https://www.proofofstakealliance.org/wp-content/uploads/2021/09/Research-Report-on-Tax-Code-6050I-and-Digital-Assets.pdf.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Blocky Inc.

It is essential for regulators to distinguish between several, often conflated, components of blockchain technologies:

- Distributed ledger technologies (DLTs) are data structures and code that produce an immutable ordering of data.
- Utility tokens are used to remunerate infrastructure operators.
- Security tokens are used to raise capital for companies resulting in speculative investment vehicles.

From the above distinctions, we make the following two comments:

1. From a technical perspective, tokens are not required for the construction and operation of DLTs. Regulatory discussions often conflate DLTs and tokens. When talking about regulation, it is important to focus on regulating tokens and not blockchain technologies as a whole. Specifically, regulatory language should not be so general as to encompass DLT data structures and code.
2. Distinguishing utility tokens from security tokens is challenging because many security tokens are also used as utility tokens to remunerate DLT infrastructure operators.
   A maximalist definition of utility tokens is that they are non-transferable between owners and non-convertible to fiat. A good example are cloud computing credits, which are non-transferable between organizations and are non-convertible back to USD.
   A maximalist definition of security tokens is that they are transferable, convertible, and their utility lies in the eye of the beholder. An example of a security token is a Dutch tulip bulb between 1634-1637.
   US companies and innovators need a clear distinction between utility tokens and security tokens that separates the grey area between the two. This distinction is necessary for blockchain companies to support the operation of DLT infrastructure, while remaining compliant with token regulations.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Bank Policy Institute (BPI)

American Bankers Association (ABA)

March 3, 2023

Via electronic mail to DARD-FTAC-RFI@nitrd.gov

Rachel Wallace, Deputy General Counsel
Office of Science and Technology Policy

Re: Comments on Request for Information; Digital Assets Research and Development

Ladies and Gentlemen:

The Bank Policy Institute[1] and the American Bankers Association appreciate the opportunity to comment on the White House Office of Science and Technology Policy's request for public comments to help identify priorities for research and development related to digital assets[2] issued in connection with Executive Order 14067, "Ensuring Responsible Development of Digital Assets."[3] The trades support the goal of the Executive Order to promote a coordinated, "whole of government" approach to fostering responsible innovation, which will help ensure that the United States remains a global leader in innovation while also ensuring that consumers, the financial system, and national security are protected. We recommend that the public and private sectors continue to collaborate on how to further responsible innovation in the United States, including through continued research and open dialogue.

The trades support responsible innovation conducted in a manner consistent with the safety and soundness of the financial system, anti–money-laundering ("AML") and countering-the-financing-of-terrorism ("CFT") standards, and robust consumer and investor protections. Digital assets and related activities have grown rapidly in recent years and have the potential to provide benefits to consumers and businesses and the financial system. As with any new technology, there are associated risks that must be carefully studied, mitigated, and managed through proper controls, regulation, and oversight.

Today, digital assets, though they may carry varying levels of risk, are often nevertheless broadly categorized.[4] Defining important terms and developing a comprehensive and harmonized lexicon for the

---

[1] See Appendix for association descriptions.

[2] 88 Fed. Reg. 5043 (Jan. 26, 2023).

[3] 87 Fed. Reg. 14143 (March 14, 2022).

[4] For example, the RFI provides that the term "digital assets" refers to all CBDCs, regardless of the technology used, and to other representations of value, financial assets and instruments, or claims are issued or represented in digital form and that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof. For example, digital assets include cryptocurrencies, stablecoins, and CBDCs. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, or through peer-to-peer technologies. For the purposes of this RFI, "digital assets" is also inclusive of its underlying technologies (e.g., DLT).

various types of digital and crypto assets and entities active within the digital-asset ecosystem, and supporting infrastructures, will help authorities more effectively target the unique risks that each present. Authorities must distinguish among digital assets, cryptocurrencies, and tokenized assets, as well as the underlying distributed ledger technology ("DLT") and blockchain infrastructure, which may differ in use across functions and activities, when they apply existing (or develop new) regulatory frameworks for them. For example, the volatility and related risks often cited in connection with "digital assets" or "crypto assets" refers to risks presented by non-bank issued cryptocurrencies and stablecoins (e.g., bitcoin and Tether)[5], which operate on wholly different infrastructures and mechanisms of operation, but are comparatively different when using a distributed ledger network for use-cases other than cryptocurrencies.[6] Traditional banking products and activities utilizing DLT, blockchain, or other novel technologies provided by federally insured or regulated banks or subsidiaries of bank and financial holding companies do not present the risks presented by non-bank crypto-asset service providers and non-bank issued cryptocurrencies or related activities because banks appropriately manage their risks and are subject to a comprehensive regulatory framework and consolidated supervision, audits and examinations. Policymakers should research and study how to develop a comprehensive framework to apply appropriate standards and oversight to address the risks presented by nonbanks engaging in cryptoasset-related activities, such as issuance and trading of cryptocurrencies, to preserve financial stability and protect consumers, investors, and businesses.

Banks stand ready to innovate in this space, but the banking regulators do not appear to have appropriately distinguished between traditional bank activities using DLT or blockchain, such as tokenizing existing bank liabilities (deposits) or securities, and non-bank issued cryptocurrencies, which present very different risks given the inherent design of the various activities. Under the existing regulatory framework and effective robust risk management function of banks, traditional banking activities using new technology are well-managed by banks with well-established controls for product development, and banks can manage the risks of traditional banking activities using DLT or blockchain. Any contrary view is hindering the establishment of a reliable and clear regulatory environment, limiting the ability of banks to engage in responsible innovation that could potentially benefit consumers and investors, create marketplace efficiencies, and strengthen the resilience of the financial system.

The RFI asks several questions about topics on which BPI and ABA have written extensively, including CBDCs.[7] Below, we provide references and citations to our prior work on this topic and others, as relevant to the particular question, in light of the limitation on comment length.

1. Goals, sectors, or applications that could be improved with digital assets and related technologies.

---

[5] Examples are non-exhaustive.

[6] *See, e.g.,* Blockchain application within a multi-sensor satellite architecture, NTRS – Nasa Technical Reports Server, NASA (link) (discussing potential application of blockchain usage with constellation and swarm satellite architectures); *see also* Biology-Inspired Distributed Consensus in Massively Deployed Sensor Networks, NTRS – Nasa Technical Reports Server, NASA (link) (abstract discussing "fully distributed consensus can be attained in a scalable fashion in massively deployed sensor networks where individual motes operate based on local information, making local decisions that are aggregated across the network to achieve globally-meaningful effects)."

[7] As we have previously detailed, an intermediated, account-based CBDC could pose serious risks to the U.S. economy and financial system that would not be outweighed by the purported benefits. *See*, *e.g*., the Bank Policy Institute's work on central bank digital currency and stablecoins (link), and ABA's work on CBDCs (link).

Using new technologies, banks have made significant progress in developing products and services that could benefit consumers and the financial system, consistent with the banks' safe and sound operation.[8] For example, banks have come to recognize that DLT is a secure method of recordkeeping that may have the potential to drive efficiencies, decrease transaction times, and reduce systemic risk. Banks' blockchain-based deposit accounts[9] have been used to clear and settle repo trades and conduct inter-affiliate, intra-company transfers.[10] Blockchain technology has also been used to facilitate information sharing across financial institutions where such information is required to clear or validate payments.[11]

Banks are also planning to use tokenized deposits to facilitate traditional trading and market activity, including spot transactions, lending, and collateral management. Blockchain-based deposits enable "advanced programmability features, the ability to exchange funds with other digital assets atomically, and the transfer of commercial bank money on shared or universal ledgers where enhanced transparency of transactions and 24/7 transfer availability are possible".[12] Today, digital assets, though they may carry varying levels of risk, are often nevertheless broadly categorized into a single group.[13] Policymakers should research and define important terms and develop a comprehensive and harmonized lexicon for the various types of digital and crypto assets and entities active within the

---

[8] Examples of banks' innovation include the Regulated Liability Network proof of concept to tokenize commercial bank, central bank, and electronic money on the same chain, which offers the promise of delivering a next-generation digital money format based on national currency units (*e.g.*, denominated in U.S. dollars). *See* Press Release, Members of the U.S. Banking Community Launch Proof of Concept for a Regulated Digital Asset Settlement Platform (Nov. 15, 2022) (link). As another example, Partior, a shared-ledger multicurrency clearing platform, was launched as a technology company by JPMorgan, DBS, and Temasek in 2021. *See* Press Release, JPMorgan Chase & Co., DBS, J.P. Morgan and Temasek to Establish Platform to Transform Interbank Value Movements in a New Digital Era (Apr. 28, 2021) (link). Partior is designed to perform atomic clearing and settlement on a 24x7 basis among participating institutions using blockchain and smart-contract technology. *See* "Partior Aims to Become the World's Ledger for Banks", DigFin (May 15, 2022) (link); "The Global Ambitions of Partior, the JP Morgan, DBS Blockchain Payment System", Ledger Insights (Nov. 16, 2022) (link).

[9] Banks are authorized to issue tokenized deposits, establish blockchain-based deposit accounts, and issue stablecoins, as governed under existing federal banking agency regulations and managed via banks' risk management systems. *See, e.g.*, Office of the Comptroller of the Currency, *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities*, Interpretive Letter No. 1174 (Jan. 4, 2020) (link). *See also* TCH, Bank Issuance of Stablecoins and Related Services: Legal Authority and Policy Considerations (Nov. 2022) (link) (provided by Sullivan & Cromwell LLP at TCH's request).

[10] Blockchain deposits can exist in four forms: non-native deposit accounts, native deposit accounts, non-native token-based and native token-based. Tokenized deposits can be native or non-native. For purposes of this response, the term "tokenized deposit" refers to both native and non-native token-based blockchain deposits. *See* Oliver Wyman and Onyx by JPMC Report: "Deposit Tokens: A foundation for stable digital money," at 14 (Feb. 9, 2023) (link).

[11] For example, Liink by JP Morgan Onyx allows a bank sending a payment to pre-validate with the receiving bank that it is sending payment to a valid open account, avoiding prolonged payment processing and rejection for invalid accounts (link).

[12] *See* Oliver Wyman and Onyx by JPMC Report: "Deposit Tokens: A foundation for stable digital money," at 14 (Feb. 9, 2023) (link). For example, banks participated together in Partior and in the Monetary Authority of Singapore's project Guardian's "institutional DeFi" protocol (link).

digital-asset ecosystem, and supporting infrastructures, which will help authorities more effectively target the unique risks that each presents.

Traditional banking products and activities utilizing DLT, blockchain, or other novel technologies do not present the risks presented by nonbank-issued crypto assets. Policymakers should conduct research and understand the different risks posed by different categories of digital assets to identify the most effective ways to address risks within those categories.

Separately, there are different types of DLT/blockchain networks that vary in breadth of access and control. Public, permissionless blockchains allow anyone to access the network and engage with it, but within public blockchain infrastructures, permissions may be imposed on interactions with certain smart contracts deployed on the infrastructure, while within private, permissioned blockchains, access is limited to parties with appropriate entitlements. These types of networks present different levels of risk. The existing regulatory framework and banks' risk management practices enable banks to manage the risks presented by permissioned networks. Policymakers should consider further study of risk identification and management with respect to permissionless blockchains, which could potentially support the development of appropriate tools, such as digital identity or "verifiable credentials," that could make public blockchain more safe and secure so that banks and other commercial segments, as well as consumers, could potentially avail themselves of the benefits of such technology. Such benefits may include greater interoperability among bank systems, enhancement in information communication, and a reduction to barriers and costs in cross-border payments.[14]

Banks appropriately manage any technology-related risks in connection with standard internal recordkeeping functions and tokenizing traditional banking products. Banks use technology only if they determine the associated risks could be appropriately managed consistent with their risk appetites and risk management capabilities. Federally-insured banking organizations are subject to comprehensive regulation, supervision, and examination for compliance with prudential, consumer protection, and data privacy requirements, among others. Larger banking organizations have separate examinations of, among other areas, custody and technology.[15] Adherence to these standards is monitored by on- and offsite banking agency examiners. Banks' books and records systems are already subject to standards and oversight to address risks associated with these systems. Changing a bank's internal books and records design from a more traditional database design to a blockchain or DLT-based design does not change the underlying activity, nor introduce unknown parties, and should be evaluated under the

---

[14] For example, the Monetary authority of Singapore's Project Guardian will "develop and pilot use cases in four main areas," including exploring "the use of public blockchains to build open, interoperable networks that enable digital assets to be traded across platforms and liquidity pools. This includes interoperability with existing financial infrastructure" (link).

[15] This supervisory oversight includes the robust evaluation of information technology risk management, internal controls, and cybersecurity risk management. Banking organizations also must meet regulatory expectations with respect to other operational resiliency obligations and recovery and resolution planning mandates Banking organizations are subject to exams that evaluate how well management addresses risks related to the availability of critical financial products and services, including risks arising from cyber events. Management must also ensure the adoption of processes to oversee and implement resiliency, continuity, and response capabilities to safeguard employees, customers, and products and services. *See* Federal Financial Institutions Examination Council, FFIEC Information Technology Examination Handbook: Business Continuity Management (Nov. 2019) (link).

existing supervisory framework.[16] Banks are able to address operational risks associated with DLT and blockchain, thus avoiding the need for additional requirements, including capital requirements, to address operational risk from new technology. The regulators must appropriately identify and understand the risks of each type of network, controls and operating model to establish proper guardrails without adopting overly punitive measures that stifle responsible innovation. However, guidance issued by the regulators currently suggests that the regulators may view the risks presented by banks' use of DLT and blockchain as akin to those presented by nonbank-issued cryptoassets, which could slow the pace of banks' ability to engage in responsible innovation in this space.[17] In particular, guidance issued by the federal banking agencies requires banking organizations to provide advance notice, and if applicable, receive supervisory nonobjection based on an evaluation of the adequacy of risk management systems and controls before conducting certain traditional banking activities using DLT or blockchain, hindering responsible innovation."[18] Banks are consistently evaluating and managing the risk of incorporating new technologies and implementing solutions to mitigate evolving risks. Banks' management of dynamic cyber risks provides an example of how regulated financial institutions are able to evolve controls to mitigate new risks.

Policymakers, in particular, the federal banking agencies, should study how banks are able to appropriately manage the risks presented by permissioned DLT, blockchain, or other novel technologies in connection with traditional banking products such as deposits and securities, and for internal recordkeeping and eliminate the requirement that banks provide prior notice, or, in some cases, obtain prior approval, before engaging in those activities. Any concerns may be addressed through the normal supervisory process, as is the case with all of a banking organization's operations. Policymakers should study the impact of the banking regulators' conflation of the risks of different types of DLT/blockchain networks and digital asset products on the United States's competitive position in global financial markets, including potential implications if U.S. banks are unable to support digital clearing and settlement activities. For example, some firms have launched innovative banking and financial products

[16] The electronic book entries present in such a recordkeeping system serve the identical functional purpose as electronic book entries used to record assets in traditional electronic books and records systems. Accordingly, the use by a bank of blockchain or DLT for internal recordkeeping purposes and accompanying internal electronic book entries should not be subject to any additional regulation beyond the existing supervisory framework applicable to a bank's internal books and records systems or additional capital requirements.

[17] For example, the Federal Reserve's Policy Statement on Section 9(13) of the Federal Reserve Act, which discusses risks related to cryptoassets, states that "the term "crypto-assets" refers to digital assets issued using distributed ledger technology and cryptographic techniques (for example, bitcoin and ether), but does not include such assets to the extent they are more appropriately categorized within a recognized, traditional asset class." The Policy Statement then undermines this relative clarity by noting that "[t]o the extent transmission using distributed ledger technology and cryptographic techniques changes the risks of a traditional asset (for example, through issuance, storage, or transmission on an open, public, and/or decentralized network, or similar system), the Board reserves the right to treat it as a "crypto-asset" (link).

[18] *See* OCC Interpretive Letter No. 1179, Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank (Nov. 18, 2021) (link); FDIC, FIL-16-2022, Notification of Engaging in Crypto-Related Activities (April 7, 2022) (link); Board of Governors of the Federal Reserve System, "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations", SR 22-6 / CA 22-6 (Aug. 16, 2022) (link).

and services in other countries due to the uncertain regulatory environment in the United States for conducting such activities.[19]

Policymakers should also consider studying the impact of the banking regulators' limitations on banks' involvement in certain digital asset activities on consumers. The public and the financial system *benefit* from banks' involvement in the activities described in the Interpretive Letters. For example, with respect to custodying cryptoassets, banks have a long history of providing, and are well-suited to provide, safeguarding services. Thus, banks continue to evaluate whether to enter this business, and, for those who have already entered this business, they are precluded from doing so at scale.[20] If regulated banking organizations are effectively precluded from providing crypto-asset safeguarding services at scale, investors and customers, and ultimately the financial system, will be worse off; the market would then be limited to custody providers that do not afford their customers the legal and supervisory protections provided by federally-regulated banking organizations.

2. Goals, sectors, or applications where digital assets introduces risks or harms.

As we have described in the past, and as policymakers have recognized, crypto assets present unique risks.[21] As recommended previously, the only way to mitigate these risks is to adopt a comprehensive regulatory and supervisory framework at the national level that addresses each risk posed by crypto-asset companies, their subsidiaries, affiliates, and other related entities active in that ecosystem.[22] Policymakers should first study and develop an ontology to distinguish among crypto asset

---

[19] For example, HSBC recently launched the Orion platform, a bond tokenization initiative, in Luxembourg. The security would be both issued and registered under Luxembourg law (link).

[20] A related obstacle to banks' serving as custodians in the crypto marketplace is the SEC's Staff Accounting Bulletin No. 121, which would require an entity safeguarding a cryptoasset to present a liability (and recognize a corresponding asset) on its balance sheet equal to the fair value of the safeguarded cryptoasset. SEC Staff Accounting Bulletin No. 121 (March 31, 2022) (link). The SEC staff has indicated that SAB 121 is driven by investor protection concerns related to legal, technological, and regulatory risks arising from custodied assets; as we have previously explained, banking organizations comprehensively address these risks through the legal, regulatory and supervisory frameworks applicable to those organizations. The federal banking agencies and the SEC should jointly study these frameworks and determine that banks should be excluded from the accounting treatment in the SAB, thereby enabling them to provide custody services for cryptoassets at scale, which should include consideration of the SEC's recent proposal to expand the range of client assets that investment advisers must secure with "qualified custodians" such as banks or broker-dealers to include crypto assets and to enhance the protections afforded clients' custodied assets. *See* letter from ABA, BPI, and SIFMA re: SAB 121 to the Office of the Chief Accountant of the SEC, the OCC, the FDIC, the Federal Reserve Board, and the Department of the Treasury (June 23, 2022) (link); *see also* SEC proposed rule changes to enhance protections of customer assets managed by registered investment advisers (Feb. 15, 2023) (link).

[21] *See, e.g.*, Financial Stability Board, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Document (Oct. 11, 2022) (link); Financial Stability Board, Review of the FSB High-Level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative Report (Oct. 11, 2022) (link); *See* President's Working Group on Financial Markets, FDIC, & OCC, Report on Stablecoins (Nov. 2021) (link); [21] U.S. Department of the Treasury, Crypto-Assets: Implications for Consumers, Investors, and Businesses 51 (Sept. 2022) (link); Financial Stability Oversight Council, Report on Digital Asset Financial Stability Risks and Regulation (2022) (link). *See also* Letter from Paige Pidano Paridon, BPI, to Daniel J. Harty, Director, Office of Capital Markets, U.S. Department of the Treasury (Aug. 8, 2022) (link); Letter from Paige Pidano Paridon, BPI, and Robert H. Hunter, TCH, to The Financial Stability Board (Dec. 15, 2022) (link).

[22] *See* Letter from BPI and TCH to the FSB (Dec. 15, 2022).

types and the risks that are posed by each asset type to best determine what laws, regulations, and other requirements are most approiate to address those particular risks. For example, stablecoins may require prudential regulation, supervision, and examination while market-based regulation may be more appropriate for other types of crypto assets.

Crypto Assets

Policymakers should study the appropriate standards and oversight to address the risks presented by nonbank-issued crypto-assets and related activities to preserve financial stability and protect consumers, investors, and businesses worldwide. For example, policymakers should research the appropriate disclosures, and how the delivery of those disclosures would be most effective, of the activities (including rehypothecation) engaged in, risk management and corporate control functions to avoid fraud, affiliate transaction restrictions and other aspects of interconnectedness, and appropriate and effective BSA/AML requirements.

Stablecoins

It is important to define key terms and concepts related to “stablecoins.” We use the term “stablecoin” to refer to nonbank-issued stablecoins and not to tokenized or blockchain-based bank deposits. In general, a stablecoin issuer commits to sell its stablecoin, and redeem it on demand, at the coin’s par value and holds a designated pool of assets to “back” this commitment. The assets backing the stablecoin need to be available to, or prioritized for, the stablecoin holders who may want to redeem, and the assets cannot be subject to claims of others. The pool of assets should consist of safe, liquid assets, such as government securities (e.g., U.S. Treasury bills) and insured bank demand deposits, which could be used to meet many redemptions with high confidence. In practice, however, some of the assets currently held by some of the largest stablecoin issuers, which they refer to as their “reserves,” are in fact less liquid and riskier assets, like commercial paper and corporate bonds, and can thus present run risk if the viability of the issuer is called into question. Stablecoin arrangements differ from existing payments systems, which have meaningful regulatory and supervisory frameworks that apply.[23]

Current laws and regulations provide a strong framework for imposing safety and soundness requirements on banks when using novel technologies, such as DLT, to engage in deposit taking and other financial services.[24] There is no federal legal framework governing the issuance of stablecoins by nonbanks, however. Should such a framework for nonbank issuers be developed, it should be designed to promote a safe, healthy, and competitive U.S. stablecoin system and should prioritize the safety, soundness, and resiliency of the stablecoin issuer; the protection of consumers; the preservation of U.S. financial stability; the prevention of financial crimes and illicit finance; and the assurance that stablecoin issuers can be resolved in a safe and orderly way if they become troubled and fail. For example, regulators should study, at a minimum, the appropriate requirements related to: capital; liquidity requirements; reporting and auditing requirements; limitations on permissible activities (including lending and rehypothecation); redemption; counterparty risk; technological standards; usage; anti-money laundering, countering the financing of terrorism, and economic sanctions obligations; operational resilience and cybersecurity; and data privacy and security. Given the significant risks that could arise should nonbank stablecoin issuers and uninsured and non–federally regulated banks be

---

[23] *See, e.g.,* Bank Service Company Act, 12 U.S.C. § 1861, *et. seq*. It should be further noted that supervisory oversight may also extend to such payment systems as a consequence of the regulatory approval national banks may need in order to invest in them. *See* 12 C.F.R. § 5.36.

[24] *See* note 8, *supra.*

granted access to central bank reserves, they should not be given such access given the lack of sufficient controls and governance.[25]

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

As referenced previously, policymakers should research and establish a universal taxonomy for the digital asset ecosystem, standard setting rules for best practices, and the operational risk management and resiliency factors that make the banking industry able to adopt new DLT/blockchain technology consistent with banks' safe and sound operation. For example, banks can safely tokenize real-world assets that are already regulated and can be facilitated through transactions on the ledger. Policymakers also should investigate the potential implications and principles of interoperability between public and private blockchains. Additionally, policymakers should study other implications of using public blockchains, specifically regarding the underlying network governance, to help inform whether there may be potential for these networks to be used by banks.

Policymakers should also study how best to recognize and take actions to mitigate illicit finance risks associated with certain digital-asset transactions, which may include reduced transparency, disintermediation of financial institutions subject to AML and CFT obligations, increased complexity, and other risks.[26] The primary "illicit financing risks associated with virtual assets come from gaps in implementation of the international AML/CFT standards across countries; the use of anonymity-enhancing technologies; the lack of covered financial institutions as intermediaries—and thus the absence of AML/CFT controls—in some virtual asset transactions; and [virtual asset service providers ("VASPs")] that are non-compliant with AML/CFT and other regulatory obligations."[27] To mitigate these risks, policymakers should study how best to ensure that "international standards for the regulation and supervision of service providers associated with stablecoins and other digital assets [are] effectively implemented worldwide."[28] The Treasury Department should facilitate cross-border cooperation and other information sharing relating to the illicit finance risks of digital assets and digital-asset transactions. The requirements and expectations regarding AML and CFT activities should be consistent for all institutions that engage in equivalent activities with similar illicit finance risk characteristics, regardless of a particular entity's status as a bank, money services business, other type of institution, or the type of digital asset related activity.

---

[25] Some nonbank entities engaged in, or seeking to engage in, stablecoin issuance and entities with banking charters that do not have deposit insurance and are not subject to consolidated federal supervision have sought access to central bank reserves. Not limiting account access to appropriately regulated entities could pose significant risk to the U.S. financial system given the significant interconnections between the private sector and the central bank. Furthermore, if certain nonbank stablecoin issuers and other less-regulated entities were granted unfettered access to central bank reserves and they issued stablecoins backed fully by deposits at the central bank, those reserves could be perceived as the ultimate safe asset in times of economic or market stress and could lead to massive outflows of deposits in the banking system into that issuer's stablecoin, further exacerbating stress on the country's banks. There may be foreign policy effects that have not yet been entirely explored, and that should be researched further, should policymakers consider granting such entities access to the central bank.

[26] *See* U.S. Department of the Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets (Sept. 16, 2022) (link); *see also* Letter from Gregg Rozansky, BPI, to Jon Fishman, Assistant Director, Office of Strategic Policy, Terrorist Financing, and Financial Crimes, U.S. Department of the Treasury (Nov. 3, 2022) (link).

[27] *See* Action Plan to Address Illicit Financing Risks of Digital Assets at 4.

[28] *Id.*

Additionally, policymakers should research how new technologies could support further compliance with AML/CFT/KYC requirements. For example, BPI has previously expressed support for proposed legislation that would establish a federal task force to identify a digital ID implementation strategy across federal, state, and local governments in a way that is user friendly and accessible and that enhances security and preserves privacy.[29] Research also should be considered regarding how programmable money/tokens could support AML/CFT/sanctions compliance because the asset itself could be programmed for compliance and thus, to interact with the token, an entity would have to meet the compliance conditions of its programmed rules.

Other important areas of research that should be pursued include how to enable more sophisticated encryption – such as post quantum safe encryption and privacy-preserving encryption – that would help strengthen the safety and privacy of all digital asset projects, whether public or private. Such research also would build on federal expertise and initiatives on encryption (e.g., National Institute of Science and Technology, National Security Agency) and links with academia (e.g., Defense Advanced Research Projects Agency). Furthermore, there is currently a void in private research on the topic, making public sector research, potentially jointly with the private sector, even more critical.

4. R&D that should be prioritized for digital assets.

The RFI appears focused on research related to a U.S. CBDC. As we have previously and extensively detailed, an intermediated, account-based CBDC could pose serious risks to the U.S. economy and financial system that would not be outweighed by the purported benefits. By attracting deposits away from banks, particularly during a period of economic stress, a CBDC likely would undermine the commercial banking system in the United States, and severely constrict the availability of credit to the economy in a highly procyclical way.[30]

Many of the potential benefits cited by proponents of a CBDC are uncertain, and, moreover, many are mutually exclusive and thus could not be realized simultaneously.[31] Some proponents of a U.S. CBDC claim that a CBDC would make domestic and cross-border payments systems more efficient. While perhaps relevant in some countries, this rationale for a CBDC seems increasingly inapt in the United States, where The Clearing House's RTP real-time payment system, operational since 2017, continues to grow in use, consumers happily pay each other with Zelle or Venmo, and PayPal and Square are used widely. In addition, the Federal Reserve is nearing launch of its FedNow, further adding to the availability of faster payments options. Any research into the potential value of a CBDC in the U.S. should consider the private and public sector solutions available or under development and their ability to achieve the same potential benefits without some of the potential drawbacks discussed above.

---

[29] *See* BPI Press Release, "BPI Supports Senate Effort to Achieve Digital ID Benefits" (Sept. 28, 2022) (link). *See also* Letter from BPI et al. to Speaker Pelosi, Republican Leader McCarthy, Majority Leader Schumer, & Republican Leader McConnell (Nov. 18, 2022) (link) (supporting passage of the Improving Digital identity Act of 2022).

[30] Through an intermediated, account-based model, consumers would hold their CBDC at an account at a bank or other intermediary, similar to the way a trust bank holds a security for a customer. Any transfer of a dollar deposit from a commercial bank or credit union to a CBDC is a dollar unavailable for lending to businesses or consumers.

[31] For example, one of the most frequently cited reasons in support of a CBDC is that it would increase financial inclusion, yet we are unaware of any substantiated use case for CBDC that would benefit low- and moderate-income people in the United States.

Inefficiencies in the current cross-border system are to some extent attributable to regulation for AML/CFT purposes, which a CBDC would not reduce. Policymakers should research other initiatives and means to modernize the payments system, including other efforts that are underway to improve cross-border payments outside of any potential CBDC issuance, including use of blockchain by the banking sector as a more effective rail for cross-border payments.[32] Improving the existing cross-border payments system is a key priority of the FSB, which has devoted and indicated it will continue to devote significant resources to this effort. The Clearing House, EBA CLEARING, and SWIFT have executed a proof of concept and announced plans to launch by the end of this year an immediate cross-border (IXB) payments system; it is being designed with the contribution of 24 financial institutions.[33] Several wholesale CBDC pilots are underway globally, but it is too early to draw conclusions as to whether a wholesale CBDC could improve cross-border payments. Thus, further research is required before determining whether a wholesale CBDC could enhance cross-border payments' efficiency.[34]

Policymakers should continue to invest in open-source research and projects underway from NIST, including research on technical standards and guidance on the use of blockchain technology,[35] cryptographic techniques, particularly regarding threshold schemes that may be used in the future, such as Multi-Party Threshold Cryptography,[36] standards and requirements, such as Security Requirements for Cryptographic Modules.[37] Policymakers also should pursue research regarding (i) specific cybersecurity standards or approaches for interacting with permissionless/pubic blockchains and provide further guidance regarding NIST's cybersecurity framework used by most banks (ii) inter-operability blockchain standards for banks.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem.

Policymakers should research how new technologies can facilitate the creation of verifiable credentials, which are digital identity tools, which may be used to ensure that transactions conducted using new technologies are only executed with verified counterparties. Researchers should also study how the banking sector can safely use private and/or permissioned chains in light of the highly supervised and controlled environments in which they operate. As part of this effort, policymakers should study examples of use cases of private permissioned networks and hybrid models to help determine how banks can leverage those models in the highly regulated and supervised environments in which they operate. Further research should be pursued on the use of permissioned smart contracts where business rules are self-executing on the network.

---

[32] As noted previously, Partior is designed to perform atomic clearing and settlement on a 24x7 basis among participating institutions using blockchain and smart-contract technology.

[33] *See* John Adams, "Banks gearing up to test real-time payments across borders," *American Banker*, (May 2, 2022) (link). *See also* "EBA Clearing, SWIFT, and The Clearing House to deliver pilot service for immediate cross-border payments" (April 28, 2022) (link).

[34] If the Federal Reserve wished to assist in these and other efforts to modernize payments, it could finalize plans announced in 2018 to convert Fedwire to a 24/365 system.

[35] *See* NIST "Blockchain." (link).

[36] *See* NIST "Information Technology, Laboratory, Computer Security Resource Center: Multi-Party Threshold Cryptography MPTC" (link).

[37] *See* NIST "Information Technology, Laboratory, Computer Security Resource Center: FIPS 140-2, Security Requirements for Cryptographic Modules (link).

* * * * *

We thank you for your consideration and review of these comments. If you have any questions or wish to discuss this letter, please do not hesitate to contact us using the contact information provided below.

Very truly yours,

/s/ Paige Pidano Paridon
Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
Bank Policy Institute
[redacted]

/s/ Brooke Ybarra
Brooke Ybarra
Senior Vice President
American Bankers Association
[redacted]

Appendix – Descriptions of the Organizations

The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks, and the major foreign banks doing business in the U.S. Collectively, they employ almost two million Americans, make nearly half of the nation's bank-originated small business loans, and are an engine for financial innovation and economic growth.

The American Bankers Association is the voice of the nation's $23.6 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $19.2 trillion in deposits and extend $12.2 trillion in loans.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Carl E. Landwehr

RFI Response: Digital Assets R&D Agenda (late)

Carl Landwehr <[redacted]

To DARD-FTAC-RFI

Reply Reply All Forward ...

[redacted]

Follow up. Start by Wednesday, September 27, 2023. Due by Wednesday, September 27, 2023.

I apologize for missing the Friday March 3 deadline; I hope these comments, submitted March 5, 2023 may still be useful.
They address only item 4, R&D that should be prioritized for digital assets. They represent my personal view.
Sincerely,
—Carl E. Landwehr
==========

Digital assets, in the sense defined by this RFI, rely heavily on cryptographic algorithms and, even more so, on protocols that use those algorithms. NIST has organized international public competitions to develop cryptographic algorithms for a variety of purposes and assess their strength; choosing algorithms developed without this degree of public scrutiny in their development is in general unwise from a technical standpoint and would be even more unwise for digital asset systems. Cryptographic protocols used in the digital asset arena should be subject to a similar degree of public scrutiny and mathematical analysis before being adopted. Significant advances have been made in recent decades that support the formal statement of properties of such protocols and in proving mathematically that those properties hold for a particular protocol and its implementation.

While cryptographic protocols and algorithms are at the foundation of digital asset systems, it is important to recognize that digital asset schemes are indeed systems, and may have flaws and vulnerabilities at various levels, including at the hardware level. Most users of Bitcoin, for example, rely on third parties to hold their keys and other related data, and in several instances flaws in those third party systems have been exploited to steal assets. Research needs to address the engineering of those systems to avoid those flaws.

Fraud has also been a significant problem for digital asset systems. Engineering digital asset systems so that fraud is difficult to conceal should be a primary requirement. At the same time, privacy of user transactions must be maintained. Where there is warranted suspicion of fraud, technical means might be sought to lift the privacy veil, but this dance of accountability and privacy has proven extremely difficult to choreograph. A combination of technical and legal constraints will likely be required, and research into these areas in combination would be appropriate.

In addition, digital asset systems will be used by the general public, which needs to understand the systems not only well enough to use them, but to understand what justifies trust in them. Educating the public in this way can also pose research challenges.

These observations motivate the following recommendations for research thrusts related to digital assets:
1. Research that would lead to the statement of properties desired of digital asset systems and to rigorous proofs that protocols for these systems, correctly implemented, can deliver those properties.
2. Research that takes a systemic view of digital asset systems, looks for technical vulnerabilities in such systems, and finds ways to eliminate or mitigate them.
3. Research that builds accountability, as well as privacy, into digital asset systems in a controllable fashion.
4. Research that takes a human-centric view of the potential use and abuse of digital asset systems to understand the likely impacts of deployment.
5. Research that develops technically sound, but readily understood, models for digital asset systems and reveals to users what they are relying on when they trust these systems with their digital assets.
=============

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Cato Institute

March 3, 2023

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
Eisenhower Executive Office Building
[redacted]

Re: *Document Number: 2023-01534*
Request for Information; Digital Assets Research and Development

Dear Ms. Wallace:

My name is Jack Solowey, and I am a financial technology policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives. I appreciate the opportunity to comment on the Office of Science and Technology Policy's (OSTP's) Request for Information regarding Digital Assets Research and Development (RFI).[1] The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets, and peace, and the Center for Monetary and Financial Alternatives focuses on identifying, studying, and promoting alternatives to centralized, bureaucratic, and discretionary financial regulatory systems. The opinions I express here are my own.

The RFI posed several important questions regarding the research and development of digital assets to further responsible innovation in line with American values. This letter specifically addresses topics 1, 2, and 4.

* * *

1. Goals, sectors, or applications that could be improved with digital assets and related technologies.

Cryptographically secure software—including private cryptocurrencies and the distributed ledgers that enable them (crypto technology)—can not only be tools for enhanced financial infrastructure, but also for furthering democratic civil society.[2]

[1] Office of Science and Technology Policy, "Request for Information; Digital Assets Research and Development," 2023-01534, 88 FR 5043, January 26, 2023.
[2] The following summaries of a few key applications that can be enhanced by crypto technology should not be taken as an exhaustive survey.

Enhanced private financial infrastructure

At a basic level, cryptocurrencies enable faster transaction settlement times, allowing fund transfers to occur within minutes instead of days, as is typical of legacy payment rails.[3] In addition, cryptocurrencies facilitate borderless international payments.[4] While these benefits often are held out as either speculative or immaterial, with the charge leveled that cryptocurrencies serve no real-world function, their utility has been revealed in high-stakes situations where practicality is the primary criterion.

Within one month of Russia's invasion of Ukraine, crypto donations to Ukraine reached nearly $100 million.[5] Fast, cross-border settlement times were a critical part of cryptocurrencies' appeal. According to Ukraine's Deputy Minister of Digital Transformation, in the early days of the war, Ukraine's national bank was "not really operating" and crypto donations were "essential," due in no small part to "fast transfers" that got "results almost immediately."[6] Throughout the world—from Venezuela to Vietnam—cryptocurrencies have been valued for their utility as an alternative to deficient traditional financial institutions.[7]

Crypto transfers can work in the absence of a functioning central bank because they enable peer-to-peer transactions that settle directly on distributed public ledgers without necessary reliance on intermediaries.[8] These technologies also enable decentralized marketplaces for financial instruments, which mitigate by design the classic risks that financial intermediaries present to trustworthy asset custody and faithful trade execution.[9] Decentralized crypto exchanges (DEXs) allow users to self-custody their assets (i.e., control their holdings with their own private keys) and to arrange transactions with a series of smart contracts (i.e., software designed to self-execute when specific conditions are satisfied), mitigating risks of theft and fraud by middlemen.[10] As my colleague Jennifer Schulp has explained, "while DEXs do have human programmers, DEXs do not rely on a middleman keeping his word because they are composed of smart contracts that are open and auditable."[11]

---

[3] Nicholas Anthony, "Congress Should Welcome Cryptocurrency Competition," Cato Institute Briefing Paper no. 138, May 2, 2022.
[4] Nicholas Anthony, "What Do Cryptocurrencies Mean for Liberty?" *Cato at Liberty* (blog), Cato Institute, January 7, 2022.
[5] Illia Polosukhin, "How Cryptocurrency Is Helping Ukraine," *Wall Street Journal*, March 23, 2022.
[6] Id.
[7] Jennifer J. Schulp et al., "Overstating Crypto Crime Won't Lead to Sound Policy," *Cato at Liberty* (blog), Cato Institute, January 27, 2023.
[8] See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.
[9] See Jack Solowey and Jennifer J. Schulp, "What Congress Should Do about Crypto Exchanges," *Cato at Liberty* (blog), Cato Institute, December 15, 2022.
[10] Id.
[11] Jennifer J. Schulp, "Testimony Before the United States Senate Committee on Banking, Housing, and Urban Affairs Hearing on "Crypto Crash: Why the FTX Bubble Burst and the Harm to Consumers'," December 14, 2022.

Achieving financial policy goals of individual autonomy and data portability

In the United States, crypto technology already has made great strides toward achieving longstanding domestic policy goals. Since the passage of the Dodd-Frank Act in 2010, realizing "open-banking" goals (i.e., that consumers should have default access to their own financial transaction data) has been a U.S. policy objective.[12] Final rules on the subject are expected no sooner than 2024.[13] Recently, Consumer Financial Protection Bureau (CFPB) Director Rohit Chopra summarized well the goals of open banking and consumer financial data portability. These included "a decentralized, open ecosystem," a diminished ability for "incumbents to build moats and for middlemen to serve as gatekeepers," that no one person or entity "'owns' critical infrastructure," and achieving "more seamless integration."[14]

These very priorities describe some of the core capabilities of decentralized finance (DeFi) enabled by crypto technology.[15] Cryptocurrencies are natively decentralized, with transactions not recorded by trusted intermediaries but by a global network of computers incentivized to validate a cryptographically secure distributed ledger (a blockchain).[16] Cryptocurrencies are permissionless, with users free to self-custody their assets and access their complete, pseudonymous transaction histories without relying on middlemen.[17] Financial rails based on open-source, decentralized software protocols are perhaps the first true alternative to critical financial infrastructure being "owned" by one person or entity.[18] Lastly, crypto projects are composable, as open-source software allows protocols and applications to be more readily interoperable.[19]

Furthering democratic civil society

These same features and capabilities not only serve to further U.S. financial policy goals, but also democratic civil society at home and abroad.[20] The permissionless, pseudonymous, and censorship resistant properties of blockchains make them strong tools for securely recording information essential to civic life. For example, when law enforcement pressured the pro-democracy *Apple Daily* newspaper in Hong Kong to shutter in connection with the Chinese Communist Party's application of an authoritarian "national security law," private individuals

---

[12] 12 U.S.C. § 5533. See also Jack Solowey, "A Tale of Two Documents: How the Bitcoin White Paper Outperformed Dodd-Frank," *Cato at Liberty* (blog), Cato Institute, November 4, 2022.
[13] Rohit Chopra, "Director Chopra's Prepared Remarks at Money 20/20," Consumer Financial Protection Bureau, October 25, 2022.
[14] Id.
[15] Jack Solowey, "A Tale of Two Documents: How the Bitcoin White Paper Outperformed Dodd-Frank," *Cato at Liberty* (blog), Cato Institute, November 4, 2022. See also Jack Solowey, "Crypto's Useful Future Was Vivified By the Correction," *RealClearMarkets*, August 23, 2022.
[16] Id.
[17] Id.
[18] Id.
[19] Id.
[20] Jack Solowey, "America, Don't Be the Anti-Network State: Crypto Policy for the Leader of the Free World," *Cato at Liberty* (blog), Cato Institute, December 22, 2022.

were able to backup archives of the journalistic outlet using secure blockchain technology.[21] In the U.S., blockchain technology has been leveraged to preserve the testimony of genocide survivors.[22] Critically, the RFI asks how a digital asset ecosystem can both embody and further democratic values. The answer is through private crypto technology that supports the preservation of vital political and historical speech, expression, and witness.

2. Goals, sectors, or applications where digital assets introduce risks or harms.

Private sector innovation can address cybersecurity risks

No technology is perfect, and it is unwise to ignore software vulnerabilities generally. While the cryptographically secure distributed ledgers at the heart of cryptocurrencies, such as the Bitcoin blockchain, have historically resisted hacking, aspects of the crypto ecosystem such as bridges (for communicating across blockchains) and smart contracts (as described above) have been vulnerable to attack.[23] Crypto technologies do not "introduce" these risks so much as, like other networked software, experience them to varying degrees.

The question then is how to address or mitigate these risks. Here, the crypto ecosystem has native resiliencies that should be embraced, not thwarted. The permissionless and composable qualities of open-source software can support ongoing iterative improvements and the dissemination and adoption of best practices.[24] Moreover, the public nature of crypto protocols makes them auditable by design, facilitating threat detection and identification of patchable vulnerabilities. Therefore, diminishing the speed of the iteration cycle and the default openness of the U.S. crypto ecosystem (e.g., through prescriptive regulations that create prior restraint, or regulation by enforcement that nudges innovation in crypto technology out of the U.S.) also can diminish the development of cybersecurity safeguards in the U.S.

Central Bank Digital Currencies are not compatible with a free and democratic society

The risks that Central Bank Digital Currencies (CBDCs) present to a free and democratic society vastly exceed any potential benefits. A CBDC (i.e., a digital national currency that is a direct liability of the Federal Reserve) should not be developed in the United States.[25]

[21] Pak Yiu, "Hong Kong's Apple Daily to live on in blockchain, free of censors," *Reuters*, June 24, 2021. See also Javier C. Hernández, "Harsh Penalties, Vaguely Defined Crimes: Hong Kong's Security Law Explained," *New York Times*, June 30, 2020.

[22] "Starling Lab: Establishing Trust for Humanity's Data," Filecoin, June 10, 2021.

[23] Jack Solowey, "Dissent Is a Part of Crypto," *Cato at Liberty* (blog), Cato Institute, August 19, 2022 citing Is Bitcoin secure? Has this network ever been hacked?" Coinbase, last visited March 2, 2023. See also "Blockchain bridges," Ethereum, last updated March 1, 2023; "Introduction to Smart Contracts," Ethereum, last updated September 1, 2022; and Corin Faife, "Nomad crypto bridge loses $200 million in 'chaotic' hack," *The Verge*, August 2, 2022.

[24] Jack Solowey, "Dissent Is a Part of Crypto," *Cato at Liberty* (blog), Cato Institute, August 19, 2022 citing Sonal Chokshi et al., "Bridge Hack, Wallet Hack," *Web3 with a16z* (podcast), August 11, 2022.

[25] Nicholas Anthony and Norbert Michel, "Central Bank Digital Currency," Cato Institute Briefing Paper no. 145, January 10, 2023.

As my colleagues Norbert Michel and Nicholas Anthony explain, the purported benefits of a CBDC are outweighed by serious risks across several areas of concern: financial inclusion, faster payments, the dollar's status as the global reserve currency, monetary and fiscal policy, financial privacy, financial freedom, private enterprise, and cybersecurity.

With respect to financial inclusion, a CBDC would not resolve, and would risk exacerbating, the privacy and trust concerns that lead some Americans to eschew bank accounts.[26] A CBDC also would provide no unique advantage in faster payments over existing private financial technology solutions, such as stablecoins or the Real-Time Payments (RTP) Network.[27] Moreover, the dollar's reserve currency status is due to the strength of the U.S. economy, rule of law, and property rights; another central bank merely deploying a CBDC while the Federal Reserve refrains from doing so is unlikely to jeopardize the dollar's reserve currency status, particularly where those other central banks are in jurisdictions with weak or nonexistent legal protections.[28]

That the central bank could use a CBDC to impose negative interest rates or penalize savings is a threat to financial autonomy and property rights.[29] In addition, a CBDC would risk undermining retail banking, both by limiting private banks' ability to extend credit due to decreased consumer deposits, as well as by creating run risks where a CBDC serves as a substitute for private banks during times of stress.[30] What's more, a CBDC would be a prominent target for hackers, and a single federal database would pose even greater cybersecurity risk than would the potential breach of a private financial institution with limited market share.[31]

A CBDC would further erode Americans' limited financial privacy, giving the federal government direct visibility into Americans' financial lives. In addition to Orwellian surveillance risk, a CBDC would provide the federal government with "countless opportunities . . . to control citizens' financial transactions," risking levels of control over private economic and civic life that are fundamentally incompatible with a liberal democratic society.[32]

4. R&D that should be prioritized for digital assets.

This letter identifies research areas worth the attention and consideration of the OSTP to support the Office's advisory mission in light of the whole-of-government approach to digital

---

[26] Id. at 2, citing Federal Deposit Insurance Corporation, "2021 FDIC National Survey of Unbanked Households," October 2022.
[27] Id. at 2.
[28] Id. at 2 citing Christopher Waller, "The U.S. Dollar and Central Bank Digital Currencies," Board of Governors of the Federal Reserve System, October 14, 2022.
[29] See Id. at 2-3.
[30] Id. at 3 citing Lael Brainard, "Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?," Board of Governors of the Federal Reserve System, May 15, 2018.
[31] Id. at 3.
[32] Id. at 3.

assets underway pursuant to Executive Order 14067, "Ensuring Responsible Development of Digital Assets."[33] The research priorities included in this response are not intended to be exhaustive, nor should they be construed as support for taxpayer-subsidized risk taking. To the contrary, the techniques and applications discussed below already have been advanced through private research and development.[34] Consistent with OSTP's mission, the Office should explore these areas by engaging with external partners—in both the for-profit and non-profit sectors—in a learning capacity in order to be able to advise the President and the Executive Office of the President on risk-based digital asset policy. Lastly, the OSTP should bear in mind the inherent unpredictability of disruptive innovations before drawing firm conclusions on the ultimate course of the crypto ecosystem's evolution.[35]

Zero-knowledge technologies

The RFI identifies zero-knowledge (ZK) proofs as a potential privacy-enhancing technology (PET). ZK proofs are indeed critical to the advancement of PET research and development. In addition, the OSTP should consider the potential of ZK proofs and related technologies to further additional goals of the crypto ecosystem: disintermediation, democratization of infrastructure governance, and financial inclusion.

ZK proofs enable a party (the prover) to prove the validity or truth of a statement to an additional party (the verifier) without having to disclose further information beyond that the statement itself is true.[36] Such "statements" can include that the prover is in possession of certain knowledge (e.g., personally identifying information (PII), a credential, or private key), which in turn can be used to verify the prover's identity without requiring the disclosure of specific PII to the verifier. Here, the potential of ZK proofs as a PET are on full display, as an individual can prove his or her identity, or an aspect of thereof, without having to reveal more PII than necessary, helping to mitigate both privacy and security risks. A common demonstrative example is that ZK proofs would enable an individual to prove that his or her age meets or exceeds a relevant threshold (e.g., voting age) without having to reveal one's exact date of birth to the verifier.

ZK proofs' ability to verify statements without revealing those statements' contents also can help to improve the scalability and overall decentralization of crypto networks. In essence, the statement that a ZK proof would be validating in that context is the proper execution and recording of a transaction over a cryptocurrency network (e.g., that a cryptocurrency transfer

[33] Executive Office of the President, "Ensuring Responsible Development of Digital Assets," E.O. 14067, 2022-05471, 87 FR 14143, March 14, 2022.

[34] See "What are zero-knowledge proofs?" Ethereum, March 1, 2023; and Colin Harper, "Multisignature Wallets Can Keep Your Coins Safer (If You Use Them Right)," *CoinDesk*, November 10, 2020.

[35] See Jack Solowey, "Don't Push Crypto Offshore, Don't Outlaw Disruptive Innovation," *Cato at Liberty* (blog), Cato Institute, February 24, 2023.

[36] "What are zero-knowledge proofs?" Ethereum, March 1, 2023; and Glossary: Zero-Knowledge Proof, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, last visited March 2, 2023.

has not involved double spending of the same tokens).[37] This can improve a crypto network's scalability in multiple ways.

For example, such proofs can be leveraged to process verifiable transactions using computing resources beyond the nodes composing primary (i.e., layer 1) blockchains, improving throughput while providing a method to validate transactions' legitimacy before they are recorded to those layer 1 blockchains.[38] In addition, ZK technology and related cryptography can enable the further development and adoption of light clients—crypto network nodes that are less capital and resource intensive.[39] While designs vary, light clients can verify transaction records without needing to download or store complete copies of a blockchain, as a full node would.[40]

The OSTP wisely prioritizes the advancement of democratic values and financial inclusion in its RFI. Crypto network scaling and light client solutions enabled by ZK technology could support both priorities. Increased transaction processing capacity directly addresses a core critique of crypto networks: that they have limited ability to process large numbers of transactions per second.[41] The benefits of crypto payments and DeFi—as discussed in response to topic 1 above—can become more widely available where those constraints are overcome.

Similarly, light clients have the potential to open participation in crypto networks to a broader group of individuals by making the ability to run a node less capital intensive. Light clients could help nodes run on ubiquitous consumer-grade devices, like notebooks, tablets, and smartphones, as opposed to hardware requiring specialized Graphics Processing Units (GPUs) and Application-Specific Integrated Circuits (ASICs) that support certain full nodes.[42] Not only would this have financial inclusion benefits, but also could serve to further democratize participation in network design, as more individuals from more diverse backgrounds became able to choose the software clients on a crypto network.[43]

In terms of advancing U.S. competitiveness and leadership, light clients are just one example of crypto technologies devolving infrastructure decisions to network edges. Where global adoption of decentralized software protocols continues apace, those concerned with seeing U.S. interests represented in the architecture of global financial infrastructure should be wary

---

[37] See Zero-Knowledge Rollups: Validity proofs, Ethereum, last updated January 23, 2023.

[38] "What are zero-knowledge proofs? Verifiable computation," Ethereum, last updated March 1, 2023.

[39] See "Nodes and Clients: Light node," Ethereum, last updated February 3, 2023. See also Polygon, "How Zero Knowledge Proofs, Aggregation Layers, and Light Nodes Can Improve Web3 Experience and Structure?," *Medium*, November 23, 2022.

[40] Id. See also, Vitalik Buterin, "Re: My first impressions of web3," Reddit, January 8, 2022; and Etan Kissling, "Light Clients After the Merge," Devcon Archive (video), October 14, 2022.

[41] "Scaling," Ethereum, last updated January 5, 2023.

[42] See "Blockchain client types," Coinbase, January 26, 2022. See also "Nodes and Clients: Light node," Ethereum, last updated February 3, 2023; and Polygon, "How Zero Knowledge Proofs, Aggregation Layers, and Light Nodes Can Improve Web3 Experience and Structure?," *Medium*, November 23, 2022.

[43] Jack Solowey, "Don't Push Crypto Offshore, Don't Outlaw Disruptive Innovation," *Cato at Liberty* (blog), Cato Institute, February 24, 2023.

of the risks of an unfavorable regulatory climate nudging crypto activity offshore. Americans being represented in the governance of crypto networks requires crypto policy that allows Americans to participate—as entrepreneurs, developers, and users—in those very same crypto networks.[44]

Multi-signature technologies

The RFI aptly identifies the importance of digital asset security. The OSTP should consider the ability of multi-signature arrangements to enhance security in the crypto ecosystem. This includes risks related to digital asset holdings, as well as to unauthorized modifications of protocol software.

Multi-signature (or multisig) methods help to secure crypto transactions and networks by requiring that two or more private key holders sign crypto transactions before they are executed or authorize access to crypto wallets or smart contracts.[45] These methods can be readily analogized to those for securing physical facilities, like vaults, with locks that require multiple different keys held by multiple different parties to permit access. Whether it's physical keys unlocking a vault made of steel-reinforced concrete, or private keys for signing crypto transactions, dispersing keys to multiple holders helps to reduce the risks of unauthorized access or tampering. In the software context, multisig arrangements can be set with different parameters. For example, two out of three private keys may be required to sign a transaction, which mitigates risks from unauthorized access, as well as from a lost key resulting in permanent asset loss.

Multisig methods also can be used to support different use cases within the crypto ecosystem. Gating a crypto wallet with multiple keys can enable a form of secure account recovery. On a broader scale, similar arrangements can be used to support secure crypto asset custody by centralized crypto exchanges, helping to guard customer assets against the types of risks exemplified by the mismanagement of FTX.[46] In addition, multiple signatures can be required before deploying upgrades to a crypto network's core code, which can not only help to prevent malicious activity but also to formalize governance procedures of decentralized projects, imposing limits on discretionary changes.

* * *

[44] Id.

[45] See Colin Harper, "Multisignature Wallets Can Keep Your Coins Safer (If You Use Them Right)," *CoinDesk*, November 10, 2020.

[46] See Jack Solowey and Jennifer Schulp, "Don't punish crypto for the sins of SBF's FTX," *New York Daily News*, November 29, 2022.

Thank you for the opportunity to comment on a national digital assets research and development agenda. I am happy to answer any questions or further engage on this topic.

Sincerely,

[redacted]

Jack Solowey
Financial Technology Policy Analyst
Center for Monetary and Financial Alternatives
Cato Institute

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Central Bank Digital Currency (CBDC)

Safety through Accountability:
Security and Privacy for Central Bank Digital Currency

Giulia Fanti (Carnegie Mellon University, Academic Institution)
Pramod Viswanath (Princeton University, Academic Institution)

This response addresses primarily questions (4) *Research and Development that should be prioritized for digital assets* and (3) *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets*.

1 Introduction

Today, over 105 central banks worldwide representing 95% of the global gross domestic product are actively exploring the deployment of a *central bank digital currency* (CBDC) [8]. A CBDC is central bank money that is (a) *digital* in nature, and (b) a liability of a *central bank*. Retail CBDCs have an additional requirement that they should be (c) *widely accessible to the public* [16]. In contrast, today there are two types of central bank money: cash, which is widely accessible but not digital, and balances on the central bank's ledger, which are digital, but are available only to select financial institutions.

Some of the potential benefits of CBDCs include greater flexibility in implementing monetary policy, improved financial inclusion (by providing direct access to central bank money at reduced risk of default), and more efficient money transfers at lower fees (by removing middlemen) [5, 6]. In banking circles, CBDCs are viewed by some as an "inevitable" step in the evolution of money [22]. In the United States, the Federal Reserve is currently in an exploratory stage, in which they are exploring the feasibility of a Digital Dollar [16].

In parallel with the momentum surrounding CBDCs is a growing fear that CBDCs will significantly increase the attack surface for the financial system at large. Central bankers are worried that CBDC will reduce their ability to prevent malicious actors from using and abusing central bank money. In fact, this has been cited by central bankers themselves as a reason not to implement a CBDC at all [21, 17]. In parallel, users are worried that a CBDC will increase the likelihood of sweeping privacy violations, both by the central bank and by third-party attackers [1]. Based on these core concerns, our premise (and the central thesis in this document) is the following:

> The study of methods for securing the many components of a CBDC, as well as convincing stakeholders (e.g., auditors, the broader public) that its algorithms and implementation are secure and privacy-preserving are an important component of a federal research agenda on digital currencies. Further, bringing *accountability*, the ability to determine the identity of malicious actors (with cryptographic evidence), across the CBDC stack is a crucial building block towards this broad goal.

1.1 The CBDC Stack

To understand the security and privacy concerns associated with a CBDC, it is helpful to first understand how a hypothetical CBDC might be structured. Although there is no consensus on the best design for a CBDC, most existing designs have a consistent *stack*, or architecture. This stack can be thought of in layers (much like the well-studied networking stack), where each layer corresponds to a different component of the system. As we move up the stack, components operate at an increasingly broad level of abstraction. Moving from bottom to top, we have the following layers:

Hardware A CBDC will require hardware to run the payment processing functionality, both on user devices and on the backend. It is unclear at this point if CBDCs will require custom hardware, or if they will run exclusively on commodity off-the-shelf (COTS) hardware. For instance, CBDCs will almost certainly not use consensus protocols from the cryptocurrency space like Nakamoto consensus (see Consensus layer) [15], which resulted in the development of custom hardware like application specific integrated circuits (ASICs) tailored for proof-of-work. At the same time, there have been discussions of using trusted computing to handle certain components of CBDC transactions, including offline payments. While many phones today come equipped with trusted hardware modules, it is plausible that as mobile payments become ubiquitous, we may require custom hardware to accelerate (and/or secure) certain functionalities.

Security and Privacy Risks: The primary hardware risks typically stem from unintended or unknown functionality, which can lead to data exfiltration or on-device manipulation. For example, if an adversary can indirectly manipulate some bits on a chip [14], they may be able to impact the correctness of the CBDC, particularly if a CBDC is running on shared infrastructure (e.g., cloud). Alternatively, an adversary may be able to infer access patterns to data using subtle side-channel attacks [20].

Consensus layer The consensus layer is responsible for processing and confirming transactions. This layer must ensure that user transactions are committed to the CBDC ledger(s) in a timely and correct fashion. There have been different algorithms and implementations proposed for this consensus layer. However, every algorithm we have seen has relied on some kind of *fault tolerance* over a distributed system. That is, on the back end, they require multiple servers to collectively maintain the state of the CBDC, while running a so-called consensus algorithm to ensure that the different servers all agree on the ledger.

Roughly, consensus algorithms can provide two types of fault tolerance: crash fault tolerance and Byzantine fault tolerance. Crash fault tolerant algorithms are able to withstand some of the distributed servers crashing, e.g., due to a power failure. Byzantine fault tolerance is a stronger condition, and can tolerate some of the distributed servers actively trying to break the consensus of the great. Both types of fault tolerance have been considered for CBDCs, and both have different tradeoffs. For instance, while Byzantine fault tolerant protocols provide stronger security guarantees, they are also less efficient than crash fault tolerant protocols.

Security and Privacy Risks. The primary security risk is that one or more malicious components may be able to double-spend funds, or otherwise compromise the integrity of the CBDC ledger. While Byzantine fault tolerant protocols protect against this, crash fault tolerant protocols do not (and they are the more common choice for implementing CBDCs [1, 13]).

A central privacy risk is that by processing user transactions centrally, the central bank aggregates massive quantities of user financial data. The predominant approach for circumventing this risk is to adopt a so-called *hybrid architecture*, in which the central bank outsources day-to-day activity to private banks, as is done today with private bank money [2]. However, at the end of the day, if the tokens are a direct liability of the central bank, they must have access to the ledger to confirm its state, and their own liabilities. The Bank of International Settlements suggests that this could occur via periodic synchronizations of private ledgers with the central bank [2].

Application layer Applications, or *smart contracts*, run atop the consensus layer. It is unclear today exactly what smart contracts will be run on a CBDC; there is some evidence that central bankers prefer not to provide full programmability, as is available in cryptocurrencies like Ethereum. Nonetheless, there will be at least some applications running atop the consensus layer, such as basic payments smart contracts.

Security and Privacy Risks. The cryptocurrency space has vividly demonstrated the potential dangers of insecure smart contracts [19]. If CBDC applications are not written securely, there is a very real risk of malicious actors stealing funds by exploiting vulnerabilities in the program. The danger is that CBDC applications are directly tied to financial transfer, so any attacks have an elevated risk of leading to direct and significant financial losses. Similar risks also stem from end user applications, e.g., mobile wallets; these risks are more similar to existing application security concerns.

On the privacy front, the risks are in many ways similar to the existing mobile application ecosystem. Applications may over-collect user data, and use it for purposes that are unrelated to the scope of the service they are providing [12].

User layer This layer consists of the users themselves, and the ways in which they utilize a CBDC.

Security Risks. The primary security risk with respect to users is that of fraudulent use: users may try to engage in illegal practices, such as money laundering or financing terrorism. This is typically countered with compliance checks and reporting. For example, in the U.S., any receipient of over $10,000 in cash "in a single transaction or related transactions" must report this transaction to the Internal Revenue Service [10]. Today, compliance is handled by controls from private financial institutions and audits from the IRS. Such controls and audits could be more complicated to implement in a CBDC due to proposed privacy mechanisms (e.g., encrypted transactions) [4, 23, 11].

Onboarding layer The final "layer" (used loosely) consists of the processes for gaining account access to a CBDC. This process is expected to be outsourced to third-party entities (e.g., private banks) [2]. For example, current trends suggest that a Digital Dollar would be identity-verified [16]. It is unclear what level of identity verification will be required, ranging from biometrics collection to presenting previously-issued ID.

Security and Privacy Risks. The onboarding process introduces a delicate tradeoff between access and security. Strict onboarding controls can ensure that unqualified indviduals are not permitted to participate, at the expense of excluding qualified individuals without the requisite documentation (e.g., no ID). These risks are particularly significant for communities in which ID possession is low. At the same time, lax onboarding controls can improve access to the CBDC, while increasing the risk of fraudulent account creation.

2 Suggested Research Agenda

If the U.S. decides to deploy a CBDC, it must be able to provide security and privacy assurances to various stakeholders: central banks, operators, and users, to name a few. Indeed, these assurances are important even if the U.S. does *not* deploy a CBDC, given that many other countries worldwide have deployed CBDCs, whose operations could affect U.S. citizens and residents. However, the "best" mechanism for providing these assurances is not known in the computer science community today. We argue that a research agenda on central bank digital currency must include the study of **security and privacy in CBDCs**, with a focus not just on protecting against attacks, but also responding to existing attacks, and also providing assurances of accountability to stakeholders.

For example, despite touching different layers of the CBDC stack, these problems could all benefit from a single, unifying *accountability* framework. That is, in CBDCs—as well as other digital systems with many conflicting constraints and requirements—"online" security checks are not always practical or necessary. We note in passing that an alternative annd complementary approach, which we believe merits additional exploration, is to design systems that do not enforce correctness online, but can be easily and efficiently *audited* post hoc.

2.1 A unifying accountability framework

As shown in Figure 1, consider a set of distributed agents or users $U = \{u_1, \ldots, u_n\}$ that participate in a system (e.g., agents could represent server replicas that are jointly validating transactions for a CBDC ledger, or users who submit transactions to a CBDC). Some of these agents may be corrupt. The system observes an arrival process $\{e_i\}_{i\geq 0}$ of events (e.g. transactions submitted for confirmation). We assume that each event e_i is associated with a set C_i of security and/or privacy checks, which must be conducted to ensure that the event is valid. For example, in a transaction processing module, C_i could include signature checks, transaction validity checks, and checks to ensure that different replicas in the ledger's distributed datastore have consistent views of the ledger.

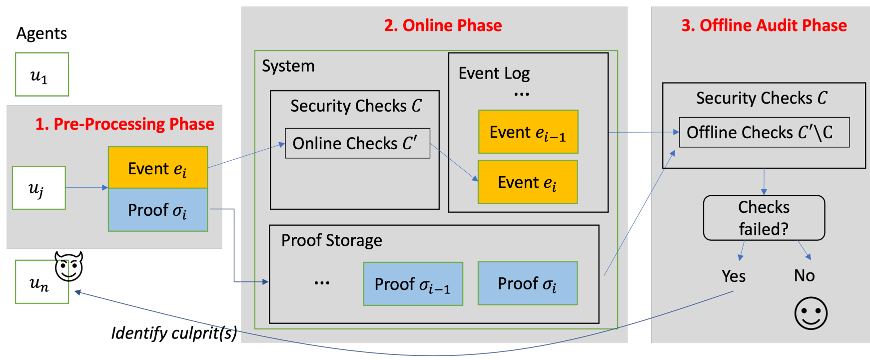


Figure 1: A three-phase accountability framework.

This accountability framework involves three phases, illustrated in Figure 1.

1. *Pre-Processing:* In the pre-processing phase, a user generates an event e_i, followed by a corresponding audit proof σ_i. σ_i can prove a statement about one or more events (e.g., a user's last 10 events).

2. *Online Processing:* In the online phase, the system executes incoming tasks e_i. During this phase, the system checks a subset $C_i' \subseteq C_i$ of the required security checks. In addition, it collects corresponding audit proofs (if applicable) σ_i from one or more agents, which can be used in the offline phase.

3. *Offline Failure Audit:* This phase occurs periodically at intervals set by the system operator. The failure audit algorithm $\mathcal{A}$ checks all observed audit metadata $\{\sigma_j\}_{j\geq 0}$ and the current state of the system to determine if there has been any violation of the security conditions that were not checked online, namely $C_j \setminus C_j'$ for all $j \leq i_t$. If the failure audit indicates that there *has* been a failure, it then runs an additional algorithm $\mathcal{F}$, which outputs a set $U' \subset U$ of part(ies) responsible for the failure.

The above framework is general enough to encompass a variety of different problems. However, today we lack the algorithms and technical tools to *instantiate* such an accountability framework for CBDCs. We believe there is a pressing need to develop the algorithms, analysis, and implementations needed to provide security and privacy assurances for a potential U.S. CBDC.

In particular:

We recommend prioritizing research and development into tools that can provide auditability and accountability for CBDCs.

Three common design challenges arise.

1. **Accountability proof structures:** We must design data structures σ_i that can depend on the event e_i, the system's response to e_i, and all history visible to the agent. σ_i enables the system to (a) identify past faults, (b) attribute faults to the responsible party, and (c) compute the audit proof efficiently in the online phase.

2. **Global correctness checks:** We must design the failure audit algorithm $\mathcal{A}(\{\sigma_j\}_{j\leq i_t}, s_t)$ that efficiently identifies whether there has been any failure.

3. **Fault attribution checks:** We must design an algorithm $\mathcal{F}(\{\sigma_j\}_{j\leq i_t}, s_t) \rightarrow A$ such that if the failure audit check fails (i.e., it identifies a failure), $\mathcal{F}$ returns the responsible agent(s) $U' \subset U$.

2.2 Full-Stack Accountability Challenges

Accountability and auditability are necessary at every layer of the CBDC stack—we saw some examples at the beginning of this manuscript. However, different layers of the stack will require different technical tools and techniques to reach these goals. A federal research program on digital assets should prioritize accountability and auditability *across the CBDC stack*. This will require research that is convergent, relying on disciplines ranging from device hardware to algorithms to cryptography to sociology.

Next, we will summarize some relevant research questions at each layer of the CBDC stack.

Onboarding layer. From a user's perspective, their first interaction with a CBDC is when they are onboarded—that is, when they receive an account. Relevant questions include how to design inclusive onboarding procedures to maximize access by residents to a potential CBDC, while also designing post hoc audit mechanisms to ensure that users are not incorrectly given accounts, or that legitimate users are not using their accounts to perpetuate money laundering. Many of these problems overlap with challenges associated with the design and implementation of digital ID systems.

User Layer. At the user layer, a major concern for CBDC operators is in accountability regarding compliance of user transactions. This becomes particularly challenging when combined with proposed privacy-preserving (e.g., encrypted) designs. A central question in this area is, "How can we provide flexible and efficient compliance checks without compromising either user privacy or system efficiency?" Today, we have answers to a very basic subset of problems in this area; for example, we can do basic checks over encrypted transactions to understand if they are within a range [7]. If CBDCs are to meaningfully protect user privacy, we require mechanisms for checking flexible and diverse compliance policies, across multiple transactions and/or multiple users, over protected (e.g., encrypted) transaction data.

Application Layer. The application layer is essential for a CBDC as the interface between the software and the end user. Because of this, it is particularly susceptible to malicious inputs from users. Indeed, in the cryptocurrency space, vulnerabilities in smart contracts have led to staggering financial losses [20]. Here, there is a need to audit smart contracts for the presence of logical or implementation errors that can be exploited for financial gain. Relevant tools can include formal methods (e.g., model checking) as well as machine learning and/or game theoretic techniques to analyze errors in algorithms or incentive mechanisms deployed in smart contracts [9, 3].

Consensus Layer. The core engine of any CBDC is its consensus layer, which governs the commitment and security of transactions. We need high-performance audit mechanisms for providing accountability at the consensus layer without harming performance. That is, if a validator node for a CBDC ledger misbehaves, can we attribute faults to the responsible party? Preliminary work has studied this problem [18], but only in a very restricted setting. Perhaps for this reason, existing CBDC pilots do not utilize (or even mention) the accountability implications or requirements of consensus protocols. We believe this is an important requirement for future CBDCs (and digital currencies more broadly).

Hardware Layer. If deployed, CBDCs would be a form of critical infrastructure. As such, we need to be able to audit hardware components in a CBDC—that is, the building blocks of this critical infrastructure. Examples of relevant security problems include ensuring that a device is not maliciously exfiltrating data, e.g. private keys, through side channels. If it is, we need to be able to determine which components of which device(s) are responsible. Note that this is a much broader question that is not specific to CBDCs or digital currencies. However it is a critically important issue in that context.

References cited

[1] Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, and Andrew Miller. Design choices for central bank digital currency: Policy and technical considerations. *National Bureau of Economic Research*, 2020.

[2] Raphael Auer and Rainer Böhme. The technology of retail central bank digital currency. *BIS Quarterly Review, March*, 2020.

[3] Kushal Babel, Philip Daian, Mahimna Kelkar, and Ari Juels. Clockwork finance: Automated analysis of economic security in smart contracts. *arXiv preprint arXiv:2109.04347*, 2021.

[4] European Central Bank. Eurosystem report on the public consultation on a digital euro, 2021.

[5] Ulrich Bindseil. Central bank digital currency: Financial system implications and control. *International Journal of Political Economy*, 48(4):303–335, 2019.

[6] Michael D Bordo and Andrew T Levin. Central bank digital currency and the future of monetary policy. Technical report, National Bureau of Economic Research, 2017.

[7] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE symposium on security and privacy (SP)*, pages 315–334. IEEE, 2018.

[8] Giulia Fanti, Kari Kostiainen, William Howlett, Josh Lipsky, Ole Moehr, John Paul Schnapper-Casteras, and Josephine Wolff. Missing key: The challenge of cybersecurity and central bank digital currency. Atlantic Council, 2022.

[9] Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramer, Giulia Fanti, and Ari Juels. Squirrl: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning. *arXiv preprint arXiv:1912.01798*, 2019.

[10] IRS. Report of cash payments over $10,000 received in a trade or business - motor vehicle dealership q&as. `https://www.irs.gov/businesses/small-businesses-self-employed/report-of-cash-payments-over-10000-received-in-a-trade-or-business-motor-vehic` Accessed on December 30, 2022.

[11] Aggelos Kiayias, Markulf Kohlweiss, and Amirreza Sarencheh. Peredi: Privacy-enhanced, regulated and distributed central bank digital currencies. *Cryptology ePrint Archive*, 2022.

[12] Urvashi Kishnani, Naheem Noah, Sanchari Das, and Rinku Dewri. Privacy and security evaluation of mobile payment applications through user-generated reviews. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, pages 159–173, 2022.

[13] James Lovejoy, Cory Fields, Madars Virza, Tyler Frederick, David Urness, Kevin Karwaski, Anders Brownworth, and Neha Narula. A high performance payment processing system designed for central bank digital currencies. *Cryptology ePrint Archive*, 2022.

[14] Onur Mutlu and Jeremie S Kim. Rowhammer: A retrospective. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(8):1555–1571, 2019.

[15] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[16] Board of Governors of the Federal Reserve System. Money and payments: The u.s.dollar in the age of digital transformation. 2022.

[17] United Kingdom House of Lords. Central bank digital currencies: a solution in search of a problem?, January 2022.

[18] Peiyao Sheng, Gerui Wang, Kartik Nayak, Sreeram Kannan, and Pramod Viswanath. Bft protocol forensics. In *Proceedings of the 2021 ACM SIGSAC conference on computer and communications security*, pages 1722–1743, 2021.

[19] Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Buenzli, and Martin Vechev. Securify: Practical security analysis of smart contracts. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 67–82, 2018.

[20] Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen, Arthur Gervais, Bünzli, and Martin Vechev. Securify: Practical security analysis of smart contracts. *USENIX Security*, 2020.

[21] Mayra Rodriguez Valladares. What is federal reserve chair jerome powell's biggest worry? *Forbes*, 2021.

[22] Keira Wright. Bank of America says stablecoin adoption and CBDC is 'inevitable'. *CoinTelegraph*, January 2022.

[23] Karl Wüst, Kari Kostiainen, and Srdjan Capkun. Platypus: A central bank digital currency with unlinkable transactions and privacy preserving regulation. *Cryptology ePrint Archive*, 2021.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Crypto Council for Innovation (CCI)

Crypto Council for Innovation

March 3, 2023

Dr. Arati Prabhakar
Director, Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

Re: Request for Information regarding Digital Assets Research and Development, 88 FR 5043

Dear Dr. Prabhakar:

The Crypto Council for Innovation ("CCI") submits this letter in response to a request for information regarding Digital Assets Research and Development, 88 FR 5043.[1] CCI appreciates the opportunity to share its information, expertise, and views on this vital issue. Digital assets represent one of the most significant innovations in finance—and beyond—in many years, with the potential to alter ownership structures, commercial applications, cross-border payments, transaction processing and settlement, access to capital, investment opportunities, and much more. These developments contribute to equitable growth and financial inclusion, as well as investor and consumer choice and security. The development of the digital assets ecosystem, therefore, is an important question for policymakers.

SUMMARY

As we discuss in more detail below, digital assets and blockchain applications, more generally, are significant and evolving technological innovations with many use cases developed under a variety of business models. These innovations have the potential to bring increased transparency, security, efficiency, and inclusion not only to financial services but to other sectors as well. As the Office considers what research will support legislation and regulation appropriate to promote responsible innovation in cryptocurrencies and other digital assets, CCI respectfully submits that the Office should be guided by key principles, including:

- Technological innovation should improve access, efficiency, and equity and empower the average consumer.
- Technical standards should be interoperable and open to facilitate permissionless and composable systems.
- Anti-money laundering regulations should be precise in order to stop illicit activities and there should be privacy-preserving technologies that respect

[1]https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development

national security interests.[2]

Advancements in blockchain technology infrastructure will be key to the evolution of our global financial system. It is paramount that the U.S. remains at the center of this technological leap in digital evolution if we are to maintain our monetary, economic, and political preeminence in the global theater.

ABOUT CCI

CCI is an alliance of digital asset industry leaders with a mission to communicate the benefits of crypto and demonstrate its transformational promise. CCI members include some of the leading global companies and investors operating in the digital asset industry, including Andreessen Horowitz, Block (formerly Square), Coinbase, Electric Capital, Fidelity Digital Assets, Gemini, Paradigm, OpenSea, and Ribbit Capital, and Spruce Systems. CCI members span the crypto ecosystem and share the goal of encouraging the responsible global regulation of digital assets to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity.

DISCUSSION

SECTION I: Goals, sectors, or applications that could be improved with digital assets and related technologies

Digital asset research and development can enhance U.S. performance in an increasingly digitized global economy. Rather than focusing on decentralized finance (or DeFi) as an end-state, U.S. policymakers should consider how *decentralized technology stacks* could make financial infrastructure and processes more dynamic, resilient, nimble, and composable. Such an approach to digital infrastructure development will help build the digital assets ecosystem as well as help expand the benefits of the nascent DeFi ecosystem to the broader U.S. consumer economy and spur productivity and innovation for a wider sector of the population.

Strengthen decentralized technology infrastructure

The Office of Science and Technology Policy should support funding a series of decentralized financial infrastructure research pilots, conducted in controlled academic environments or through partnerships with research institutions. The pilot research areas should focus on the following use cases:

- Decentralized Exchange Platforms: In this use of decentralized finance, a platform composed of smart contracts allows participants to trade directly between assets without

[2] *See* CCI's Global Regulatory Blueprint in its comment letter to the Financial Stability Board.

any fear of counterparty risk. This type of trading makes it easier for people to trade more quickly and efficiently. OSTP should direct funding toward the development of a testnet blockchain platform run by a consortium of U.S. universities to experiment with various decentralized exchange designs.The research should also explore how retail shareholders can vote directly rather than the current proxy system of voting by mostly large institutional advisors.[3]

- Humanitarian Aid Distribution: The relative speed and efficiency of decentralized finance systems compared to conventional finance should be leveraged for disbursements of humanitarian aid in environments where banking systems are weak or unusable due to natural disaster, war, or political instability. There are multiple real-world examples of crypto-asset funding efforts delivering needed resources in a humanitarian crisis, such as during the beginning of the Russian invasion of Ukraine and after the devastating earthquakes in Turkey and Syria.[4] U.S. academic institutions should partner with the U.S. Agency for International Development to run a pilot that identifies and tests various scenarios of aid distribution. This pilot could help determine technological and operational features to improve global aid distribution.

- Tokenization of Traditional Financial Assets: An innovative way to improve current financial systems would be to apply decentralized finance to established asset classes that are already well-understood and highly regulated. In this research effort, OSTP should work with prudential financial regulators to inform multiple asset tokenization pilots in an academic testnet environment. In each pilot, academic researchers should construct smart contracts that align with and enforce current regulatory requirements for financial products and services. Central banks and mainstream commercial banks around the globe are already experimenting with asset tokenization, such as the New York Fed's recent proof-of-concept with global banks and the SWIFT organization to transfer regulated liabilities over a blockchain ledger.[5] Also, Project Dunbar, led by the Bank for International Settlements (BIS) Innovation Hub in partnership with the central banks of Australia, Malaysia, Singapore, and South Africa, is testing the use of central bank digital currencies (CBDCs) for improving international settlement.[6] Another project is Project Guardian, the Monetary Authority of Singapore's collaborative initiative with the financial industry that seeks to test the feasibility of applications in asset tokenization and decentralized finance (DeFi) while managing risks to financial stability and integrity.[7] These types of experiments are likely to increase globally, especially as the People's Republic of China is leading other multilateral pilots to use blockchain technology for

[3] https://corpgov.law.harvard.edu/2019/11/19/retail-shareholder-participation/
[4] https://cryptoforinnovation.org/crypto-and-humanitarian-aid-reducing-costs-and-improving-speed/; https://cryptoforinnovation.org/crypto-case-study-ukraine/; https://blog.chainalysis.com/reports/cryptocurrency-donations-provide-fast-relief-for-turkey-syria-earthquake-victims/#:~:text=Additionally%2C%20crypto%20businesses%20Binance%2C%20Tether,Turkey%20affected%20by%20the%20earthquakes
[5] https://www.newyorkfed.org/aboutthefed/nyic/facilitating-wholesale-digital-asset-settlement
[6] https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm
[7] https://www.mas.gov.sg/schemes-and-initiatives/project-guardian

cross-border wholesale payments.[8] Failure to stay ahead of innovation on this front may detrimentally affect the United States' ability to conduct R&D in the future.

- Blockchain research on public sector use-cases: Blockchain or distributed ledger technologies provide significant benefits outside of the digital assets space. In this research effort, OSTP should identify the areas where it is appropriate and beneficial to enable and invest in distributed ledger technologies within government agencies. This will identify the technological resources needed at federal government agencies and key use cases for such technology in these agencies. For example, this could include supply chain management purposes (similar to those mentioned above regarding humanitarian aid), data management, personal identity verification (digital identities), and regulatory reporting purposes.

SECTION II: Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

Ramp up cybersecurity resilience and public-private partnerships

To mitigate the risks of illicit finance relating to digital assets, the U.S. government cyber agencies should prioritize research into cybersecurity resilience within the crypto-asset ecosystem in order to develop standards and institutions to safeguard users and their assets. Also, U.S. federal law enforcement should partner with the private sector to enhance research on cybercriminal networks and strategies to counter them. The following are key research areas that the U.S. should support:

- Bridge security: The Office of Critical Infrastructure Protection and Compliance Policy (OCIP) at the Department of Treasury, the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security, and the Office of the National Cyber Director at the White House should collaborate to conduct a study on the vulnerabilities and viability of DeFi bridge platforms. Hacks of bridges accounted for almost $2 billion in stolen crypto-assets in 2022.[9] Importantly, engagement with the private sector can yield potential solutions, such as collaboration with Self-Regulatory Organizations (SROs) and white-hat hacker groups. SROs like Financial Industry Regulatory Authority (FINRA) and New York Stock Exchange (NYSE) have long worked with their government counterparts to enforce governance.[10] In February 2023, the DeFi platform Oasis.app was able to recover $140 million in hacked crypto funds based on a back door discovered by a group of white hat hackers.[11] The joint agency cyber study

[8] https://www.lawfareblog.com/mbridge-somewhere-central-banking-having-its-sputnik-moment
[9] https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/#:~:text=That%20trend%20intensified%20in%202022,cross%2Dchain%20bridge%20protocols%20specifically
[10] https://www.brookings.edu/research/how-to-improve-regulation-of-crypto-today-without-congressional-action-and-make-the-industry-pay-for-it/
[11] https://www.politico.com/newsletters/digital-future-daily/2023/02/27/when-courts-control-defi-00084610

should include an analysis of the practices and structural problems that led to such hacks and identify how best practices in the traditional financial sector could be transferred to the crypto sector.

- Crypto-asset info-sharing: Treasury should support the formation of information-sharing and analysis centers (ISACs) for crypto-assets by conducting studies that analyze how standards around traditional finance and cybersecurity risk management should be applied to the crypto space.

- Public-private research partnership and exchange: In order to increase the technical expertise on digital assets within US law enforcement and intelligence agencies, OSTP should sponsor a research-focused career exchange program. The exchange should enable members of the digital asset private sector to spend one to two years working within a U.S. law enforcement or intelligence agency and for U.S. national security officials to spend the same amount of time working in the private digital asset space. Participants in these exchanges should research how to best use digital asset technology to improve U.S. safety and security and how to mitigate risks around illicit finance.

SECTION III: R&D that should be prioritized for digital assets

Enable user-focused infrastructure, protocol interoperability, and privacy-enhancing technologies that respect national security

Digital assets are a broad category, and the U.S. must focus research on some key technical areas to harness decentralized technology's strategic economic, social, and security benefits. OTSP should prioritize the following research areas:

- Smart contracts: An important feature of blockchain technology is the ability to program transactions. Because blockchains are purely software code created on and for the internet, developers can, in many cases, design internet-based functions via blockchains that can not easily or efficiently occur through traditional finance. Various countries have also been using smart contracts in real estate and healthcare. The Republic of Georgia has been developing a blockchain-based land title registry since 2016, and similar projects are underway in the United Arab Emirates.[12] The U.S. should provide funding to deepen the expertise in smart contract design within U.S. educational institutions and enterprises.

- Cross-chain interoperability: Interoperability across blockchains is the major challenge in the crypto ecosystem. Most blockchains were built using different standards and

[12] https://ideas.repec.org/a/tpr/inntgg/v12y2019i3-4p72-78.html; https://dubailand.gov.ae/en/news-media/dubai-land-department-achieves-a-technical-milestone-with-the-adoption-of-blockchain-technology-in-cooperation-with-smart-dubai-and-other-partners/#/

programming bases and are thus not interoperable. Participants have developed workarounds, such as bridges. Intensive research is needed to develop ways for users to operate seamlessly across different blockchain protocols.[13]

- Zero-knowledge proofs: Privacy is a fundamental human right and social good. As people's everyday lives create and reveal more data about themselves, there is a growing need to build technical systems and policies to safeguard 4th amendment protections in the digital age. This also is important for cybersecurity. Privacy-preserving technology allows data computation and targeted analysis while remaining encrypted to those performing the computation and malicious actors who might seek to steal or corrupt that information. Zero-knowledge rollups and configurable privacy blockchains are emerging forms of privacy-preserving technologies that balance individuals' privacy interests with broader public policy and societal requirements, such as effective compliance, transparency, and safety.[14] OSTP should work with the National Institute for Standards and Technology (NIST) in the U.S. Department of Commerce to conduct research on zero-knowledge proofs (ZKPs) and how they could be applied in a variety of digital use-cases where selective disclosure and screening are necessary to balance both privacy and security.

- Digital Identity: In order to help ensure American consumers can operate on the internet more securely and privately, the U.S. government should expand its support of digital identity initiatives that use decentralized and privacy-preserving technology. FinCEN's focus on digital identity should continue, but there should be more focus across agencies on applying digital identity solutions to the areas in which they engage the public. Digital identity plays a key role in modernizing and lowering barriers to access to public services such as those related to healthcare, Social Security, veteran benefits, certifications, and licenses.[15] It has the potential to increase convenience, eliminate unnecessary travel, and lower costs for users through remote online authentication. For the U.S. government, digital identity can boost administrative efficiency and reduce the risks of identity fraud. To ensure user privacy and data security in a wide array of use cases, the U.S. government should gain further understanding of how to apply zero-knowledge proofs (ZKPs) and selective disclosure to identity solutions.[16] To guard against monopolies and walled gardens, research efforts should also seek out the benefits of open and interoperable digital identity systems. In addition, it will be important for the U.S. government to work with the private sector to issue guidance and allow for experimentation with digital identity, including projects that incorporate zero-knowledge

---

[13] See remarks by Acting Comptroller Michael Hsu, https://www.occ.gov/news-issuances/speeches/2022/pub-speech-2022-37.pdf

[14] *See* https://a16zcrypto.com/content/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/

[15] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

[16] *See* https://a16zcrypto.com/content/article/zero-knowledge-canon/

proofs. CCI would be happy to facilitate such exchanges as part of a public-private research partnership.

- DeFi: Decentralized finance ("DeFi") is an emerging area of blockchain-enabled financial services and instruments, including brokerage, banking, and exchange, that does not involve the use of intermediaries. Financial intermediaries often introduce inefficiency through higher costs or slower execution. By eliminating intermediaries, DeFi holds the potential to level the playing field for many financial actors who have traditionally been disadvantaged, such as lower-income and unbanked and underbanked individuals and small businesses. More specifics in this research priority area are addressed above in section I.

- Self-hosted Wallets: Wallets (both hosted and self-hosted wallets) are essential to the future of digital assets and are primarily used to store private keys – the passwords that give users access to their cryptocurrencies, NFTs and tokenized assets. Unlike a normal wallet, which can hold actual cash, crypto wallets store digital assets on corresponding blockchains but can only be accessed using a private key. If the users lose their private keys, they lose access to the assets. There have been many hacks over the past few years due to a lack of rigorous research and audits of wallet applications, especially in cybersecurity and access control. OSTP should work with the cryptographic research community and industry players to investigate topics such as multi-party computation (MPC) and programmable access control mechanisms to ensure wallets provide consumer protection and user experience requirements.

- Private key management: Blockchain transactions rely on private cryptographic keys. In order to enhance security and usability for everyday consumers, research is needed on ways to improve the consumer user experience of private key custody, including ways for retail customers to manage their private keys in a safe and efficient manner.

- NFTs: Non-fungible tokens (NFTs) represent unique records minted and tracked on a blockchain that can be used to verify the authenticity and ownership of a particular item asset. Blockchain-based digital identity, in addition to the uses discussed above, can be used to prove ownership of NFTs.[17] While NFTs are useful for developing digital collectibles, OSTP should support research to identify how NFTs could be applied in practical business and public service activities where auditing and verifying asset ownership and provenance are needed. The California Department of Motor Vehicles' pilot using NFTs for title management exemplifies the type of innovative exploration the public sector can undertake by partnering with blockchain firms.[18] In particular, there is significant legal research needed around the policy frameworks that should accompany the growth of NFTs in tracking physical world ownership. OSTP will need to collaborate closely with U.S. legal and audit professional communities on compatibility with existing

[17] https://www.cbinsights.com/research/decentralized-identity-verifiable-credentials/
[18] https://blockworks.co/news/california-pilots-blockchain-car-title-management-system-on-tezos; *see also* https://www.cbinsights.com/research/decentralized-identity-verifiable-credentials/

frameworks. Other jurisdictions—both adversarial and friendly to the United States—are developing strategies to leverage NFTs for public and private sector use cases. For example, the Chinese government is collaborating with software firms to develop NFT-based ownership authentication systems that could be deployed for government records and private sector information-sharing.[19] Japan's majority political party in 2022 released an NFT White Paper to articulate a national NFT strategy for the Web3 era, and guidance to the broader startup and institutional developer community.[20]

SECTION IV: Opportunities to advance responsible innovation in the broader digital assets ecosystem

Explore embedded supervision

In regulating the DeFi space, the U.S. and other jurisdictions will need to explore and develop methods of regulatory supervision that fit the technology's unique features. One approach to appropriate supervision of DeFi is embedded supervision, in which some regulatory requirements for consumer protection, AML/CFT compliance, and other critical matters are built into the DeFi ecosystem through smart contracts. The Bank for International Settlements published a working paper on this issue in 2019, and there appears to be growing discussion about embedded supervision in regulator circles.[21]

OSTP should work with prudential regulators as well as industry and academic experts to conduct research on applying smart contracts for DeFi supervision. This research should emphasize the technical solutions and the policy decisions and changes which may be necessary for building an appropriate regulatory framework for DeFi. Collaborative efforts across the public and private sectors are necessary to craft policies that keep pace with fast-moving technical advances in the digital assets space.

OSTP should also coordinate with all the US regulatory representatives to the Global Financial Innovation Network (GFIN) to evaluate how each financial regulator is evaluating responsible innovation in their respective sector and to learn from the GFIN representatives what other regulators are doing to promote responsible innovation globally.

SECTION V: Other information that should inform the R&D Agenda

Research private-sector alternatives or complements to a CBDC

As the U.S. explores the technical and policy possibilities for a central bank digital currency (CBDC), OSTP should prioritize research on how the private sector might achieve or

[19] https://www.lawfareblog.com/chinas-nft-plans-are-recipe-governments-digital-control
[20] https://www.taira-m.jp/Japan%27s%20NFT%20Whitepaper_E_050122.pdf
[21] https://www.bis.org/publ/work811.pdf

complement the aims and functionality being proposed in various CBDC models. In particular, research is needed on the potential for stablecoins, built on open infrastructure, to upgrade and improve US payment systems without constructing a CBDC. Specific topics include researching the validity of stablecoin private issuance, identifying the benefits and risks of such issuance mechanisms (such as 1:1 reserves vs. algorithmic), and the need for licensure among issuers.

Require greater computer science expertise

In order to craft and manage effective digital asset policies and regulations, U.S. agencies whose work closely involves digital assets each must hire a substantial number of full-time equivalents (FTEs) with computer science skills and expertise. The number of FTEs may vary by agency but should be based on a formal assessment of current levels of computer science technical skills and a prioritization of current and emerging expertise areas.

Innovation Centers

Relevant financial regulatory and policy-making agencies should have centers that enable internal experimentation with blockchain technologies in order to inform rule-making and awareness of use cases for digital asset innovation. In doing so, the U.S. government also needs to consider how to ensure ethics guidance does not preclude officials from having the familiarity with digital assets needed to understand and monitor the ecosystem.

CONCLUSION

In conclusion, digital assets and blockchain applications have already delivered and promise further to deliver great benefits to consumers, investors, businesses, and the economy as a whole. As the Office considers how to promote responsible innovation in this area, we hope the Office will be guided by the key principles outlined above. These principles will support responsible innovators in this field to continue creating products and services that leverage blockchain technology's inherent strengths and bring transparency, security, and efficiency to a range of users and sectors.

Respectfully submitted,

[redacted]

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Centro Cultural Andino, Inc.

From: Centro Cultural Andino Inc.
To: DARD-FTAC-RFI
Subject: RFI Response: Digital Assets R&D Agenda
Date: Friday, January 27, 2023 12:41:09 PM

Hello Government of the people by the people,

I urge the White House to strongly consider embracing cryptocurrency or as better stated crypto assets. If America wants to retain their world economic advantage and remain a beacon of freedom in the world we must always strive to embrace technology that enhances liberty, especially digital freedoms.

I, Andre Herrera, write to you as a citizen and as President of a non-profit that fights to preserve the heritage and freedom of the Andean-American people. Digital assets are a protection against the devaluation of foreign currency that those of South American descent are being affected by.

The USA must embrace this technology for it cannot be stopped and can only be delayed. Crypto is the value layer of the internet; the US embraced the internet long ago and in doing so the largest companies in the world were founded in America. If we do not embrace crypto assets we will be pushing American innovation overseas and into the hands of our enemies. Just as we cannot stop people from using the internet, likewise we cannot stop people from accessing crypto.

Here are my demands: we must publish a guide on how to safely access the leading crypto networks, allow for a Bitcoin spot ETF and an Ethereum Spot ETF, create a new federal agency dedicated to publishing and documenting crypto innovation, we must provide a front end for people to click on safe links, we must recognize good/useful crypto from bad crypto, and we must remain committed to preserving digital privacy.

Embracing DeFi empowers the people, digitizing finance will boost GDP and increase the speed and ease of doing business. Peer to peer digital networks that are socially enforced have the power to secure data, voting rights, and defend our nation from outside cyber attacks. These crypto networks are resilient and growing exponentially. America must upgrade its infrastructure if it wants to stay relevant in this digital age. We must embrace technology, for it will only make us stronger and empower our citizens to continue spreading the ideas of Democracy throughout the world.

The following digital assets are the most important to me: Hex, Ethereum, Bitcoin, Cardano & XRP. Hex, Cardano and XRP specifically are American creations. Let us keep it that way and keep being a leader in the crypto space.

Please reach out to me if you require more specifics or information. Thank you for your time.

Best regards,

--

André Herrera
President
Centro Cultural Andino, Inc.

[redacted]

[redacted]

https://www.centroculturalandino.com/

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Chamber of Digital Commerce (The Chamber)

CHAMBER OF DIGITAL COMMERCE

March 3, 2023
White House Office of Science and Technology Policy
[redacted]

Delivered via DARD-FTC-RFI@nitrd.gov

Re: Digital Assets Research and Development; Request for Information

On behalf of the Chamber of Digital Commerce ("the Chamber"), we respectfully submit our comments on the Office of Science and Technology Policy's Request for Information ("RFI") on Digital Assets Research and Development.

The Chamber is the world's first and largest blockchain trade association. Our mission is to promote the acceptance and use of digital assets and blockchain technology. We are supported by a diverse membership that represents the blockchain industry globally. Through education, advocacy, and close coordination with policymakers, regulatory agencies, and industry across various jurisdictions, our goal is to develop a responsible, pro-growth environment for digital assets highlighting the opportunities this emerging industry will present to the United States. Our members include the industry's leading innovators, operators, advisory firms, and investors in the blockchain ecosystem.

We appreciate the opportunity to engage with you and your staff on these critical issues. We hope to continue the conversation and find ways we can work with you to help advance financial inclusion, consumer protection, social equity, and other worthwhile policy goals through a balanced policy approach to digital assets.

Sincerely,

[redacted]
Perianne Boring
Founder and CEO

[redacted]
Cody Carbone
Vice President, Policy

1. **Goals, sectors, or applications that could be improved with digital assets and related technologies**

Our primary goal for the blockchain and digital assets industry is to raise global economic prosperity through the frictionless exchange of digital assets. Unfortunately, our existing financial system relies on outdated, legacy infrastructure that requires multiple intermediaries to facilitate transactions, which is costly and time consuming. Blockchain technology allows for the peer-to-peer transmission of digital assets, which has the potential to enable a more inclusive financial system, with greater security and consumer protection.

For the U.S. to remain competitive, we need to develop a regulatory structure that allows the research and development of blockchain and digital asset innovations to continue to flourish and mitigates the risks regulators currently associate with these different types of assets. There are many different types of applications and sectors that can be improved by blockchain technologies and digital assets. That being said, for purposes of responding to this question, we focus on: blockchain technology, payments and U.S.-dollar backed stablecoins, smart contracts, and non-fungible tokens (NFTs).

A. Blockchain Technology

Blockchain technology offers immense possibilities for business, government, and consumers. Blockchain's potential is being felt in many industries beyond financial services. For example, California recently announced that they are piloting a new program to digitize car titles and put them on the blockchain to improve its current processes and enhance security with a long-term goal of adding consumer-facing blockchain applications, such as the creation of NFT car titles.[1]

As California has illustrated, blockchain technology serves as the foundation upon which many applications can be built, much like how the Internet underpins multiple use cases such as e-mail, e-commerce, and business processes. Blockchain's characteristics enable faster, more efficient transactions, eliminating the need for multiple intermediaries and the possibility for inadvertent or manual errors across numerous locations or geographies.

Blockchain is a revolutionary breakthrough technology, allowing the creation of infrastructure toward an Internet of value (or "for intelligent value transfer networks."). While technological progress is clear, it does not automatically follow that America will maintain its preeminence in the blockchain sector. Already, industrialized nations are making significant advances in promoting and adopting this technology, threatening the status of the U.S. in this area. The

[1] https://blockworks.co/news/california-pilots-blockchain-car-title-management-system-on-tezos

Chamber was pleased to see that Congress enacted legislation in 2022 to establish a national R&D strategy for distributed ledger technology (DLT)[2] in addition to the creation of a blockchain and cryptocurrency specialist position within the White House Office of Science and Technology Policy.[3] However, more needs to be done and the United States must commit to learning how blockchain works, examine its strengths and weaknesses, and how those attributes can create new mechanisms for enabling the provision of products and services. Specifically, since crypto remains the most prominent use case of blockchain technology, many are less familiar with the non-financial applications of blockchain. Therefore, R&D on the non-financial aspects of blockchain, including NFTs, could demonstrate new ways that this technology could promote efficiency and accuracy in consumer transactions. Ultimately, the U.S. should lead by example and create a statutory and regulatory environment that allows for an organic transition from a legacy technology infrastructure to the blockchain, thus maintaining the U.S.' position of technological and commercial dominance throughout the world.

B. Payments and U.S. Dollar-Backed Stablecoins

Digital assets and stablecoins have the potential to fight global poverty by making cross-border payments faster and more affordable. Today, a typical remittance fee can be as high as 10.9% per transaction,[4] and the World Bank estimates that "[g]lobally sending remittances costs an average of 6.3% of the amount sent.[5] In addition, international money transfers can take anywhere from 1 to 5 business days depending on the banks involved, the destination country, bank hours of operation, and currency conversions needed.[6] In contrast, payments providers operating in South America and Africa using bitcoin and other open cryptocurrencies charge transaction commissions as low as 1%.[7] Since analysts expect that the remittance market will grow by $200 billion to over $900 billion by 2026, lower fees will ensure that more funds go directly to individuals and their families.[8]

Domestically, the lack of a real-time payment system available 24 hours a day forms the basis for why Americans pay approximately $26 billion in overdraft and high-cost check cashing fees

[2] NDAA 2022
[3] The position was created with enactment of the CHIPS Act of 2022. Subtitle H, Section 10671
[4] "Bitcoin gains traction as a vehicle for sending remittances home to Mexico," Mexico News Daily, May, 2021.
[5] "Remittance Prices Worldwide," The World Bank, January 2023.
[6] Cecilia Hendrix, "How long do international money transfers take?," Western Union, April 5, 2021.
[7] Andalusia Knoll Soloff, "The new wave of crypto users: migrant workers," Rest of World, April 26, 2021.
[8] Polly Jean Harrison, "Global Remittance Market is Expected to Grow by $200 Billion by 2026," The FinTech Times, June 29, 2021.

each year.[9] In 2021, the U.S. Consumer Financial Protection Bureau revealed 20 banks each earned between $50 million and $1.4 billion in overdraft and non-sufficient fund fee revenue.[10]

Under the U.S.' existing legacy payment system, settlement can take anywhere from hours to days, leading individuals to use check cashers or payday lenders to receive real-time access to funds. Meanwhile, in other countries around the globe, real-time payment settlement is very present. The United Kingdom has a robust instant payments system, which supports over 8 million transactions per day.[11] The Bank of England uses Real-Time Gross Settlement (RTGS) Infrastructure to operate CHAPS, a sterling same-day payments system used to settle high-value wholesale payments as well as time-critical, lower-value payments.[12]

While the U.S. also has a RTGS system, it carries fewer than 1 million transactions per day and is used almost exclusively by financial institutions and large corporations.[13] Further comparing the U.S. and U.K. systems, transfers between U.S. banks incur fees averaging from $10 to $35 for same day transactions, whereas the U.K. payments system is free, available at all times, and settles within seconds.[14] The U.S. lags even further behind India, where the number of real time payments, over 48 billion, was almost seven times greater than the combined real-time payments volume of the U.S., Canada, and the UK in 2021.[15] The Reserve Bank of India paved the way for India's lead by creating and encouraging supportive infrastructure such as QR codes for merchants and radio-frequency identification (RFID) tags for toll gates.[16] India's rise to the top of the real-time payments market demonstrates the importance of clear regulatory guidance and a robust research and development strategy to compete.

While we appreciate that the Federal Reserve is working towards its own real-time payments architecture with FedNow, this has been a multi-year effort, expected to end later this year. Furthermore, FedNow is not a blockchain-based service and therefore, relies on third parties inevitably requiring trust and additional costs from users. Furthermore, at launch, FedNow will only support domestic payments between U.S. depository institutions.[17] FedNow's limitation to

---

[9] Aaron Klein, "The fastest way to address income inequality? Implement a real-time payment system," Brookings Institution, January 2, 2019.

[10] https://files.consumerfinance.gov/f/documents/cfpb_overdraft-chart_2022-04.pdf

[11] Bank of England, "Bank of England's RTGS and CHAPS services: Service Description," December, 2018.

[12] Ibid.

[13] Christian Catalini & Andrew Lilley, "Why is the United States Lagging Behind in Payments?," July 27, 2021.

[14] Ibid.

[15] ACI Worldwide, "India Surges Ahead as the World's Leader in Real-Time Payments – Boosting Economic Growth," April 26, 2022.

[16] The Economist Intelligence Unit, "Going Digital - Payments in the post-Covid world," 2021.

[17] Board of Governors of the Federal Reserve System, "FedNow Service Frequently Asked Questions," September 2, 2022.

domestic payments could eliminate opportunities for vulnerable populations overseas, such as refugees and victims of natural disasters, to receive cross-border humanitarian assistance.[18]

The delay in FedNow implementation or another effective US real-time payments infrastructure has forced the industry to find ways to accomplish the same goal that deserve further research and development. For example, the Bitcoin *Lightning Network*[19], a layer 2 protocol designed to tackle Bitcoin's scalability issues, can process nearly 1 million transactions per second (TPS). Comparably, Visa processes nearly 1,700 TPS.[20] The *Lightning Network* was created to reduce Bitcoin blockchain congestion and lower Bitcoin-mining fees, leading to greater scalability and use of Bitcoin as a payment tool.

The *Lightning Network* has already proven effective in transforming payments in its short lifespan. Twitter now allows tipping using the *Lightning Network* and El Salvador enables Bitcoin payments among its citizens using the Chivo Wallet, which features *Lightning Network* functionality.[21]

C. Smart Contracts

Smart contracts are computer code that, upon the occurrence of a specified condition or conditions, are capable of running automatically according to prespecified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger.[22]

With additional research and development, smart contracts will help to realize the many possibilities of DLT. Certainty of outcome, automation of performance, and efficiencies in the streamlining of processes are reasons enough for smart contracts to be fundamental to the uptake of DLT. Their potential is now being actively considered and developed in various sectors. In financial services, for example, smart contracts are used for B2B bank payments, securities clearing and settlement, collateral management, derivatives contracts, securities asset servicing, international money transfers, and syndicated lending. For many sectors, it is the ability of smart contracts to be transformative in relation to existing business processes that is compelling. For others, it is the potential of smart contracts to reduce execution risk by making transfer of the asset or instrument in question nearly inevitable by virtue of automatic performance.

---

[18] UNCHR, “UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine,” December 15, 2022.
[19] https://lightning.network/
[20] “Visa acceptance for retailers,” Visa, accessed July 20, 2022.
[21] Ibid.
[22] “Smart Contracts: Is the Law Ready?,” Chamber of Digital Commerce, September 2018.

D. Non-fungible Tokens (NFTs)

The current use cases of NFTs, mainly digital collectibles, are already helping create a more inclusive and dynamic economy. However, NFTs should be viewed as more than that. Over time, this technology has the potential to transform the infrastructure underpinning much of our online economy and should be researched further to leverage the technology for efficiency and security purposes. For example, the European Union is currently considering the use of NFTs to help combat the counterfeiting of real-world goods by allowing owners of intellectual property to issue digital tokens for physical goods, which will be recorded on the blockchain and used in trade to prove that the item is genuine.[23]

Additionally, U.S. financial institutions are considering leveraging NFTs to solve one of their major challenges: document fraud. Solutions include using NFTs for storing sensitive data and maintaining accurate, unalterable, and immutable records.[24] NFTs can also tokenize personal data, such as medical records and investor qualifications/credentials, which will protect privacy and create a more efficient verification system. Health industry stakeholders believe storing personal data on the blockchain would avoid compromising confidentiality and tampering by external sources and allow authorized healthcare providers access when required.[25]

2. Goals, sectors, or applications where digital assets introduce risks or harms:

As with any nascent industry, there are risks associated with rapid growth and adoption. However, the Chamber continues to stress that discussion of risks in the digital asset community should not be considered in a silo but in comparison with legacy systems that struggle with the same risks. We appreciate the many components of government that encourage innovation in financial technologies and stress the need for more regulatory flexibility to enable such innovation to occur.

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets:

A. Decentralization

---

[23] https://torrentfreak.com/images/wipo_ace_15_10.pdf

[24] Konstantin Richter, Newsweek, *How NFTs Can Impact the Financial Industry*, https://www newsweek.com/how-nfts-can-impact-financial-industry-1716215.

[25] Chrissa McFarlane, *Forbes, Tokenized Blood? How NFTs Are Transforming Healthcare*, https://www.forbes.com/sites/chrissamcfarlane/2021/06/02/will-nfts-save-healthcare/?sh=1e29faf6eae3.

Some of the most promising social benefits of digital assets have yet to be introduced. For example, Decentralized Finance (DeFi) could result in significant improvements in social equity and financial inclusion in the financial services sector, as DeFi protocols enable users to participate in financial markets and access services regardless of their location, wealth, or credit score.

DeFi could also mitigate some of the risks associated with traditional financial services by leveraging decentralized, transparent, and trustless blockchain networks. For example, DeFi protocols can reduce counterparty risks in transactions by using smart contracts to automate financial transactions, reducing the need for intermediaries and the associated risk of counterparty failure.

Separately, decentralized identity solutions and systems should also be further researched for their ability to improve privacy protections and mitigate concerns linked to CBDCs and other traditional offerings. Decentralized identity allows individuals to control their personal data and reduce reliance on centralized actors to manage and store sensitive information. In traditional systems personal information is stored in databases controlled by government agencies or corporations, which have been susceptible to data breaches and theft. Decentralized identity systems use blockchain technology to store and manage personal information, enabling users to only share the data they want to, with whom they want to, and when they want to.

4. R&D that could be prioritized for digital assets

A. Environmental Impact of Digital Asset ["proof-of-work"] Mining

Since China's ban of digital asset mining the U.S. has become the global leader in hash rate. This is an opportunity for the U.S. to assert leadership on several fronts: expanding economic growth via digital asset adoption, securing the Bitcoin network, and perhaps most importantly, an unprecedented opportunity to deploy infrastructure that enables a clean energy transition.

The digital asset mining industry today is spurring U.S. economic growth, job creation, and innovation, especially in rural areas where opportunity and innovation are needed most. This is being achieved while also creating financial incentives for the buildout of renewable energy infrastructure.

Yet, these opportunities are sometimes overshadowed in policy debates with misinformation. While digital asset mining currently uses less than 0.1% of the world's energy,[26] headlines make

[26] Bitcoin Mining Council, "Global Bitcoin Mining Data Review Q1 2022," March 2022.

claims such as “Bitcoin Uses More Energy than Many Countries,” or “Bitcoin Mining Makes Seneca Lake Feel Like a Hot Tub.”

The reality is digital asset mining can be far more flexible with its energy needs, particularly when compared to other energy-intensive industries, such as data centers and manufacturing facilities. Claims that the proof-of-work protocol somehow uses an outsized share of electric power to the detriment of the world’s environment are unfounded. Accordingly, the Chamber of Digital Commerce’s digital asset mining industry members are committed to using carbon neutral or renewable resources across the industry and partnering with the renewable energy sector.

The Biden Administration has established robust climate goals. Digital asset mining can serve as a catalyst to achieve these worthy goals, offering unique capabilities that traditional data centers and energy consumers cannot. While providing a utility with a reliable base customer that provides consistent demand and revenue for utilities to build out clean energy infrastructure, digital asset miners can power down to allow critical usage of energy during crises.

Why are these policies important? Bitcoin has been adopted by over 100 million individuals worldwide, and digital asset mining is the foundation of this ecosystem, creating an opportunity for millions of people in less fortunate economic circumstances to access a new financial system by allowing them to store their savings in a medium that is independent of rapidly increasing inflation, banks fees, and long-standing inequities in our banking system.

B. Digital Identity

A national R&D agenda for digital assets should prioritize the investigation and development of standards for privacy-enhanced digital ID. Promising advances in privacy enhancing technologies aim to simultaneously protect an individual’s personal information while securely sharing necessary information to confirm identity.[27] Additionally, digital ID has the potential to help mitigate fraud and ID theft in federal programs and enable KYC, KYB, and associated illicit finance controls. Specifically, decentralized identity solutions can facilitate near-real time onboarding and address security risks involved with the sharing and reuse of Personally Identifiable Information (PII) in compliance by packaging such information into credentials and bringing verifiable identity to the user level for KYC/KYB checks. Verifiable credentials backed by KYC and KYB data can also be delivered directly to clients’ wallets, enabling the attachment of a client’s KYC status, which can facilitate transaction identification. Further, digital ID has

[27] Gorfine Daniel and Mosier, Michael. “Opinion: Stablecoin and other digital assets are falsely framed as a choice between personal privacy and national security. We can have both,” MarketWatch, July 19, 2022.

the potential to advance financial inclusion, providing individuals lacking traditional proof of identity with access to safe and trackable services in the traditional financial system.[28] Therefore, a national R&D strategy should include digital ID innovation, as digital ID offers a unique opportunity to modernize KYC and KYB processes and create access to financial services.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem

As with any new innovative technology, digital assets may pose opportunities and risks that are not well understood. However, a rational and balanced approach to regulation can help ensure that risks are mitigated and the benefits of these innovations are advanced responsibly.

Today, measured policymaking is necessary to fulfill the promise of DeFi and digital assets to create a financial system that is faster, cheaper, safer, and more inclusive. Regulating this innovative space will require addressing many of the same problems found in traditional finance, including consumer protection, fraud, money laundering and other financial crime, and overall financial stability. Policymakers and regulators can enforce existing rules to protect against bad actors while providing adequate regulatory guidance, relief, or changes that enable positive innovation to flourish. To achieve these ends, regulators should consider these policy recommendations:

- **Ensure regulatory coordination in the U.S. and globally.** Disparate guidance from domestic and global regulatory bodies has made it extremely challenging and costly for digital asset and DeFi projects to maintain compliance with applicable regulations as they develop.
- **Clarify how custody rules apply to digital assets.** The SEC, the Office of Comptroller of the Currency ("OCC"), and state regulators each have differing custodial requirements for digital assets. Providing continued clarity on how existing custody rules apply to digital assets, and allowing the traditional, regulated financial system to interact with digital assets, will provide a safer arena for consumers to navigate the digital asset ecosystem.
- **Leverage digital assets and blockchain technology to bolster AML/KYC compliance.** Money laundering transactions involving cryptocurrencies represent only a tiny fraction of the total value of assets laundered throughout the world. Moreover, the traceability feature of blockchain technology makes it a less-than-ideal mechanism for illicit finance and has proven to aid regulators in tracking down money launderers.[29] Technological developments are facilitating innovation with the potential to significantly enhance KYC compliance. These developments could allow for the establishment of a formal "digital KYC utility" that would

[28] Appaya, Sharmista and Varghese, Minita. "Digital ID - a critical enabler for financial inclusion." World Bank Blogs, June 20, 2019.
[29] Uberti, supra note 71.

verify customer identities across market participants, rather than the current approach of requiring entities serving end-users to obtain and verify the name, date of birth, physical address, and telephone number before onboarding a client.[30] Although the technology still needs to evolve for expanded and continuous use, digital KYC utility could enhance compliance with AML/KYC regulations and permit firms to more efficiently identify potential indicia of illegal behaviors.[31] More broadly, policymakers should encourage the development of portable digital identities. Portable digital identities allow consumers to access one system for identity verification and use the power of the blockchain to transport that identity and access services across firms. Not only will this drastically improve access to services for consumers but will also result in less opportunity for identity fraud.

[30] Letter from Perianne Boring, President, to Kenneth Blanco, FinCEN Director, Chamber of Digital Commerce, November 26, 2019.

[31] Ibid.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Chamber of Progress

March 3, 2023

Rachel Wallace
Deputy General Counsel
The White House
Office of Science and Technology Policy

RE: Request For Information - Digital Assets Research and Development (FR Doc. 2023-01534)

On behalf of Chamber of Progress, a tech industry association working to ensure that all Americans benefit from technological leaps, I appreciate the chance to submit comments to the White House Office of Science and Technology Policy (OSTP) on a National Digital Assets Research and Development Agenda. Responses are provided below:

1. **Goals, sectors, or applications that could be improved with digital assets and related technologies.**

Financial Services
Digital assets can improve financial services by enabling faster and cheaper transactions, reducing the need for intermediaries, and providing new opportunities for financial inclusion. Digital assets can enable cross-border payments and remittances, microfinance, and peer-to-peer lending.

Identity and Access Management
Digital assets could have a groundbreaking impact on identification and verification credentials. Digital assets could improve identity and access management by enabling secure and decentralized identity verification, reducing the risk of identity theft and fraud, and enabling greater control over personal data. They can potentially reduce the need for passwords and other authentication methods, and enable the sharing of data on a need-to-know basis.

The state of Rhode Island recently piloted a program on the blockchain to issue credentials to Certified Public Accountants (CPA). The credentialing process reduced the time to issue a CPA license from weeks to 30 minutes by establishing an identity blockchain network that digitizes and automates workflows enabling the secure exchange of information among the state agency and citizens.[1]

[1]https://www.forbes.com/sites/patrickmoorhead/2022/10/05/rhode-island-wants-to-make-it-easier-to-do-business-using-blockchain-technology/?sh=7f55b5b27a25

2. Goals, sectors, or applications where digital assets introduce risks or harms.

Market Instability

Similar to other areas of the financial services industry, harmful business practices and fraud committed by bad actors contribute to severe market fluctuations. Unfortunately, this results in investors and consumers losing most (or all) of the value of their assets. The bankruptcies of large digital asset companies last year left customers unable to access their accounts or recoup their investments.[2] Additionally, rapid price swings and token devaluation could harm participants of the digital asset marketplace, including banks and other financial institutions. This led to recent guidance issued by the Office of the Comptroller of Currency (OCC) and other bank regulators to reduce potential effects digital assets could have on the banking market.[3]

Fraud and Scams

While critics have expressed concern[4] about the fraudulent use of digital assets,[5] Chainalysis' 2023 Crypto Crime Report showed that digital asset scam revenue fell by 46% from 2021 to 2022.[6] Although scams remain the largest form of digital asset crime,[7] many of these scams do not originate from digital assets and closely resemble common scams that have evolved over time,[8] indicating that criminals leverage new technology to continue traditional scams identified by law enforcement.

Fraudulent Tokens

One of the largest sectors in digital assets with the most exposure to investor harm is the creation and promotion of fraudulent tokens. Because anyone can mint their own token on the blockchain, digital assets may be created with the intention of defrauding its investors. A blockchain risk monitoring firm, Solidus Labs, published a report sharing that over 118,000 scam tokens were created in 2022.[9,10] These tokens are often programmed in a way so that investors cannot sell the token–known as a "honeypot"–or are advertised with deceptive marketing websites and fake partnerships to lure in unsuspecting investors.[11]

Market Manipulation

One potential risk in the digital asset industry is market manipulation, which can be a by-product of fraudulent tokens. A popular term used in the digital asset industry is a rug pull, which is an exit scam occuring when a team heavily promotes their project's token before disappearing with the funds, leaving their

---

[2] https://www.bloomberg.com/news/articles/2022-07-06/voyager-account-holders-likely-won-t-get-all-their-crypto-back
[3] https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-1a.pdf
[4] https://www.cnn.com/2023/01/25/investing/crypto-elizabeth-warren-ftx/index.html
[5] https://fortune.com/2022/09/22/jpmorgan-jamie-dimon-dangerous-crypto-decentralized-ponzi-scheme-not-good-for-anybody/
[6] https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf
[7] https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf
[8] Fireside Chat - Janay Eyo and Clark Flynt-Barr, "Consumer Empowerment in the Age of Digital Assets." https://www.youtube.com/live/GdQT6ZRR2iE?app=desktop
[9] https://cointelegraph.com/news/350-scam-tokens-were-created-every-day-this-year-solidus-labs
[10] https://8990222.fs1.hubspotusercontent-na1.net/hubfs/8990222/Solidus%20Labs%202022%20Rug%20pull%20report.pdf
[11] https://8990222.fs1.hubspotusercontent-na1.net/hubfs/8990222/Solidus%20Labs%202022%20Rug%20pull%20report.pdf

investors with a valueless asset.[12] These scams involve artificially inflating the price of the token, often through wash trades. Wash trades are illegal transactions made to inflate the trading volume of an asset in order to give the appearance of rising popularity. Given that there is minimal regulatory oversight around newly created tokens, or industry standards for listing tokens on a centralized or decentralized exchange, it can be challenging for consumers to make informed decisions on the best choices for digital asset participation.

Digital assets are not regulated in the same way as traditional financial assets, which can expose investors to potential fraud, market manipulation, and other risks. Due to minimal policymaking and rulemaking around this nascent industry, consumers are at risk of losing savings and retirement funds from long-established poor market practices. Longterm, the volatility of digital assets could pose a risk to consumers' financial stability if there is not sufficient regulation – especially if more digital assets are widely adopted as a means of payment or investment.

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

Last year, President Biden's Executive Order 14067[13] On Ensuring Responsible Development of Digital Assets led to follow up reports from different agencies covering topics from digital asset sustainability to implications for customers and businesses. The Financial Stability Oversight Council (FSOC) also issued a report, outlining risks and regulatory gaps if the digital asset industry continued to grow without the appropriate regulation.[14] We recommend that this specific report should be updated and released annually to include any new risks and recommendations, as novel technology is introduced in the industry and as the regulatory landscape continues to develop.

In addition to reporting, there could be research conducted on the economic implications of digital asset ownership. This research may include a study on digital assets' effect on financial stability, intergenerational transfer of wealth, as well as the economic well-being of households transacting and investing in digital assets. The Federal Reserve conducts an annual Survey On Household Decisionmaking (SHED), which identifies potential risks to financial stability in households nationwide.[15] Additionally, a national survey could be conducted to gather data on the utilization of digital assets.

Gathering information on the usage by digital asset owners, and their demographic information, could help the government determine appropriate risk thresholds around specific activities for digital assets. Understanding consumer behaviors and industry trends through annual reporting would be an effective way to mitigate potential risks and reduce misconceptions about digital assets.

4. R&D that should be prioritized for digital assets.

[12] https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it
[13] https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets
[14] https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf
[15] https://www.federalreserve.gov/publications/report-economic-well-being-us-households.htm

Scalability
As more people use digital assets daily, blockchains processing each transaction should be able to increase the amount that can be processed per second. Industry participants like the Ethereum Foundation[16] and Lightning Labs[17] are developing innovative ways to lower processing times while minimizing transaction costs. Prioritized research could focus on developing new consensus algorithms along with building secure products and services on pre-existing blockchains.

Interoperability
Many digital assets are stored on blockchains built using different coding languages. While this offers consumers to participate in ecosystems that meet their needs, it could fragment developer energy, disrupt user experience and lead to product redundancy. Multiple blockchains can make asset transfers across them difficult, resulting in the creation of software used specifically for conducting transactions between them.[18] The software, called a cross-chain bridge, could potentially leave consumers' assets at risk of being hacked. Some bridges were exploited recently,[19] and research can be conducted to increase safety and security features for bridge transactions. Research can also focus on developing products and services that enable interoperability, such as developer tools with portability software for use on multiple blockchains.[20]

Usability
Digital assets can be challenging for non-technical users to understand and use. Research could focus on improving the usability of digital assets by designing user-friendly interfaces, simplifying transaction processes, and integrating them into existing financial systems.

Security
Quantum computers – complex problem-solving systems more powerful than supercomputers – poses a potential threat to blockchain technology.[21] In the future, quantum computers may easily be able to break the encryption that secures all blockchain transactions; a normal computer would take over half a billion years to break Bitcoin's encryption, a quantum computer might only need ten minutes.[22] If an attacker were able to break the encryption of a blockchain transaction, they could potentially steal or duplicate a digital asset. Research should prioritize developing security tools and safeguards for digital asset transactions against quantum computing.

5. **Opportunities to advance responsible innovation in the broader digital assets ecosystem.**

Workforce Development and Training
The top constraining factor hindering the United States' growth in the digital asset market is the current lack of skilled blockchain professionals. The increased adoption of

[16] https://ethereum.org/en/upgrades/sharding/
[17] https://lightning.engineering/loop
[18] https://www.investopedia.com/what-are-cross-chain-bridges-6750848
[19] https://www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html
[20] https://m.mondovisione.com/news/neon-labs-deploys-ethereum-virtual-machine-evm-on-solana-cross-chain-neon-e
[21] https://www.ibm.com/topics/quantum-computing
[22] https://decrypt.co/resources/quantum-computer-crypto-explainer-guide

digital assets will continue to increase the demand for blockchain business solutions and hiring. It is essential to meet the demand for skilled digital asset professionals by increasing the funding and availability of blockchain-based workforce development programs. Other ways to prepare the current workforce for widespread digital asset adoption is through reskilling and upskilling. Research from the World Economic Forum shows that the United States will see $85 billion in additional gains from upskilling its financial services workforce.[23]

By increasing the number of American professionals innovating in the blockchain industry, the United States can maintain its globally leading position with the greatest share of the global blockchain market. Although projections of digital asset market cap are uncertain, the current global blockchain market is valued at roughly $1 trillion.[24] In 2020, the United States employed more than 400,000 blockchain engineers and was expected to grow at an annual rate of 5%-10%.[25]

Clear Regulatory Structure

The United States must establish a clear regulatory environment in order to retain and attract cryptocurrency and blockchain businesses. Otherwise, companies will move overseas – where they will have less incentive to follow American laws or reflect American democratic values. It is critically important for successfully thwarting humanitarian crises financed by terrorism and preventing money laundering for illicit activities.

For example, foreign crypto exchanges that facilitate payment transactions would be less incentivized to follow war-time sanctions, like those issued against Russian oligarchs following the invasion of Ukraine. Our nation's economic and national security interests greatly depend upon the United States' ability to attract and retain the business of major cryptocurrency exchanges.

We must not lose sight of the opportunities the digital asset industry is bringing to the table of American innovation. This rapidly developing industry needs the full support of the United States, so we can build a more progressive future.

Sincerely,

[redacted]

Janay Eyo
Director, Financial Policy
Chamber of Progress

[23] https://www3.weforum.org/docs/WEF_Upskilling_for_Shared_Prosperity_2021.pdf
[24] https://coinmarketcap.com/
[25] https://www.onetonline.org/link/summary/15-1299.07

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Chia Network Inc. (“Chia”)

March 2, 2023

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

Via Electronic Mail: DARD-FTAC-RFI@nitrd.gov

Re: RFI Response: Digital Assets R&D Agenda

Dear Ms. Wallace,

Chia Network Inc. ("Chia") welcomes the opportunity to provide information, data, and expert opinion to the Office of Science and Technology Policy ("OSTP") request for information on "Digital Assets," (Doc No.2023-01534) as published in the Federal Register dated January 26, 2023 ("RFI").

Chia applauds the Science and Technology Policy Office and Administration's further exploration into the application and utility of digital assets and blockchain technology. Chia believes the initial adoption of digital assets myopically leverages the technology as a tool for financial speculation, undermining the broader set of capabilities of blockchain technology. Cryptocurrencies should not be used or viewed as a separate "asset class." Instead, blockchain and the underlying cryptocurrencies can be deployed as rivalrous technologies enabling and building the next innovative solutions to financial and human rights challenges.

For this RFI, we will seek to raise areas and use cases where we believe blockchain technology is uniquely applicable, provides substantial benefits to commerce and finance, and bears further research. Given we have built and actively stewarded a public layer-1 blockchain, we believe we are well-positioned to address the positive impact of blockchain technology through the aperture of utility across a spectrum of industries and use cases. We are actively developing foundational blockchain primitives – discrete, segment-agnostic functional applets – enabling more efficient, transparent, and secure data management through distributed ledger technology.

Further, we will share our experiences constructing the digital infrastructure for the Climate Action Data Trust ("CAD Trust"), a collaborative effort between the World Bank, the Monetary Authority of Singapore ("MAS"), the International Emissions Trading Association ("IETA"), among others, to deploy technology in support of the Paris Agreement on climate; as well as demonstrate efficacy as a market instrument with the International Finance Corporation (“IFC”).

Goals, sectors, or applications that could be improved with digital assets and related technologies:

A. Equitable Access to a Global and Liquid Store of Value

Chia believes that the underlying infrastructure of the global financial system is evolving, and digital assets and blockchain technology are driving change. Integration of digital assets into the current financial system has demonstrated the strengths and opportunities of these digital assets, and highlighted the weaknesses of how these assets have been built, audited, deployed, and used. Adoption is valuable as a first step, but we believe that demonstrated applicability is the most necessary component for broad utilization beyond the initial use cases today.

We believe that real-world and significant use cases exist for digital assets and blockchain. For example, payments with stablecoins and cross-border remittances - especially in non-OECD countries where financial institutions and infrastructure is not widely accessible - are important uses of the technology. Existing payment systems are dated, require mutual counterparty trust, and are increasingly complex for cross-border transactions. The crisis in Ukraine highlights some weaknesses in the current financial system; digital assets can provide an alternative and safer way for people to access, transact with, and protect their wealth. With blockchain technology, payments could be available to anyone, anywhere, 24×7, and settle transparently with finality, at a fraction of today’s cost, in just a few minutes.

Markets are also an ideal application of digital assets and blockchain. We believe meaningful use cases exist in commodities, debt, and equities, and their options and derivatives, that have yet to be explored and comprise a significant portion of global financial activity. Issuing and enabling assets on-chain with a 24x7 interoperable market can increase liquidity and access, reduce market fragmentation and friction, and offer increased opportunity for more equitable engagement. Blockchain enables the trading of assets among two or more entities anywhere in the world at any time and in a way that ensures that no party can defraud another. It makes completing a trade trustworthy and fast.

We believe our applicability-first approach demonstrates the unique value proposition of digital assets. We have taken a novel and compliant approach to building partnerships - notably with multilateral and government entities - to deploy our digital assets and blockchain technology.

I. Deployed Use Case: The Carbon Opportunities Fund in Partnership with the IFC

The Carbon Opportunities Fund (the “fund”) is a partnership with the IFC, and Cultivo. This partnership acquires high-quality, nature-based carbon offsets that will be reflected in the CAD

Trust, tokenized on the Chia blockchain, and made available to be traded and/or retired to offset carbon footprints. Chia implemented a cross-border and cross-market "internet of markets," creating a single venue for price discovery and trading. The COF relies on the trust created from the operation of the CAD Trust on the Chia blockchain.

II. Use Case for Further Research: Faster Finality of Settlement

Current markets require a delay from the time a transaction is agreed upon until finalization so that centralized entities can confirm and record both sides of a trade and transfer assets and ownership. For example, in equity securities, this delay (generally two business days, shifting to one business day in May 2024) can be costly due to margin requirements at clearinghouses and lost business. As demonstrated with the Carbon Opportunities Fund, blockchain technology has the potential to decrease this delay from days to minutes, reducing the need for clearinghouses and decreasing margin requirements for brokerages.

B. Deprecating Traditional Databases in Multi-Entity Commerce and Consortia

Physical paper records and centralized private digital databases facilitate global commerce today. This outmoded infrastructure cannot keep up with the increasing complexity, jurisdictional distribution, or shifting regulatory environment, and we sought to operationalize distributed ledger technology to meet the needs of global connectivity today.

Chia developed a technology primitive, the Chia DataLayer, which enables a shared data network built on top of the public Chia blockchain. This functionality exists in a few permutations across the industry but with varying degrees of security and transparency. Some examples of this include pinning data to a blockchain and private blockchains.

The Chia DataLayer offers a key differentiation – allowing groups of enterprises, governments, developers, and individuals to create a system of databases that can reference and ensure consistency between one another, verifiable on our public blockchain. Federated databases can have a range of access controls set by the federation's participants, allowing for full transparency or access to only select information. All updates are append-only, immutable, and coordinated on-chain. As a result, with Chia DataLayer there is strong multi-party collaboration where all parties can audit information and do not need a trusted third party.

Specifically, this technology stores cryptographic hashes *representing* data on the Chia blockchain - not the data itself, ensuring every participating entity retains its data sovereignty. As the data changes and updates, additional hashes are subsequently stored on the blockchain. The blockchain verifies this data's validity by comparing the hashes on-chain after a data update or change. If the original data's hash matches the hash stored on-chain, then the original data is guaranteed to be valid, certifying transparency and auditability within a data network. Ultimately, this process creates an immutable record and enables the ability to prove data provenance and integrity.

We believe key segments would benefit from the ability to validate and maintain strict compliance with shared data in a consortium, partnership, or vendor-to-customer relationship.

I. Deployed Use Case: The Climate Action Data Trust and World Bank Climate Warehouse Digital Ecosystem

The CAD Trust provides quality and high-integrity foundational infrastructure for carbon markets. This system offers the private sector, NGOs, and governments the ability to look into a single portal and identify what is happening, where, and how many times units are being issued while avoiding double counting. The technology clearly demonstrates the supply and demand dynamics of the Voluntary Carbon Market, building trust and confidence in quality carbon credits. The CAD Trust seeks to bring transparency and efficiency to the voluntary carbon market and increase funding to impactful projects supporting the environment and local communities across the world.

Each participant in the CAD Trust (carbon registries and nation-state members) publishes data in their DataLayer tables, using their Chia wallet and keys and running on their infrastructure. Subscribed to data from other nodes in this network, these members receive updates on data changes, allowing them to compare the received data to the proof on the blockchain and confirm that the data is correct. A “governance” node, run as a collaborative effort between the MAS and IETA, publishes another DataLayer table with the list of the DataLayer tables published by each of the recognized participants. Each participant and any public observer only needs to know the DataLayer table ID for the governance node to locate all other participants’ data.

II. Use Case for Future Research: Supply Chain

Supply chain management faces several challenges, such as managing inventory, coordinating with suppliers, and customs and regulatory requirements. Post-trade processing relies on manual, complex, paper-based processes subject to loss, delay, and error, causing supply chain shocks in an increasingly complex and fragmented world.

The Chia DataLayer would streamline the monitoring and validation of manufacturing inputs from numerous parties. Blockchain technology enables the real-time sharing of verified trade documentation between trusted partners on a permissioned system, creating an immutable record from source materials to trades. These digital records allow partners to see real-time opportunities to improve trades and avoid or mitigate potential risks. Permissioned access to data can provide substantially more control than traditional paper-based documentation, a benefit for enterprises seeking to share only what is needed when it is required. Additionally, real-time documentation enables assessing a specific shipment’s regulatory compliance before arrival to avoid costly delays.

III. Use Case for Further Research: Healthcare

Medical records' sensitive, confidential nature requires the utmost protection, and yet, the traditional system of maintaining paper records or centralized digital records remain inefficient, fallible, and prone to data breaches. Blockchain technology may facilitate the transformation of the management and sharing of medical records by providing a permissioned, compliant, secure, auditable, and efficient infrastructure. Blockchain-based, electronic medical records ensure that only authorized personnel can access private information, ensuring that patients' information remains confidential.

For example, by leveraging DataLayer, patients can have complete control over their data. They can grant permission to healthcare providers to access their records and revoke that access at any time, ensuring their privacy is respected and that their information is not shared without their consent. This technology can also streamline the information-sharing process between different authorized healthcare providers, allowing access to a patient's records instantly, regardless of their location or system type.

Goals, sectors, or applications where digital assets introduces risks or harms

A. Ability of consumers, investors, and businesses to understand contracts, coding, protocols / Smart contract design and security / Frauds and scams & Potential losses associated with interacting with counterparties directly

We believe the industry's friction and pain stem primarily from building on flawed premises – choice of consensus mechanism and programming environments. We see two issues commonly related to security concerns: building a network upon Proof of Stake (PoS) and using Solidity and the Ethereum Virtual Machine (EVM) development environment; both open organizations, especially enterprise users, to risk through centralization, unsecured development, and poorly audited development environments.

PoS blockchains risk 34% attack (purchasing and staking up to 34% of the coins), which may lead to decision-making in the hands of only a few individuals or organizations. Under PoS, "the rich get richer." Due to the risk of losing funds, validators tend to outsource the complexities of staking to centralized exchanges and pools. The act of delegating capital to centralized entities creates third-party risk for users and results in centralized control of the blockchain. For instance, in February of 2020 after Tron "acquired" Steemit, the community sought to invoke a new, exact copy of the Steemit blockchain that would reduce the voting power that Tron and Steemit would have in the system. On March 2, Tron was allegedly able to coordinate with three custodial staking providers who utilized delegated capital to retain control of the blockchain.

We also regularly see Solidity development environment and EVM as significant vectors of attack and source of dangerous and costly bugs – a recent example of malicious activity through smart contracts. Solidity, which was derived from JavaScript, optimizes for wide-scale developer adoption at the cost of decreased security and auditability. Financial technology with a reductive approach to security for ease of simplicity and adoption will not serve the needs nor meet the standards of corporate, financial, and government stakeholders. Chia believes and hopes the market will coalesce around blockchains and digital assets that are inherently more secure and take cyberattack vectors with the utmost seriousness in hardening their systems from bad actors and, increasingly, nation states.

Further, EVM's account model places a central and monolithic smart contract on the blockchain where various capabilities and authorizations are stored in one long list. All transactions interact with this centralized, monolithic smart contract (for example, smart contract standards including ERC-20 assets and ERC-721 NFTs) to alter ownership accounts and amounts. By extension, the account model requires users to trust that the monolithic smart contract cannot be exploited, which is an assumption challenged by the prevalent use of multisig and upgradable smart contracts.

Broader external risks come from euphoria and lack of due diligence on the underlying technology - both at the individual and enterprise scale. We find many enterprise-suggested use cases thus far to leverage blockchain technology and digital assets incorrectly. A practical example is a company utilizing a blockchain when a database would be more effective; or seeking to tokenize an asset without any form of verification or credible standards from third-party registries.

Digital assets and blockchain are tools with specific and valuable use cases, but they create risk when stretched or applied unnecessarily with poor security considerations.

I. Area for Further Research: Jurisdictional and legal conditions

Chia believes the current regulatory framework can and should apply to digital assets and blockchains with minimal updates. While many claim that the intersection of the Securities and Exchange Commission ("SEC") and the Commodities Future Trading Commission ("CFTC") as a regulator of digital assets is confusing, we believe that both must be involved in regulating digital assets. Simply put, digital assets can be securities and commodities depending on the facts and circumstances – and are recognized by the *Howey* test.

Appropriate amendments to legislative definitions and greater collaboration between the SEC and CFTC would provide additional clarity for ecosystem participants, and ultimately, greater protection for consumers and end users from illegal activities, fraud, and other rug pulls.

Consumers should be provided details such as financial information, risk factors, and company (or token) performance to prevent bad investments – as is the norm with the purchase and sale of securities. SEC-mandated practices protect consumers. In the current ecosystem, many digital asset issuers have held an Initial Coin Offering (ICO), utilized Simple Agreements for Future Tokens (SAFTs), or conducted capital raise events in a manner which, in our opinion, creates a securities offering or investment contract. The challenge is that these aren't backed by any organizational structure or accountability, nor do they provide adequate disclosures for securities, creating significant risk for those investing in these speculative assets. If the SEC regulated such speculative assets closely, many consumers could have avoided the pain of the meltdowns that involved Terra Labs, Celsius, and other similarly situated companies.

Consumers are being harmed by the current practices of many in the ecosystem. We believe appropriate enforcement will lead to clarity and a path forward for others digital asset and blockchain companies to act in accordance with the law. Our current regulatory framework is workable and companies will adapt their business practices to include U.S. consumers.

II. Area for Further Research: "Upgradable" Smart Contracts

The novelty of blockchain technology, the dearth of available smart contract auditors, and the lack of established industry best practices and frameworks create a risky environment for consumers and entities interacting with smart contracts on a public blockchain. The Oasis multi-sig retrieval presents a recent example of potential risk. Without clear disclosures, guidance, and protocols for how a technology will be used, even in a court-ordered, white hat scenario, there exists a significant burden of knowledge in an esoteric technology to the consumer.

In the Oasis example, the organization leveraged a vulnerability in its own multi-sig capabilities to unanimously revert transactions and redirect funds. While this was done in accordance with the local laws, it demonstrates a few key fallacies in the DeFi claims of the organization and exposes challenges with smart contracts.

A company working with financial assets and advertising decentralized and safe custody should be decentralized in practice. The ability for Jump and Oasis to undo the immutability of the blockchain demonstrates elemental centralization to the smart contracting technology, creating the potential for censorship and nefarious activity (including rug pulls); a vulnerability shared by all blockchain networks using upgradable smart contracts.

Chia built its smart contract technology using Lisp, an eminently auditable and secure development environment. The Chia blockchain's coin model is also decentralized, as each coin is its own copy of a smart contract and is solely under the control of the owner. We believe more research should be conducted into smart contracting technology and the underlying development environments. Many of the exploits and largest hacks are enabled through the mutability of this technology and consumers ultimately pay the price.

Chia was founded as a better blockchain, bridging security and sustainability through an innovative approach. With over 100,000 nodes throughout the world, we believe we are setting the standard for how blockchain technology and cryptocurrencies should work.

Chia appreciates the opportunity to provide our response to the OSTP's RFI regarding the Digital Assets R&D Agenda. Please do not hesitate to contact us. We would be pleased to meet with the OSTP and its staff to discuss our response at any time.

Respectfully submitted,

[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Circle

Circle Internet Financial, LLC
[redacted]

March 3, 2023

Office of Science and Technology Policy
Executive Office of the President
[redacted]

Re: Federal Register Document 2023-01534

To Whom it May Concern:

Circle appreciates the opportunity to provide comments to the White House Office of Science and Technology Policy (OSTP), National Science and Technology Council, National Science Foundation, and the Fast Track Action Committee on Digital Assets Research and Development for the Subcommittee on Networking and Information Technology Research and Development. The establishment of a National Digital Assets Research and Development (R&D) Agenda is an essential foundation to harnessing the crosscutting benefits of cryptographic and blockchain technologies in a manner that supports economic growth and development, protects consumers, fosters responsible innovation, and promotes American competitiveness. Since Circle's founding in 2013, we have prioritized constructive engagement with policymakers and regulators in the United States as well as globally and appreciate this open dialogue in framing the long-term, whole-of-government R&D priorities.

About Circle

Circle is a global financial technology firm that provides internet-native payments and treasury infrastructure on open blockchains. Circle's foundational technology allows for the frictionless exchange of value on the internet. Circle is the sole issuer of USD Coin (USDC), a "digital dollar" also known as tokenized cash or payment stablecoin, with about $43 billion in circulation as of March 3, 2023, and issuance on eight blockchains. Circle is regulated in the United States through state money transmission licenses and USDC is always redeemable on a 1:1 basis for fiat dollars, bankruptcy remote, and fully reserved by high quality liquid assets.

USDC allows for payments that are instantaneous, immutable, cheaper than existing means of payment like wire transfers, and programmable into smart contracts. USDC has been integrated as a settlement option in leading merchant and credit card networks; supports cross-border remittances and humanitarian assistance; and is deployed as a payment option by e-commerce platforms. A full description of Circle's activities, including discussion of its operational risk management practices, terms of use and legal rights, audited financial statements, and filings with the Securities and Exchange Commission (SEC), can be found on our website.

As a financial services company, Circle's response focuses primarily on the benefits and implications of blockchain technology in the financial services industry.

1. Goals, sectors, or applications that could be improved with digital assets and related technologies.

Using public blockchains, payment stablecoins like USDC offer the near instantaneous ability to transfer funds globally with lower fees, greater transparency and finality, and more programmability than existing payment systems. By researching and developing blockchain technology and setting standards, the U.S. has the opportunity to ensure that the global digital economy is rooted in democratic principles that promote U.S. values and support American competitiveness. Circle is already seeing the below benefits being realized and notes, where applicable, where these applications advance the recommendations highlighted in the Treasury Department's September 2022 *"Future of Money and Payments"* report:[1]

Faster, Cheaper Payments with Programmable Money: Current financial architectures rely on often slow and expensive platforms — that necessitate the involvement of multiple intermediaries, parallel messaging through systems like SWIFT, correspondent banking relationships, and other cost-intensive factors — to process a single transaction. However, like the internet itself, the inherently open and peer-to-peer nature of public blockchains allows individuals and businesses to transact globally in seconds with an on-chain transaction cost as low as a few cents.[2] Payment stablecoins simplify that transaction process by serving as a financial instrument automatically written to an immutable ledger, which reduces settlement and credit risk; is inherently traceable; and facilitates real-time market information. USDC was used to settle $4.5 trillion in transactions in 2022, more than three of the top five global credit card companies combined.[3] Furthermore, the use of programmable smart contracts are already generating novel economic activity, for example, by enabling micro-payments for intellectual property and fractionalizing complex property ownership.

Significantly Reducing Transaction Costs for Cross-border Payments and Remittances: Cross-border payments like remittances are plagued by high transaction fees and, at times, delays in processing. But payment stablecoins like USDC and certain decentralized finance protocols drastically reduce costs, helping to support a more inclusive payment landscape, in line with recommendation 2 from the *Future of Money* report. Even in highly competitive remittance corridors such as the U.S.-to-EU, Circle has found that the cost of blockchain-based foreign exchange and conversion can be far lower than that of existing payment rails. A $500 remittance from USD to Euro can cost as low as $4.80 using payment stablecoins and decentralized finance rails, a small fraction relative to the global average cost of $28 through banks and $19[4] through traditional remittance operators.[5] This 80% cost reduction could translate into $30 billion in savings annually for low- and middle-income households.[6] Use of stablecoins for remittances — a $781 billion market in 2021 according to the World Bank — is already seeing significant uptake.[7]

---

[1] U.S. Department of the Treasury, *The Future of Money and Payments*, September 2022, (https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf).
[2] Circle, *State of the USDC Economy*, January 2023, (https://www.circle.com/hubfs/PDFs/2301StateofUSDCEconomy_Web.pdf), p. 14.
[3] Ibid, *State of the USDC Economy*.
[4] World Bank, *Remittance Prices Worldwide*, (https://remittanceprices.worldbank.org/).
[5] Adams et al., *On-Chain Foreign Exchange and Cross-Border Payments,* January 20, 2023, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4328948).
[6] Ibid, *On-Chain Foreign Exchange and Cross-Border Payments*.
[7] Knomad and World Bank Group, *Migration and Development Brief 37*, November 2022, (https://www.knomad.org/sites/default/files/publication-doc/migration_and_development_brief_37_nov_2022.pdf).

The largest cryptocurrency exchange platform in Latin America, with more than 3 million users, reported a 400% increase in remittance volume using USDC in 2022, up to $1 billion in remittances, or about 5% of total U.S.-Mexico remittance volume.

Overcoming "Last Mile" Problems with Humanitarian and Charitable Assistance: Due to their inherent versatility and traceability, payment stablecoins are being used to strengthen the delivery and speed of humanitarian assistance; can more effectively mitigate fraudulent abuse of aid; and serve those who lack access to traditional financial services — helping to advance a more inclusive payment landscape for disaster response and aid, in line with recommendation 2 from the *Future of Money* report. In partnership with the United Nations High Commissioner for Refugees (UNHCR) and International Rescue Committee (IRC), Circle launched a pilot program for delivering humanitarian aid to internally displaced persons (IDPs) in Ukraine in November 2022.[8] In addition to cost savings, the program allows multiple points of beneficiary validation and traceability of USDC following receipt by the beneficiary, while also serving as a safer store-of-value to IDPs. For beneficiary institutions and charities, Circle has found that the transaction costs using USDC are reduced by a conservative average of between 1.92% and 2.70% per donation compared with a traditional payment processor. Additionally, the ease and scalability of payment stablecoins attracts marginal donors by lowering the costs of transfer and empowers traditionally untapped populations to donate directly to communities in need, evidenced by the $1.25 million in USDC donated to Ukraine since the start of the Russian invasion[9] and the $500,000 donated to Turkey and Syria in the first week following the catastrophic earthquake in February 2023.[10]

Opens Paths to Financial Access: Roughly 20% of Americans today lack adequate banking services[11] and major banks in the U.S. often require customers to hold large minimum balances in order to waive account fees. Payment stablecoins and blockchain wallets provide a low-cost alternative to cash that serves as both store-of-value and means of access to digital commerce, evidenced by the fact that roughly 75% of wallets holding USDC hold less than $100, lower than all common minimum balance requirements at banks.[12] In addition to offering a cryptographically secure way for individuals to store wealth, users can also exchange their USDC for cash at tens of thousands of locations around the world.[13] Such a solution helps to increase financial access, in line with recommendation 2 from the *Future of Money* report.

Addressing Inefficiencies in the Foreign Exchange (FX) Market: The Bank for International Settlements (BIS) recognizes settlement risk in FX markets as a systemic source of risk that can

---

[8] UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine

[9] Etherscan, USDC held by address, (https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48?a=0x165CD37b4C644C2921454429E7F9358d18A45e14).

[10] Etherscan, USDC held by address, (https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48?a=0xe1935271D1993434A1a59fE08f24891Dc5F398Cd).

[11] FDIC, 2021 FDIC National Survey of Unbanked and Underbanked Households, (https://www.fdic.gov/analysis/household-survey/index.html)

[12] Wallets surveyed were on Ethereum Virtual Machine (EVM) compatible blockchains only.

[13] Circle, *Coinme Announces USDC-powered Global, Borderless Digital Cash and P2P Payments*, (https://www.circle.com/en/pressroom/coinme-announces-usdc-powered-global-borderless-digital-cash-and-p2p-payments). See also: MoneyGram, *MoneyGram Launches Pioneering Global Crypto-to-Cash Service on the Stellar Network*, (https://ir.moneygram.com/news-releases/news-release-details/moneygram-launches-pioneering-global-crypto-cash-service-stellar).

undermine financial stability, impacting one-third of daily FX turnover, or around $2.2 trillion.[14] The near-instantaneous, or "atomic," nature of payment stablecoins combined with the ability to make payment-versus-payment transactions, facilitated by distributed ledger technology, has the capability to eliminate settlement risk for FX trades. Likewise, "always-on" liquidity and settlement can reduce the chance of flash crashes or after-banking hours distortions that often afflict the FX market.[15] On-chain FX transactions between Circle's USDC and Euro-denominated payment stablecoin, Euro Coin (EUROC), are available 24/7, carry lower fees, and have consistently traded within 0.05% of the USD-Euro exchange rate.[16]

Underpinning Dollar Primacy in the Digital Economy: De-dollarization in the fiat economy has increased in recent years as a result of greater non-USD integration and efforts by countries such as China and Russia to create non-USD settlement infrastructure outside the reach of U.S. sanctions and law enforcement.[17] By contrast, regulated, USD-denominated and -backed stablecoins like USDC import robust compliance measures and the rule-of-law to the digital asset space and ensure that the USD is the reserve currency of the digital economy, which helps to protect national security in line with recommendation 4 from the *Future of Money* report.

2. Goals, sectors, or applications where digital assets introduce risks or harms.

The last year has served as a benchmark not just of the utility value of blockchain-based payment services, but also of the risks that unregulated, opaque, and offshore digital asset firms can pose to consumers and financial markets. As the White House noted in January, however, the risks and behavior seen over the last year are neither novel nor inherent to the underlying cryptographic technology.[18] As a result, many of the most prominent risks in the digital asset space — such as market manipulation, fraud, antitrust, ponzi schemes, etc. — can be effectively mitigated by extending existing financial sector safety and soundness controls, prudential standards, consumer protection, and market conduct constraints to the digital asset sector. Novel risks created or amplified by digital assets include:

Privacy and Information Safeguard Risks: While introducing important benefits in transferability and traceability over physical cash, payment stablecoins create an immutable history of activity that facilitates profiling and targeting of individuals; can be exploited by hacks and cyber fraud; and, can be used for surveillance and unauthorized data collection by criminals and foreign governments. Experts note in the February 2023 St. Louis Federal Reserve Bank Review that, "in contrast to popular belief, permissionless blockchains are completely transparent. All confirmed transactions are publicly observable and stored as part of the blockchain's history."[19] The European Union – as part of efforts to assess the data privacy risks of blockchain technology –

---

[14] Bank for International Settlements, *FX settlement risk: an unsettled issue*, December 5, 2022, (https://www.bis.org/publ/qtrpdf/r_qt2212i.htm).
[15] Bank for International Settlements, *The sterling 'flash event' of 7 October 2016*, January 2017, (https://www.bis.org/publ/mktc09.pdf)/
[16] Liao, Adams, Lader, Puth, Wan, January 2023, "On-chain Foreign Exchange and Cross-border Payments."
[17] Wall Street Journal, February 2023, "Russia Turns to China's Yuan in Effort to Ditch the Dollar," (https://www.wsj.com/articles/russia-turns-to-chinas-yuan-in-effort-to-ditch-the-dollar-a8111457)
[18] White House, "The Administration's Roadmap to Mitigate Cryptocurrencies' Risks," January 27, 2023 (https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/).
[19] Matthias Nadler and Fabian Schar, Federal Reserve Bank of St. Louis Review, February 2023, "Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers," p.1.

has found that public-key information alone can enable the identification of an individual's real-world identity and create a pattern of transaction activity that can be used to single out users.[20] Circle offers recommendations below for public-private cooperation to strike the right balance in preserving individual privacy while still being able to maximize the benefits of blockchain transparency in order to trace illicit activity.

Illicit Finance*:* While the use of virtual assets for money laundering still remains far below that of fiat currency,[21] 2022 saw a record volume of crime in the digital asset space, with more than $3.8 billion stolen in crypto hacks alone.[22] Based on Circle's review, this stems from two broad risk categories: 1) money laundering from illicit actors seeking to generate or launder the proceeds of crime; and the more prominent risk of 2) fraud, hacks, and other cyber crime directed at cryptocurrency users. Neither risk can be attributed entirely to blockchain technology and instead results from a combination of cybersecurity vulnerabilities, non-compliance with anti-money laundering and countering the financing of terrorism (AML/CFT) controls, and pooling of funds creating "honeypots" for criminals. The pseudonymous nature of blockchain allows for increased traceability using blockchain analytics but also provides a tool for non-compliant users or virtual asset service providers (VASPs) to obscure the movement of funds.

Offshore Exposure: As noted, the most prominent financial risks presented by digital assets already exist in the traditional financial sector. However, the inherently global reach of offshore VASPs amplifies the exposure of U.S. persons to illegal extraterritorial activity. These risks include traditional offshore illicit financial activities such as tax avoidance and obfuscation of beneficial ownership but also direct exposure to antitrust, fraud, money laundering, and market manipulation. These risks are further exacerbated by: the lack of domestic or international framework for digital identity management, particularly among peer-to-peer finance; weak or asymmetric data protection provisions; and differing cybersecurity standards.

Cybersecurity Risks*:* The illicit finance risks resulting from hacks and cyber crime are most prominent where honeypots are accompanied with cybersecurity vulnerabilities, such as with cross-blockchain bridge protocols or decentralized autonomous organizations. Cross-blockchain transfers alone constituted more than 50% of all crypto crime in 2022 and remain an attractive source for cyber criminals.[23] Actors exploiting such vulnerabilities include cyber criminals and rogue nation-states such as the Lazarus Group, a cybercrime syndicate linked to North Korea.[24]

---

[20] European Parliamentary Research Service, July 2019, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).
[21] Treasury Department; February 2022 National Risk Assessment; (https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf), and the September 2022 Action Plan to Address Illicit Financing Risks of Digital Assets (https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf).
[22] Chainalysis, February 1, 2023, "2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers," (https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/).
[23] Chainalysis, February 1, 2023, "2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers," (https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/).
[24] Josh Smith, "Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups - report," (https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01/).

Financial Accessibility: Existing banking infrastructure has created economies of scale that provide transaction cost reductions in proportion to transaction size. However, these cost savings remain regressive: with the greatest efficiencies, discounts, accessibility, and optionality accruing only at the wholesale level. Consumers – particularly the roughly 1-in-5 un- or under-banked Americans[25] — and small businesses in turn pay far higher costs as a percentage of value on domestic and international transfers.[26] While payment stablecoins can lower those costs, a key risk to digital financial accessibility and inclusion is the degree to which the technology is built on, or requires access to, existing banking infrastructure. Requiring a bank account to establish a digital wallet, for example, imports existing socio-economic barriers and biases from the banking sector and transposes patterns of de-risking and de-banking to the digital space.

Environmental Risks*:* The sustainability of blockchain technology remains a comparatively poorly understood risk, with little reliable research assessing the risks across consensus mechanisms or the use of scalability tools such as Layer 2 protocols or rollup architecture.[27] As a result, energy usage estimates differ widely even within a single blockchain. Available data suggests that Proof-of-Work consensus mechanisms can use up to 100,000 times the energy per transaction as a credit card transaction.[28] On the other hand, Proof-of-Stake (PoS)-based transactions can be more than 100 times as energy efficient as a credit card transaction and even degrees-of-magnitude more when batching transactions. Ultimately, more research is needed to standardize risk metrics, understand the environmental impacts, and prioritize technologies to mitigate those risks.

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

Circle recommends that the U.S. government introduce research focused on:

Compliant Privacy-Preserving Technologies: The risks accompanying identity management in the digital space exist on a spectrum, requiring an optimum balance that ensures authorities can adequately identify, trace, and prevent illicit activity while preserving consumer financial protections already enshrined in statutes like the Bank Secrecy Act (BSA). Circle recommends that the administration conduct research into technologies that preserve privacy for consumers without sacrificing AML/CFT controls or weakening standards that defend data from leakage or cyber-intrusion. As the 1999 Gramm-Leach Bliley Act makes clear, financial privacy and protections against undue exposure are fundamental rights that should be equally applicable to digital assets. Importantly, these competing risks demand a whole-of-government approach as they cross both policy functions and agency remits.

Given the transparency of most public blockchain infrastructure, users have been forced to rely on unregulated Privacy Enhancing Technologies (PETs) to retain privacy and protect personal

---

[25] FDIC; November 2022; "2021 FDIC National Survey of Unbanked and Underbanked Households;" (https://www.fdic.gov/analysis/household-survey/2021report.pdf).
[26] IMF; K. Kpodar and P. Amir Imam; "How Do Transaction Costs Influence Remittances?" p.8.
[27] Office of Science and Technology Policy, "Climate and Energy Implications of Crypto-Assets in the United States," (https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pd): 13.
[28] IMF Fintech Notes; June 7, 2022; "Digital Currencies and Energy Consumptions;" (https://www.imf.org/en/Publications/fintech-notes/Issues/2022/06/07/Digital-Currencies-and-Energy-Consumption-517866), p. 9.

identifying information (PII), rather than risk exposing sensitive data. PETs are intrinsically "dual-use," and further analysis is needed to lay out standards that preserve legitimate utility. Technical efforts to set standards have been fragmented and heterogeneous, creating a need for best-practices or government-led efforts, similar to NIST's ongoing Privacy Enhancing Cryptography project, focused on data preservation and transparency reference materials.[29] Alternatively, further research into how Layer-1 Zero-Knowledge Proof (ZKP) systems or stealth key setups,[30] harnessing elliptic curve cryptography,[31] could create BSA-compliant means to preserve privacy directly on-chain, in turn reducing the need for consumers to turn to PET solutions in the first place. OSTP should likewise explore the benefit of modernizing Gramm-Leach Bliley by establishing safeguards for centralized actors to avoid the mishandling of data during record-keeping. For example, technology used to collect IP addresses in order to abide by sanctions compliance laws can also aggregate user PII in unsafe ways, creating a data honeypot that is vulnerable to leakage or exploitation.[32]

Digital Identity Solutions: While the permissionless nature of digital asset technologies allows users to conduct transactions without intermediaries, they have also enabled a subset of actors to engage in money laundering, fraud, hacks, and cybercrime with on-chain pseudo-anonymity.[33] Further U.S. R&D on how best to incorporate digital identity tools into online systems – whether involving inherently public goods like a digital driver's license or private tools — would provide a verifiable and tested solution while allowing digital assets to remain scalable, accessible, and interoperable. Both third-party and open-source digital identity solutions can reduce some of the key risks and vulnerabilities identified in the Treasury Department's 2022 *National Money Laundering Risk Assessment* such as cross-border regulatory gaps and non-compliance.[34] Research on digital identity guidance for individual wallet owners, frameworks for credentialing, and the use of third-party KYC tools would also support a reduction in illicit finance while promoting standardization centered on U.S. regulations. Circle has taken the first steps in this effort with Verite, a set of digital identity standards that help users and institutions cryptographically prove claims about their identities to impede the activities of bad actors.[35]

Environmental Concerns: There remains a need for research into the environmental impact of various consensus mechanisms. Circle estimates, for example, that USDC transfers on the Ethereum blockchain required roughly 132.65 MegaWatt-hour (MWh) of energy to process more than 408 million transactions in 2022, equivalent to the running of only 400 refrigerators.[36] This reflects a cost of 6.366 Watt-hours (Wh) of energy per transaction, comparable to the average 1-5

---

[29] NIST Computer Resource Center, "Privacy-Enhancing Cryptography," (https://csrc.nist.gov/projects/pec).

[30] NOTE: A stealth key is a unique address, based off of a receiver's metakey, that allows the recipient to receive private transfers for each transaction without the recipient generating more keys. Elliptic Curve Cryptography is a form of Public Key Cryptography that allows for shorter public addresses while maintaining security. See FN. 29.

[31] Vitalik Buterin, "An incomplete guide to stealth addresses," (https://vitalik.eth.limo/general/2023/01/20/stealth.html).

[32] Getblock, "Blockchain RPC Provider That Won't Track You: Case of Getblock," https://getblock.medium.com/blockchain-rpc-provider-that-wont-track-you-case-of-getblock-6089028a423c.

[33] Chainalysis Team, "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Hights Amid Surge in Sanctions Designation and Hacking," (https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction/).

[34] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf): 40-42.

[35] NOTE: Learn more at https://www.circle.com/en/verite.

[36] Ethereum estimates based on the 93.4% of USDC supply located on Ethereum and roughly 5.1% of Ethereum transactions involving USDC. Solana estimates based on an annualized energy cost of 746.738 MWHs and 2.7% of USDC supply.

Wh per credit card transaction estimated by the IMF.[37] By contrast, USDC running on the Solana network requires 0.9 Whs per transaction, consuming less energy than a *single* credit card transaction. Further research by OSTP and standardization of metrics across policy priorities like sustainability and scalability would help measure impact and support government and private efforts to utilize leading technology. This would account for efficiency gains from newer blockchains like Solana or catalog the effects of the transition to PoS on the Ethereum protocol, which recently reduced the network's carbon footprint by 99.98%.[38]

Financial Accessibility Technology: In order to harness the potential for digital assets to increase financial access, the U.S. government should focus R&D efforts on enabling technologies that facilitate payments in non-traditional and underserved contexts. For example, further research into Near Field Communication (NFC)-enabled hardware would allow users to access their digital cash without reliable internet infrastructure and bolster the ease of merchant integration.[39] Coupled with other technologies such as offline "cold-storage" wallets, these innovations could secure funds for disaster relief; support added security for those unable to access traditional banking services; and provide an alternative and safer form of value storage than physical cash.[40]

Cybersecurity Safeguards*:* Smart contract protocols — and in particular bridges — represent a critical but often vulnerable[41] piece of blockchain infrastructure, enabling digital asset interoperability between walled-off networks. While blockchains with sufficiently decentralized validation architecture are generally more secure against direct manipulation, research into more advanced protocol safety and soundness audits, as well as bug detection programs, would prevent exploits of more complex systems, similar to existing Systems and Organizations Controls compliance processes.[42] To solve problems inherent to smart contract bridges, Circle has been developing a new Cross-Chain Transfer Protocol (CCTP) which eliminates the honeypots caused by conventional bridges that amplify security risks.[43] The CCTP instead relies on cryptographic attestations that USDC on the source chain has been burned, minting native USDC at the sender's destination and providing a safer environment for the transfer of value across blockchains. Research into more generalizable standards for cross-chain bridging would help secure asset transfers and cut off a critical supply of illicit financing for America's adversaries.

4. R&D that should be prioritized for digital assets.

Circle suggests the following areas in which OSTP R&D could create cross-functional benefits:

---

[37] IMF Fintech Notes; June 7, 2022; "Digital Currencies and Energy Consumptions;" (https://www.imf.org/en/Publications/fintech-notes/Issues/2022/06/07/Digital-Currencies-and-Energy-Consumption-517866), p. 9.

[38] Digitconomist, "Ethereum Energy Consumption Index," (https://digiconomist.net/ethereum-energy-consumption).

[39] John Kiff, "Taking Digital Currencies Offline," (https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline).

[40] NOTE: Financial literacy remains a key barrier to accessibility, with a 2014 S&P Global Study estimating only 57% of Americans could be considered financially literate, even among users of financial products. R&D on interoperability involving consumer testing would help bridge this divide, complementing existing literacy initiatives such as OSTP's past Change the Equation, Equal Futures or Tech Inclusion Initiatives.

[41] Chainalysis Team, "Vulnerabilities in Cross-chain Bridge Protocols Emerge as a Top Security Risk," (https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/).

[42] AICPA, "SOC 2 - SOC for Service Organizations: Trust services Criteria," (https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report).

[43] Circle Internet Financial Developers, "Cross-Chain Transfer Protocol," (https://developers.circle.com/stablecoin/docs).

Efficient Post-Quantum Signatures for Blockchains: The U.S. government has taken a number of steps to fortify our economy and critical infrastructure against the emergence of quantum computing, which collectively help keep the U.S. economy at the forefront of technological innovation.[44] NIST's recent post-quantum standardization competition for digital signature schemes was an important first step but further research is needed to adapt the results to the requirements of public blockchains, given the special requirements for blockchain signatures.[45] Until then, quantum vulnerability in blockchain signatures remains a serious threat. To bolster U.S. national security, OSTP should support research designing novel, efficient, post-quantum signature schemes with short signatures that are at least as versatile as the current signature schemes used in the blockchain ecosystem.

Efficient Post-Quantum ZKPs: ZKPs are already used by PETs in the blockchain ecosystem. They allow users to prove useful statements about transactions, such as sanctions compliance, without leaking any private information. However, the current ZKP protocols are vulnerable to quantum algorithms, and any nation or organization that successfully constructs a quantum computer with approximately 3,000 logical qubits would be able to almost instantly compromise applications that use ZKPs. While post-quantum ZKP solutions already exist, they are too inefficient to compete with their more widely used counterparts. Additionally, existing post-quantum ZKP solutions are currently prohibitively costly for real-world applications. Public blockchains generally seek to minimize the computation, storage, and network bandwidth requirements of network operation to maximize node decentralization, and R&D could help design more efficient and secure post-quantum ZKPs for use.

Cryptographic Protocols with Selective Auditing: Mirroring existing BSA standards, financial regulators want to be able to verify that risk management processes and specific transactions meet a certain set of conditions pertaining to financial crimes compliance without receiving information about all lawful transactions. Cryptographic tools based on indistinguishability obfuscation could allow software developers to generate special keys for regulators to check whether blockchain transactions meet certain policies, e.g. “transactions do not include funds originating from X blacklist AND transactions do not include amounts greater than $10,000.” Such capabilities would help financial institutions more easily verify blockchain transaction compliance with regulations while preserving the financial privacy of their users without fear of noncompliance with financial regulations.

The same building blocks could also lead to other powerful solutions, such as selective broadcast encryption where a transaction originator could identify specific parties that can read the full information of the transaction. OSTP should consider advancing research into the application of multilinear maps to generate bit-fixing pseudo-random functions as a first step toward creating these tools. Such research would in parallel support development of ZKPs that take transaction details, such as origin or amount, needed to verify compliance with AML rules. The output of the ZKP would then be verified by the regulator or financial institution, which would use a

---

[44] President Biden recently signed the Quantum Computing Cybersecurity Act which aims to promote research and development of quantum computing and cybersecurity in the United States, and the NSA recently set a 2035 deadline for the adoption of post-quantum cryptography across all national security systems.
[45] For more information about the NIST competition, *see NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, Jul. 5, 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

corresponding set of multilinear maps to check that the proof is valid without requiring access to any further details about the transaction itself. If the proof is valid, the institution, regulator, or law enforcement would have a high degree of confidence that the transaction is compliant with the relevant AML rules, without the potential for spillage of transaction details.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem.

The advancement of the digital assets ecosystem depends on the development of legal, regulatory, and supervisory models that encourage innovation while ensuring financial stability, protecting consumers, and preventing illicit finance. The U.S. should advance open and democratic principles in the digital assets ecosystem and lead in developing frameworks to create a safe and thriving marketplace for the innovations that protect the rights and interests of end users. To ensure responsible growth, consumer protection, and robust industry oversight, OSTP should focus on three key elements:

1) **The passage of legislation to bring privately-issued dollar digital currencies into the U.S. regulatory perimeter and create an acceptable supervisory framework for these novel technologies, products, and services.** Legislation should include high prudential and conduct standards for digital currency issuers, such as capital, liquidity, cybersecurity, bankruptcy, safety and soundness, and consumer protection rules. Consultations with industry during the rulemaking process following legislative passage would help ensure sound regulation and help shape the international regulatory landscape.
2) **The protection of the rights of end users with safeguards to protect citizens' use of open, secure, and transparent public blockchains and their privacy on those blockchains.** Fundamental American values such as the right to individual privacy, and freedom from unwanted data collection by governments or large corporations should guide efforts to protect users in the digital asset ecosystem. Both government and industry have an obligation to ensure that consumers are protected from harm and informed about their rights and choices when interacting with new technologies and platforms.
3) **The creation of durable frameworks for novel and rapidly evolving technologies.** The regulatory and supervisory frameworks that are ultimately created should be neutral to rapidly changing technologies and new market entrants. Oversight should include the active education and upskilling of regulators; consultation and collaboration with industry through regulatory sandbox efforts; rules to encourage fair market conduct; and public-private partnerships to educate the general public about the design and applications of digital asset technologies and financial services.

Engaging with International Standard-Setting Bodies to Enshrine American Values: The U.S. benefits from a diverse financial services sector, and its capital markets are the largest and most mature in the world due to a combination of legal and regulatory clarity and efficient and competitive markets and capital formation. As such, the U.S. should lead and frame the regulatory dialogue on innovative financial services in international fora and with global standard-setting bodies, such as the BIS, Financial Stability Board, and the the Financial Action Task Force. With the certainty afforded by legislation and regulation, Circle and other responsible industries would be better positioned to promote and defend American standards.

Circle believes that U.S. policymakers and regulators should leverage their participation in international standard setting bodies to ensure USD primacy in international markets and foster democratic values in the digital economy, such as openness, diversity, and competitiveness. U.S. leadership will be particularly important in striking a global balance between privacy from surveillance and AML/CFT compliance, such as with development of digital ID management; interoperability of public blockchains and wallets; and privacy-preserving compliance tools and enablers such as ZKPs or digital asset mixers. As these technologies proliferate, U.S. leadership in digital asset markets and blockchain-based payments systems will be crucial to the development of standards that can serve as a bulwark against authoritarian regimes which pursue top-down, invasive, and potentially coercive systems using digital assets.

Promoting Resilience and Countering Repression in the Global Digital Economy: As more than 100 countries explore central bank digital currencies (CBDCs) and cross-border CBDC settlement, several countries and international organizations have emerged as leaders in shaping the standards and application of cross-border blockchain infrastructure due to their "first mover" status. Notably, China and other countries are designing and/or piloting their own CBDCs and using the experience and expertise gained to directly feed into the supra-national efforts of organizations like the BIS to design interoperable cross-border CBDC systems.[46] China's central bank, the People's Bank of China, has been a lead collaborator in Project mBridge at the BIS, facilitating the use of its pilot CBDC, the eCNY (e-yuan or e-renminbi) in cross-border trade and investment flows, and driving interoperability between its CBDC system and that of other neighboring states.[47] The U.S. and its allies should actively engage in discussions to prevent de-dollarization and the "soft influence" that imports weak data and privacy controls, sanctions agnosticism, and state-controlled market entry into the global infrastructure governing digital assets and CBDCs.

Promoting Digital Financial Literacy: Alongside these concerns, the U.S. government should seek out ways to make nascent digital asset markets efficient, competitive, and straightforward for end users.[48] Existing financial architecture is built on familiar, but nearly 50-year old standards, and the relative youth of blockchain technology and services related to digital assets has exposed disparities that are not as readily visible in traditional financial services. For example, it can create challenges to both users and regulators in understanding the overlap with existing financial services, particularly in the peer-to-peer space. As digital asset markets mature, the U.S should devote resources and research to determine the ways in which digital asset market participants can make their offerings more accessible; disclose to consumers the potential risks associated with digital assets (including their custody and exchange); and how digital asset platforms can transparently, securely, and easily offer their services to consumers.

---

[46] Project mBridge: Connecting economies through CBDC, https://www.bis.org/publ/othp59.htm, The Bank for International Settlements. Published: October 26, 2022.
[47] Project mBridge: Ibid.
[48] For an example of digital asset financial literacy initiatives, see: https://www.circle.com/en/pressroom/circle-brings-crypto-literacy-curriculum-to-hbcus-with-circle-u

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

C.J. Poe

From: C.J. POE
To: DARD-FTAC-RFI
Subject: RFI Response: Digital Assets R&D Agenda
Date: Thursday, February 2, 2023 9:38:41 PM

Cryptocurrencies have the potential to be the best thing to happen to the United States because they offer a number of benefits that traditional fiat currencies do not. Firstly, cryptocurrencies offer faster and cheaper transactions compared to traditional banking systems. Transactions can be processed almost instantly and at a fraction of the cost of traditional bank transfers. This makes cryptocurrencies particularly useful for people in underbanked communities who may not have access to traditional financial services.

Another advantage of cryptocurrencies is that they can provide a hedge against inflation. Unlike traditional fiat currencies, the supply of cryptocurrencies is limited, which means that they are less susceptible to inflationary pressures. This makes them an attractive investment option for people looking to protect their savings from the devaluation of traditional currencies.

Finally, the decentralized nature of cryptocurrencies also allows for greater financial freedom and independence. People can make transactions without the need for a middleman or third-party, giving them greater control over their financial lives.

Overall, the emergence of cryptocurrencies has the potential to revolutionize the way that people think about and use money, making it the best thing to happen to the United States.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Coinbase Global, Inc.

coinbase

To:

Office of Science and Technology Policy
[redacted]

Date:

March 3, 2023

RFI Response: Digital Assets R&D Agenda

Coinbase Global, Inc. welcomes the opportunity to respond to the Office of Science and Technology Policy's Request for Information on "Digital Assets Research and Development." Crypto and Web3 technologies have incredible potential to innovate the finance and technology sectors, so we commend OSTP's interest in this topic.

We focus our response on the first two questions in the RFI. First, we discuss four specific goals, sectors, and applications that can be improved using crypto – these include personal identification, cross-border payments, environmental conservation, and the healthcare industry. Next, we discuss the risk the United States faces if the digital asset economy is pushed outside of the United States to international jurisdictions.

We believe that each of these topics is worthy of additional research and exploration so they can be better understood.

We appreciate your thoughtful examination of each of these issues, and look forward to continued engagement.

Sincerely,

[redacted]

Faryar Shirzad
Chief Policy Officer
Coinbase Global, Inc.

coinbase

Introduction:

Coinbase welcomes this chance to discuss research and development opportunities for the digital asset ecosystem. Crypto and Web3 have tremendous potential to improve our nation's technology infrastructure across a variety of domestic and international uses. Research on how this technology can develop, and ultimately benefit the public, will help unlock use cases that have not yet been placed at the forefront of the crypto conversation.

We are focusing on the first two questions set forth in OSTP's request for information:

- Our discussion on "goals, sectors, or applications that could be improved with digital assets and related technologies" addresses how digital asset technology can improve identity verification, cross-border payments, environmental conservation, and transmission of healthcare data. We encourage additional research on each of these topics.

- Our discussion on "goals, sectors, or applications where digital assets could introduce risks or harm" focuses on the threat to the United State's economic, national security, and technological development interests if crypto activities leave the United States as a result of a poor regulatory environment and become disproportionately located in international jurisdictions. We strongly encourage additional research on this.

How Coinbase Thinks About Crypto and Web3:

Coinbase plays an integral role in the global cryptoeconomy as the largest and only publicly-traded crypto exchange in the United States. Coinbase was founded in 2012 as an easy and trusted place to buy and sell Bitcoin. Since then, Coinbase has helped fuel the development of an entire industry with thousands of different blockchains, tokens, and projects. This includes, for example, Base – an Ethereum Level 2 network that is designed for developers to build decentralized applications onchain.

We believe that crypto will be based on the following three pillars, which recognize crypto as:

1. Investment. We want to empower everybody to achieve economic freedom through investing in and using crypto. Crypto tokens serve as an investment in the underlying network because crypto assets are the unit of account that allow networks to operate, thus facilitating other use cases.

2. New financial system. Crypto is opening up a new financial system. This means creating digital tools and services that enable people to engage in financial transactions, such as extending or receiving credit, using payment instruments, and settling payment obligations, all in a safe, compliant way. Decentralized finance and other new technologies will drive innovation and expand opportunities to improve our financial system.

3. App platform. Crypto and blockchain technologies will provide the next app platform. Fundamental to crypto is the decentralization of ownership, which gives individuals the opportunity to develop new financial and non-financial applications. Coinbase is building tools that enable individuals, institutions, and developers to plug into the crypto infrastructure to create new products and more easily use existing ones.

Much of the public conversation around crypto and Web3 is focused on the first and second pillars, related to crypto's role in finance. These areas contained the first use cases for both crypto and Coinbase, as our company was originally conceived as a platform to buy/sell Bitcoin. To be sure, these uses remain critically important. But crypto has transformed beyond just finance. Our response therefore places special focus on the third pillar, crypto as an app platform. This is the area that seasoned entrepreneurs and young developers alike are flocking to in order to harness the decentralized capabilities of Web3 and transform various facets of the economy and internet.

Question 1. Goals, Sectors, or Applications that Could be Improved with Digital Assets and Related Technologies:

Thirteen years ago, the Bitcoin whitepaper laid out how crypto assets and blockchain technology could immutably transfer value over the internet without using a centralized intermediary. In the years that have followed, a variety of use cases have emerged using this decentralized method for transmitting and storing information. In this section we explore four areas that are particularly worthy of additional research: (1) decentralized identification, (2) cross-border payments, (3) environmental conservation, and (4) healthcare.

Decentralized Identification

Decentralized identification ("DiD") offers a new form of identity management that relies on blockchain technology to solve the security, privacy, and consent issues presented by paper and digital IDs. DiD gives individuals control over their identity, rather than outsourcing identity management to a centralized authority like big tech.[1]

DiD works by relying on trusted third parties, called "issuers," to verify key identifiers. These issuers could include government agencies, universities, employers, and banks. The process of creating a DiD begins when an issuer distributes an identifying credential, such as a digital birth certificate or proof of employment. That credential is stored on a blockchain and accessible via the user's digital wallet. When a third party needs to request identifying information, like proof of good credit in the context of making a major purchase, the user presents the credential to the requester by accessing the information stored on the blockchain. This proof can be generated in a number of easily accessible ways, including as a QR code on the user's phone.

[1] *See* Decentralized Identity, What's at Stake?, International Association for Trusted Blockchain Applications (Nov. 2020).

Because the credential is stored on the blockchain and controlled by the user, there is no need for other third parties to keep a record of that credential in their own siloed databases. There is also no need for tech companies to provide federated login solutions for their products. DiD shifts the source and management of verification from centralized institutions to a decentralized ledger, while ensuring that identifying information stays fully within the control of the individual.

DiD technology is growing rapidly, with public and private innovations poised to integrate DiD into our everyday lives. The Ethereum Name Service (ENS), for example, provides the convenience of cloud-based login services while letting users retain control over the information they share with other websites. ENS makes it easy to read and share crypto addresses by mapping an easily recognizable name, such as "Christopher.eth," onto a machine-readable ENS address, which is a 40-character string of numbers and letters.

ENS has a number of potential uses in Web3. The start-up Spruce, for example, has developed a "sign in with Ethereum" feature that consumers can use to access traditional web services using their Ethereum wallet address. This means centralized Web2 sites can verify a user's identity and other relevant information without needing to store sensitive personal or financial information on their own servers. In a world where information is regularly stolen from centralized servers as a result of cyber attacks and data breaches, storing that information on fewer servers provides tangible value.

Governments are also starting to embrace DiD. A project sponsored by the European Commission is developing interoperable DiD solutions that would facilitate faster and more reliable security checks for EU citizens.[2] And as part of its national blockchain strategy, India is building a decentralized, digital platform that will host IDs and documents related to education, healthcare, and agriculture.[3] Cities like Buenos Aires are also spearheading efforts to construct DiD platforms in order to give residents access to city services and financial service providers.

Other innovative DiD projects include:

- Using DID to improve financial compliance programs at banks and virtual asset service providers, including wholly decentralized platforms. Once a customer undergoes a "know your customer," or KYC, evaluation at one institution, the institution can issue an attestation token that lets other banks or service providers rely on that same verification. These KYC analyses have the potential to be significantly more effective because they use data stored on the blockchain that is available immediately and shows a complete, constantly updated record.

---

[2] *See* The European Self-Sovereign Identity Framework Lab. The selective sharing capability of DiD is especially useful for federated governments like the United States, EU, and others, where personal information is often stored by multiple countries or states with varying security infrastructures.

[3] *See* National Strategy on Blockchain, Ministry of Electronics & Information Technology, Government of India (Dec. 2021).

- Humanitarian uses, including the use of digital credentials and biometric data to prevent the trafficking of vulnerable children by eliminating the forgeability of Power of Attorney and identity documents that typically enable illegal border crossings.[4] Another project is providing a blockchain-based platform to support drivers' licenses and land titles for the 400 million people in Africa who lack paper identification.

- In the "identity of things" domain, building a trusted vehicle data source to confirm the accuracy of used car data and the safety of vehicles by using the blockchain to track parts on the supply chain and record information on vehicles over time, including repairs, mileage, and ownership.

Recommendation: Additional research into how decentralized identification can be used by federal, state, and local governments, and the benefits this technology can bring when more fully incorporated, including for low income populations and other groups that are less likely to have conventional forms of identification.

Cross-Border Payments

The legacy process of sending money abroad is complex and costly. Traditional payment networks are relatively efficient at connecting domestic financial institutions, but rely on a slow, complicated network for international transfers. Differences in the legal requirements across countries make KYC and anti-money-laundering (AML) obligations more costly, and contractual recourse is uncertain when payment settlement fails. In addition, many remittance recipients are unbanked and live far from cashout points, so they find it difficult to convert their remittance payment to local cash currency.

For these reasons, the market for remittances has been dominated by large banks and money transfer operators like Western Union and Moneygram. The lack of competition results in little incentive for these large organizations to change their practices.

According to the World Bank, the cost of sending $200 cross-border "continued to be too high", averaging 6.4 percent in 2021.[5] While these costs are slowly decreasing over time, they are more than twice the 3 percent target set by the U.N. Sustainable Development Goal. Costs also vary considerably among different regions, service providers, and means of payment. The average cost of sending money using banks — the most expensive way to remit money — is over 10.5 percent.[6]

Crypto remittances can change this. Crypto enables individuals to send and receive remittance payments in a more efficient, less costly manner, from anywhere in the world. Assets stored in

[4] Decentralized IDs for Self-Sovereignty of Future Generations, Blockchain for Humanity Global Challenge.

[5] *See* Remittance Prices Worldwide Quarterly, the World Bank (June 2022).

[6] *Id*.

crypto wallets not only preserve value, but provide recipients the ability to participate in staking or other yield-producing services that are often not otherwise available to those who receive remittances. For those who live in high-inflation countries, cutting those losses that would otherwise be experienced due to inflation is critical.

Crypto remittance use is growing because of its practical advantages over conventional remittances, particularly in less developed countries or where there has been societal upheaval of some sort.[7] This has been demonstrated during the crisis in Ukraine, which first legalized digital assets in March 2022, in response to the millions of dollars worth of crypto aid that poured into the country at the start of the crisis.[8] The Ukrainian government found itself with urgent need of aid assistance, and yet its banking system and cross border flows were impeded. To deal with this urgent situation, the government turned to blockchain technology, and has become one of the most dramatic examples of the use case crypto. Since the start of the Ukrainian crisis, the country has received millions in financial aid through crypto, and used crypto to purchase critically needed humanitarian and defensive supplies.

Another example that demonstrates the power of crypto remittances can be seen in sub-Saharan Africa, which saw a 1,200% increase in cryptocurrency payments in recent years, placing countries like Kenya, South Africa, and Nigeria among the top nations for crypto use.[9]

The Coinbase Institute has previously estimated that consumers can save between 2-8 percent in fees when they send funds using crypto when compared to traditional payment methods.[10] For a payment of $200, that equals up to $16 in additional money going directly to the recipient rather than to intermediary institutions. Making remittance payments in crypto can also save users time because transfers happen instantly. And unlike other types of digital payments, crypto transfers are more easily accessible by the unbanked.

Recommendation: Additional research into the benefits of crypto remittance payments, and how those payments could lower fees and provide increased access to funds for populations in need, such as migrant populations.

Environmental Conservation

There has been significant public discussion regarding crypto's impact on the environment as a result of the energy required to conduct proof of work transactions. But the industry is largely transitioning

[7] Crypto Emerging as a Favored Form for Cross-Border Remittances, Pymnts (Oct 2021).

[8] Ukraine Legalizes Crypto Sector as Digital Currency Donations Continue to Pour in, CNBC (Mar 2022).

[9] The Role of Cryptocurrencies in Sub-Saharan Africa, Brookings Institute (March 2022).

[10] Crypto and Remittances, Coinbase Institute (June 2022).

to consensus mechanisms like proof of stake, which use up to 99% less energy. Even proof of work mechanisms have a number of attractive features because of their predictable energy load.[11]

In fact, crypto can promote a number of use cases that improve energy and environmental conservation efforts by allowing individuals to more readily participate in those efforts and take ownership over conservation initiatives. These use cases are developing quickly, but current examples include unlocking access to wholesale energy markets, capturing carbon credits on-chain, and incentivizing recycling.

Capturing Carbon Credits On-Chain: Carbon markets are trading systems in which carbon credits are bought and sold. One tradable carbon credit is the equivalent of reducing or avoiding one ton of carbon dioxide (or the equivalent amount of a different greenhouse gas).

Traditional carbon markets suffer from a lack of validity and transparency, and protocols put in place by governing bodies to establish validity within these markets have unfortunately seen little success.[12] In some instances credits are double counted, meaning the actual tonnage of emitted carbon being offset is lower than the number of available carbon credits would suggest. The quality of land that is used for a given carbon credit is not necessarily validated, so it is difficult to determine if a given carbon credit truly offsets the amount of greenhouse gas the credit is supposedly designed to counter. It is also increasingly difficult for smaller participants to enter the carbon market because these markets are largely catered toward large corporations.

NFTs and blockchain technology can help solve these problems. Blockchain provides a permissionless method by which carbon credits can be viewed, transferred, and traced, that is more readily accessible than traditional markets.

Web3 companies are using this technology, today, to make the carbon credit market more effective and accessible. Outsyde, Inc., for example, acquires and manages at-risk lands. Once acquired, Outsyde fractionalizes ownership of the acquired land and then distributes that fractionalized ownership interest as an NFT on the Algorand blockchain network. Using the Algorand network's microequity exchange, Outsyde can mint up to 1 million shares for each piece of property. At the end of 2022, Outsyde oversaw more than $45 million in land assets across the United States. As a result of the efficiencies afforded by its use of blockchain technology, 92% of every investment dollar it spent went toward acquiring and conserving at-risk lands.

And Outsyde is not the only example. International Finance Corporation, a World Bank Group member that focuses on investment in less-developed countries, teamed with the Chia Network last

[11] *See* Crypto and the Climate, Coinbase Institute (May 2022).

[12] *See, generally*, Voluntary Carbon Markets in ASEAN: Challenges and Opportunities for Scaling Up, Imperial College London (July 2021).

year on the Carbon Opportunities Fund, which is also designed to provide blockchain-based carbon credits.[13]

Unlocking Renewable Energy Markets: Energy markets have long been operated by a system of producers, intermediaries, and consumers. Wholesale energy producers create electricity and other forms of energy using a variety of mechanisms (fossil fuels, solar, wind, etc). Grid operators transport the energy product over a relatively long distance using physical power grids, and then local utility companies sell it to the consumer, based on the utility company's ability to more efficiently transact with consumers in that market. The utility company, in other words, acts as an intermediary.

In many communities the number of utility companies is relatively limited, and even more limited are the options for choosing where your energy ultimately comes from. But the blockchain has the ability to change that.[14]

A variety of new energy sources are penetrating the power grid, and with those new options comes the opportunity for consumers to exercise their preference as to where their energy comes from. There is a demonstrated interest among a large number of Americans in using more renewable, environmentally friendly energy sources. Just as blockchain technology can enable decentralized, peer-to-peer financial transactions, so too can it effectuate peer-to-peer exchanges of monetary value in return for energy from a given provider. This enables consumers to exercise a greater degree of preference in where their energy comes from, thus further unlocking the renewable energy market and allowing consumers to select the provider that offers the most competitive price.

The first platform to take advantage of this peer-to-peer path toward energy independence was Suncontract, which has seen great success in Slovenia and throughout Europe, and currently has more than 5,000 customers.

Incentivising Recycling: Recycling plays a major role in helping to avoid unnecessary waste. Government programs have encouraged an increase in recycling participation as a result of policy decisions designed to encourage communities to participate in recycling programs. But while recycling is on the rise, individual citizens do not necessarily have sufficient motivation to properly dispose of their waste.

The blockchain can enable governments and private enterprise alike to reward people for eco-friendly actions like recycling. Many different types or organizations are willing to reward people for disposing of their waste in a responsible, eco-friendly way – including garbage recycling plants, municipalities, companies, and even NGOs. The blockchain can thus be used to connect those organizations with consumers.

---

[13] Carbon Opportunities Fund Launches First-of-its-Kind Investment Platform to Issue Tokenized Carbon Credits, International Finance Corporation (Aug 2022).

[14] *See, generally*, Blockchain Based Decentralized Local Energy Flexibility Market, Claudia Antal Pop, *et al* (Nov 2021).

Crypto start-ups Empower and Recereum both use blockchain based platforms to connect entities that receive waste to individual consumers. Consumers using these services can scan a QR code when they submit waste to be recycled to a participating organization. The information regarding who disposed of the waste is then added to the blockchain. When the physical waste and corresponding QR code are received by the participating organization, the organization can use the QR code and corresponding blockchain information to confirm receipt, identify the consumer who provided the waste, and reward the consumer for recycling using crypto, over the exact same network that was used to relay the information regarding the waste.

Rewards-driven recycling is not new or unique to the blockchain, but the ability to relay both waste and financial information using the same rail is unique. Combined with the decentralized, efficient nature of the blockchain, a blockchain-based system of reporting waste information and providing financial rewards is more easily scaled than other options, allowing blockchain recycling incentives to more readily reach small communities and developing nations.

Recommendation: Additional research into the benefits of incorporating crypto and blockchain on environmental conservation efforts, particularly with regard to capturing carbon credits on chain, unlocking renewable energy, and incentivising recycling.

Healthcare

The current state of healthcare records is disjointed. The industry suffers from a lack of infrastructure and common standards that would allow for the safe transfer of highly personal health data. In most cases data is held in centralized, siloed locations, where it cannot be easily shared or distributed. Medical providers can find themselves receiving information that is years old – thus no longer helpful to the provider – while better, more up-to-date information sits untapped.

The Office of the National Coordinator for Health Information Technology ("ONC"), a staff division of the Department of Health and Human Services, has recognized this problem. ONC published a roadmap for improving interoperability in healthcare in 2015,[15] and has continued to address the interoperability problem since then. In 2021, ONC launched a new initiative aimed at achieving certain interoperability outcomes by 2030.[16] ONC received more than 700 submissions from the public on the interoperability challenge as part of that initiative, and then summarized the public's feedback. The summaries included the following:

- Individuals need internet-based access to their past and present electronic health information from clinical and administrative sources.

[15] Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap, Office of the National Coordinator for Health Information Technology (2015).

[16] Health Interoperability Outcomes 2030, Office of the National Coordinator of Healthcare Technology (2021).

- Individuals need the ability to seek and receive care (e.g., telehealth) without needing to gather and provide their health information themselves.
- Prior to administering care, an individual's care team should have access to updated electronic health information that reflects the latest changes in their health and care.
- Individuals need tools to set preferences and control how, with whom, and for what purposes their electronic health information is shared.
- Paper forms should no longer be used prior to receiving care.[17]

Crypto and blockchain technology can accomplish these goals. Blockchain networks can be used to store and transmit health data using smart contracts and other operations in order to solve the interoperability problem.

When a healthcare provider receives information from a patient in connection with an examination, diagnosis, or other relevant medical interaction, the provider would transmit the relevant information to a healthcare-based blockchain, where it is stored and connected to the identity of the patient in question (using the same DiD protocols discussed above). Using cryptographic encryption, personally identifiable information (PII) and Protected Health Information (PHI) would not be accessible unless the patient, who has the ability to control their information, choses to share it.

Thus, the flow of information goes as follows:

(1) Healthcare provider examines, diagnoses, or provides other health service, and tracks clinical data in its own centralized IT system;

(2) Certain data from that centralized system is automatically sent to the blockchain using APIs, and matched with the patient's DiD. The data information is stored on the blockchain and protected by encryption;

(3) Other health organizations can submit queries to the patient's public DiD in order to receive relevant information about the patient;

(4) The patient controls what information to send, and whether to submit information at all, using their private keys.

Innovators have started to build solutions specifically for the storage of healthcare information and other healthcare needs. Patientory allows users to store medical records on the "PTOYMatrix" blockchain network using information from their healthcare provider. The user has the ability to assign that information to their private key and share it later. Medicalchain provides a similar service, including verifying insurance information in order to avoid delays in care. And WholeCare focuses on using the blockchain to provide information specifically to caregivers, so that caregivers know relevant information regarding medication protocols, doctor's appointments, and other details needed to provide care for those who need it.

[17] *Id.*

Recommendation: Additional research into the benefits of using crypto and the blockchain in the healthcare industry, including possible public/private collaborations.

Question 2. Goals, Sectors, or Applications Where Digital Assets Could Introduce Risks or Harms:

The crypto industry has recently experienced a series of public failures, and in some cases, deliberate frauds, that caused some of the public to doubt the industry. That doubt is on full display in certain statements released by the Administration, including its roadmap to mitigating cryptocurrency's risks.[18] But the Administration should not allow the acts of those like FTX to cause the United States to over-rotate, and push out an industry with the potential to bring forth incredible innovation. Other jurisdictions are currently enacting and operationalising regimes that will both protect consumers and encourage the development of the crypto industry within their borders. This includes the European Union, Brazil, Australia, the United Kingdom, Singapore, UAE, Japan, and others.

Thus, we encourage OSTP to research the potential ramifications that could be experienced if crypto is pushed outside of the United States.

Coinbase has provided analysis on this issue. In January, Coinbase's Chief Policy Officer Faryar Shirzad published a piece explaining why maintaining a strong crypto industry is critical to maintaining the national security of the United States.[19] We reiterate those points here.

The presence of crypto exchanges and other intermediaries in a particular country will ensure that critical on- and off-ramps to the crypto economy operate under domestic rules and comply with any national security controls or laws that a country may impose. This helps to ensure that governments can stop bad actors who wish to move illicit funds or otherwise engage in illegal activities, thus protecting our national security objectives.

Crypto markets are also largely U.S. dollar-denominated. Around 95 percent of all crypto trades are conducted with the use of dollars or dollar-denominated stablecoins. By embracing crypto, the United States can help to ensure it retains the dominance of the dollar in crypto, thus ensuring crypto markets reinforce the strength of the U.S. dollar. At a time when central banks around the world are also exploring the potential to issue their sovereign currency in digital form – known as central bank digital currencies (CBDCs) – embracing dollar-denominated crypto assets is critical. Adoption of blockchain and distributed ledger applications in the U.S. will also ensure that its finance and technology systems remain on the cutting edge.

Recommendation: Additional research into the risks faced by the United States if the crypto industry is pushed out of the United States and relocates mostly overseas.

---

[18] The Administration's Roadmap to Mitigate Cryptocurrencies' Risks, Brian Deese, et al (Jan 2023).

[19] National Security in the Age of Digital Innovation: The Critical Role of Crypto, Faryar Shirzad (Jan 2023).

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Coinroll Inc.

RFI Response

Digital Assets R&D Agenda

Prepared for

Networking and Information Technology Research and Development (NITRD)

Jeffry Waye/CEO
[redacted]

Jay Bugg/CPO
[redacted]

Justin Taylor/CTO
[redacted]

Robert Uy/CLO
[redacted]

coinroll

Coinroll Inc.
[redacted]

[redacted]

Respondent Type: *Industry*

1. Goals, sectors, or applications that could be improved with digital assets and related technologies

In addition to our response 4.B that outlines improvements we believe the following can continue to be improved

A. **The primary sector is Finance**. The finance sector suffers from an amalgamation of rules and laws that do not adequately address the new age of digital currency. Coinroll has a strong vantage point through which to enable collaboration between industry, academia, and the government to ensure a stable, scalable method for enabling the next stages of digital global economies

B. Government involvement would be needed in **markets of transferable ownership** such as real estate, transportation, and organizational governance.

C. Blockchain and smart contracts can be a means to **automate distribution of benefits**. Veteran Affairs (VA), Supplemental Nutrition Assistance Program (SNAP), Disaster Recovery should be more accessible and accountable, however significant barriers exist to overcome. A smart contract that provides this benefit to anyone that meets the requirements. This intermediary would reduce the misuse by the individuals put in place to issue the funds; bias against underserved communities; individuals or organizations trying to misappropriate funds.

2. Goals, sectors, or applications where digital assets introduces risks or harms

In addition to our response 4.B that outlines improvements we believe the following can continue to be improved

A. Our ability to **secure individuals, businesses and institutions** that use it if we use the Bitcoin or Ethereum blockchains. *As computing technology continues to advance, we would continually be at-risk from High-Performance Computing (HPC) and Quantum computing. For example, wallet security ownership duplication/signature decryption through ML using known address exploring each reinforcement / supervised / unsupervised learning to reverse engineer decryption of unknown addresses private keys or attacks on storage security of a target's private keys.*

B. **Disruption of privacy** from malicious advertisers, threat actors and others using pattern of life models to isolate high value targets.

C. **Continued exploitation from organizations** for money laundering, circumvention of sanctions, theft, ransom and fraud. *i.e. State and non-state actors such as the State of Russian and Russian international businesses and oligarchies using bitcoin and ethereum blockchains to circumvent sanctions.*

D. The current environment, little trusted and independent 3rd party research and advice, **allows for malicious actors to easily propagate financial crimes on the chain itself**, primarily through "rug pulls".

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

A. In response to 2.A, we can expand a national lab, NSA or US Cyber Command efforts to **explore cryptography of the current and new blockchain technologies**. This would include work in homomorphic encryption and zero-knowledge proofs for evaluation and use-cases of deterrence to real-world exploits. *i.e. Los Alamos National Laboratory (LANL) Quantum Initiative and Quantum Cryptography.* Note DARPA had previously funded a vulnerability assessment of Blockchain technology with Trail of Bits[1].

B. An opportunity to research a blockchain data pipeline to secure enclaves for data enrichment of single and multi-sourced intelligence.
   a. Potentially with the **Defense Innovation Unit (DIU)** "*the only DoD organization focused on accelerating the adoption of commercial technology at speed and scale*" **whom our CTO has worked with and DIA** for Natural Language Processing (NLP) of Collection Management single and multi-sourced intelligence for DIA/CIO's global application Collection Requirements Analysis Tool for the Enterprise (CRATE).
   b. Potentially with **Tradewind** is a suite of services designed to accelerate the adoption of artificial intelligence/machine learning, digital, and data analytics solutions throughout the Department of Defense (DoD). A core pillar of Tradewind is the Tradewind Ecosystem where Industry, Academia, and other innovators can connect the Government, and identify contracting opportunities.

C. **Sentiment and behavioral analysis** of the individual, business and institutional roles with a US CBDC and the emerging trends and revelation of any novel use cases. Then **impact analysis** on domestic, cross-border and international monetary systems. Current themes for the individual are impacts on financial freedom, financial risk, availability and stability of the new system. Various modeling and simulation methods will be used to explore training and test data from real-time data pipelines as well as synthetic data generation.

Citations

1. DARPA vulnerability assessment. https://www.darpa.mil/news-events/2022-06-21

4. R&D that should be prioritized for digital assets

A. Prioritization of the **equivalent core banking services** for deposit, loan, and credit services supported by the underlying blockchain ledger and robust reporting capabilities. Coinroll understands this need for institutions and began building a multichain ecosystem for deposits, loans, and credit services which are supported by Bitcoin and Ethereum blockchain ledgers and we're building internal and external reporting capabilities.

B. Coinroll can work with the government to **set the standard for these common products and services on a new blockchain ledger**:
   a. a secure and trusted node infrastructure operated by banks, institutions, and governments
   b. Identity for individuals, businesses and governments to be accessed freely in any country's blockchain with enhancements to protecting their privacy.
   c. CBDC deposit, loan, and credit banking services
   d. Expandable to other countries to deploy and connect with for cross-chain equivalent of foreign currency exchanges, cross-border payments, international banking services.
   e. Built-in compliance with current laws and rules with reporting, support of sanctions, and the ability to react to new regulations
   f. Real-time taxation and collection
   g. Clearly identified commodity and security trading extending current and future laws and rules
   h. Obtain a new level of safety and security on in commerce that does not inherit the current systems design disadvantages identified and continued collaboration from #1 and #2 goals.
   i. Providing enforceable and reportable government investments through tax credits, grants or loans directly to parties of interest such as underserved communities in a targeted industry
   j. Upgradable security protocols
   k. A regulated Decentralized Finance (DeFi) exchange for Liquidity Pool's buyers and sellers
   l. Data enrichment of secure enclaves single and multi-source intelligence

4. Continued

C. A **modeling and simulation cloud-based platform** for the blockchain, operations, potential events, future features, laws, and rules. Working with AWS, GCP and Azure computing platforms using their AI/ML solutions that enables public internet and secure enclaves to leverage these capabilities. This will utilize responsible AI that takes strides to remove bias against underserved communities, exposure of privacy for people or communities through lack of aggregation of data processing. In addition, there needs to be explainable AI such as the work of Dr. Ryan Kramer and the Air Force Research Laboratory (AFRL) with COVID-19[2] among other many use-cases.

D. Coinroll can advise and / or build a **Treasury seized digital assets auction house** for seized cryptocurrencies, NFTs and more.

E. Coinroll can advise and / or build **Treasury digital asset savings bonds** for CBDC and/or Bitcoin, Ethereum and other Blockchains.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem

A. The Government needs to establish an environment that embraces change from the contract requirements paradigm and the **establishment of a software factory ecosystem**. These digital asset software factories have focus areas with common overlaps of purpose and collaboration in software development, data science and artificial intelligence. Examples of software factories include DoD CIO's USAF/Kessel Run, USArmy/ECMA, and 20+ more. These software factories can consist of cross-functional teams from across the government such as representatives from each department of the White House Cabinet such as State, Justice, Defense, and more, the US Federal Reserve Board, the International Monetary Fund (IMF), select governments central banks and their advisors. By having these different perspectives, purposes and areas of expertise we can have a more holistic blockchain for Digital Assets that embrace diversity. Each team will consist of Subject Matter Experts (SMEs) from the domain of interest, dedicated Software Developers shared staff from User Interface/User Experience (UI/UX), security and operations teams. Creating their own DevSecOps principals such as the DoD Reference Guide[1].

B. In response to 2.D, creating the standards similar to **Credit Rating Agencies** (S&P, Moody's and Fitch) that publish financial research and analysis on stocks, bonds, and commodities, Coinroll can provide the same for blockchains and cryptocurrencies or Digital Assets. Coinroll will supply recurring reporting based on past, present and future findings which will include a list of highest-graded Digital Assets. This will include CBDC's and/or Bitcoin, Ethereum and other blockchains.
   a. This will lead to **Innovation and regulation** of Initial Coin Offerings (ICOs), Decentralized Autonomous Organization (DAOs) and Commodity and Security Trading definitions and rules of conduct
      i. Decentralized Finance (DeFi) exchanges, their liquidity providers and DeFi exchange aggregators
      ii. Identity management for Know Your Business (KYC) / Know Your Customer (KYC) in digital assets

Citgations

1. https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
2. Dr. Ryan Kramer and AFRL machine learning and AI experts develop models for COVID-19 decision-making https://www.airuniversity.af.edu/News/Display/Article/2224113/afrl-machine-learning-and-ai-experts-develop-models-for-covid-19-decision-making/

6. Other information that should inform the R&D Agenda

A. **Blockchain is not a means of improvement** in several sectors where reliability is already established in a digital world.

   a. **Blockchain did not improve supply chains** in agriculture, transportation, smart grids, and more. Simply the act of digitizing this information resulted in massive savings due to improvements before the blockchain integration began for use of tools such as IBM's[1]. In most cases automated data collection, processing and dissemination via common Data Engineering and Analytics practices that feed into Data Science models provides significant advancement in generating insights into a supply chain.

Citgations

1. Gartner Says 80% of Supply Chain Blockchain Initiatives Will Remain at a Pilot Stage Through 2022
https://www.gartner.com/en/newsroom/press-releases/2020-01-23-gartner-says-80--of-supply-chain-blockchain-initiativ

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Consensus Networks, Inc.

Fortior Blockchain, LP

Nathan Miller, CEO
Consensus Networks, Inc.
South Bend, Indiana

Brian Haney, Partner
Fortior Blockchain, LP
Sheridan, Wyoming

Office of Science and Technology Policy
Request for Information
Digital Assets Research and Development

March 3, 2023

Information Response

Table of Contents

Dedication

All else being peripheral, this Response is inspired by and dedicated to the late and the great, Hal Finney. On March 19, 2013, Hal Finney created a topic in the Bitcoin Forum, Bitcoin and me (Hal Finney). Finney explained his contrarian response to first learning of Bitcoin,

> “When Satoshi announced Bitcoin on the cryptography mailing list, he got a skeptical reception at best. Cryptographers have seen too many grand schemes by clueless noobs. They tend to have a knee jerk reaction.”[1]

A visionary for freedom and privacy, Finney will always be a keystone to Bitcoin’s success. He was undoubtedly intimately involved in Bitcoin’s conception.

> “When Satoshi announced the first release of the software, I grabbed it right away. I think I was the first person besides Satoshi to run bitcoin. I mined block 70-something, and I was the recipient of the first bitcoin transaction, when Satoshi sent ten coins to me as a test. I carried on an email conversation with Satoshi over the next few days, mostly me reporting bugs and him fixing them.”

No matter the circumstances, Finney saw the good in life.

> “Today, I am essentially paralyzed. I am fed through a tube, and my breathing is assisted through another tube. I operate the computer using a commercial eyetracker system. It also has a speech synthesizer, so this is my voice now. I spend all day in my power wheelchair. I worked up an interface using an arduino so that I can adjust my wheelchair's position using my eyes.
>
> It has been an adjustment, but my life is not too bad. I can still read, listen to music, and watch TV and movies. I recently discovered that I can even write code. It's very slow, probably 50 times slower than I was before. But I still love programming and it gives me goals.”

Finney’s words reflect his pain and suffering after being terminally diagnosed with amyotrophic lateral sclerosis, which is commonly known as Lou Gehrig's disease. Still his strength was signified by his expressions of gratitude for the things he loved in life, including programming and the pursuit of noble goals.

[1] Hal Finney, Bitcoin and me (Hal Finney) (March 19, 2013), https://bitcointalk.org/index.php?topic=155054.0.

I. Introduction

About Consensus Networks, Inc.

Consensus Networks is a US based blockchain infrastructure provider, focused on creating secure key generation, sharing, and self-custody technologies for use in the Web3 space. Consensus Networks has been awarded SBIR contracts from the DoD and NIH for the development of Web3 and blockchain technology use cases in healthcare, logistics, and secure information sharing. Most recently, Consensus Networks has extended this technology to help users' self-custody and manage their digital assets and cryptocurrencies.

About Fortior Blockchain, LP

Fortior Blockchain, LP is a blockchain infrastructure startup focusing on the development of governance technology for applications including voting and compliance automation. The company was founded in the year 2021 after the co-founders won the top prize at the 2021 MIT Bitcoin Expo Hackathon for the development of new voting software on the Algorand blockchain. Since that time, the company has won several grant awards from non-profit foundations for the development of open-source voting and compliance technologies. Moreover, Fortior Blockchain has hosted several secure votes using its post-quantum secure voting technology[2] to handle global votes for decentralized decision making.

Information Offering

Thank you for your request for comments to identify specific opportunities related to digital assets and related technologies. Below are some insights and recommendations regarding the outlined topics.

[2] U.S. Patent Application 17,410,676, Decentralized voting using quantum intelligence (2021). *See also* U.S. Patent Application 17,375,542, Smart Contract System Using Artificial Intelligence (2021).

II. Benefits of Blockchain Technology

Supply Chain and Healthcare: Blockchain technology could be used to track medical supply chains, reducing the risk of counterfeit or low-quality products entering the market. Critically, blockchain technology can also validate chain of custody for schedule II substances to enable and greatly improve patient access to prescriptions. Decentralized blockchain networks are naturally posed to support emerging IoT and 5g technologies which depend on distributed computing to power their networks. The combination of blockchain and IoT has the potential to power truly real-time supply chains and provide businesses with better tools to manage their inventory leading to help avoid many of the shortfall issues of the past few years.

Digital Identities (DIDs): DIDs could be created using blockchain technology to provide a secure, transparent, and decentralized means of verifying an individual's identity. This could not only be used to streamline government payments in the case of social security or stimulus checks but also link information systems, like Medicare and Medicaid, to improve efficiency within these and other government programs.

Secure Voting: Interference in U.S. elections is largely being driven by substantial Russian investments in artificial intelligence (AI) cybersecurity applications.[3] One direct example includes the Internet Research Agency, a Russian intelligence company, and The Main Intelligence Directorate of the Russian Army’s hacking operations during the 2016 Presidential Election.[4] Another example includes the Cambridge Analytica Scandal, where 87 million Facebook users had their personal data exposed without their consent and used by Cambridge Analytica to support political campaigns.[5]

Blockchain voting helps solve ongoing problems in voting and election security.[6] Blockchain technology enables governments to decentralize the voting process through secure information channels, that validate and affirm voting results with an order of magnitude improvement over existing voting systems. Privacy and security are maintained on blockchains in open-source fashion by post-quantum cryptography, such as the SHA-512 hash protocol. This ensures that private information is not leaked to or manipulated by malicious attackers.

It is also an improvement over current systems, where voting records and other information are often made public without the consent of participants. Another improvement of distributed public ledger technology is the ability for voters to certify that their votes are being counted correctly.

[3] Congressional Research Service, Artificial Intelligence and National Security 24 (January 30, 2019).
[4] U.S. Department of Justice, Report on The Investigation into Russian Interference in the 2016 Presidential Election, Vol I at 4 (March 2019).
[5] Felipe González, et al., Global Reactions to the Cambridge Analytica Scandal: An Inter-Language Social Media Study 1 (2019).
[6] Emily Wells, et al., Blockchain Benefits and Risks, The Military Engineer, 62 (2018). (“Blockchain technologies are being considered as solutions to various cybersecurity and information technology threats and challenges. The Department of Defense (DOD) is evaluating blockchains for current and potential uses.”)

The public ledger allows each individual voter to check the voting record of their personal address, thus serving to increase voter confidence in the electoral process.

Electronic Cash: Although the first and most widely known use case for blockchain, electronic cash or digital currency, has the potential to greatly enhance financial access for individuals around the world. The Federal Reserve's Research and Analysis published in January 2022 does an excellent breakdown of potential impact of government adoption of electronic cash.[7]

III. Risks and Harms of Blockchain Technology

While digital assets and related technologies offer several benefits, they also introduce risks and harms.

Fraud and Illicit Activity: Although often cited as a source of fraud and other illegal activity, the immutable nature of the blockchain ledger makes fraud more difficult in the long run as users' activity is permanently recorded. Although today, some users can take advantage of the general public's lack of knowledge of the technology, in the long run, blockchain will be an effective fraud and laundering prevention tool. Other illicit activity, such as the alleged fraud at FTX, generally occurs outside of the blockchain ledger and within private transactions, usually outside of the United States, where regulators and enforcement agencies have a more difficult time tracking criminal activity. Financial regulatory frameworks could leverage blockchain technology to provide a more permanent and transparent record of transactions to reduce fraud and prevent illicit activity. Additionally, a coherent regulatory policy would ensure that many digital asset and cryptocurrency companies stayed headquartered in the United States (unlike FTX) where they can receive additional oversight.

Digital Privacy: Digital assets could introduce privacy and security concerns, particularly when personal data is stored on a decentralized blockchain network. In the case of DIDs, although they can provide improved streamlining of government programs and aid, if misused, could represent a severe threat to first amendment rights where citizens operating outside of desired norms could see increased surveillance or retaliatory action through reduction of federal benefits. For the United States to implement a DID program for its citizens, it must carefully consider first amendment and privacy considerations. Today, there is no federal digital privacy law, and such a law must go hand in hand with any DID technology implemented by the federal government.

[7] https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

IV. Proposed Research Agenda

Federal research opportunities should be introduced to continue the development of tools to counter illicit financial activities using blockchain technology. For the implementation of a Central Bank Digital Currency (CBDC), careful consideration must be given to the desire consensus mechanism for the protocol. Although blockchain technology is often viewed through a lens of an immutable ledger, the consensus mechanism, or methodology by which a distributed set of computers agrees upon the state of the blockchain, is equally, if not more important. The consensus mechanism is the primary feature which provides security to a blockchain protocol, preventing malicious actors from disrupting the chain.

A federally issued CBDC will have several difficult choices to make:

> 1) To use a private blockchain for the issuance of a CBDC. Although simplest in implementation, the benefits are marginal and security lowest. For example, since consensus is limited in a private blockchain, an administrative manager of the CBDC, if compromised or hacked, could disrupt an entire currency.
> 2) To use a public blockchain. A public blockchain would likely provide a great deal of reliability and security but would depend on public and private interests running nodes and likely reveal private information undesirable to be released about specific money flow to individuals and institutions.
> 3) To implement a custom consensus mechanism. This could be a way to blend the security and accessibility of a public blockchain with the desired privacy of a private blockchain. A custom consensus mechanism could leverage aspects of both public and private blockchains. For example, private blockchain federations could be used in clusters for private tasks and transactions with hashes of their actions recorded to a public blockchain. The public blockchain could be secured by public or private institutions, like banks or commercial blockchain service providers, which would maintain a record of public action and hashes of private actions. When private federations are audited, their records would be proven by publicly recorded hash. This would allow situational privacy with a public record for oversight as needed.

Additionally, research could be conducted for the development of digital assets that are accessible, reliable, and secure, even in areas with limited connectivity, could help bridge the digital divide and promote equity.

Technical research could be prioritized to develop better and more efficient consensus algorithms for blockchain networks, reduce energy consumption, and enhance security and privacy. Additionally, research in social sciences and interdisciplinary studies could help explore the potential impact of digital assets on various sectors, such as finance, healthcare, and identity verification. Furthermore, hardware and software development could focus on developing better tools to secure digital assets and protect against cyber threats.

The US could advance responsible innovation in the digital assets ecosystem by supporting education and workforce training related to digital assets, setting standards to ensure democratic values in the use and governance of digital assets, and maintaining access to the necessary hardware for emerging digital assets through supply chain opportunities. This would ensure that innovation in the digital assets space is grounded in ethical, social, and environmental considerations.

Collaborations between the Federal Government and other entities could help foster innovation and advance the development of digital assets. Additionally, exploring emerging areas such as decentralized finance (DeFi) and non-fungible tokens (NFTs) could create new opportunities to leverage digital assets. In conclusion, the development of a National Digital Assets R&D Agenda is a critical step in ensuring that the US remains at the forefront of digital asset innovation while also mitigating potential risks and harms.

V. Policy Considerations

A. Open Source Code is a Public Good.

With respect to code, open source software programs using digital assets for various purposes or in a decentralized way are also a public good. Open source software projects forgo the ability to drive high profit margins from proprietary software development and instead focus on product creation for the public good. Most open source projects are also decentralized because anyone around the world can contribute. Additionally, assets associated with open source projects are more likely to be used as tools, rather than passive investments. Moving forward legislation for blockchain technologies should respect the confluence of open source software and the public good.[8]

B. Agency Oversight and Respect for Constitutional Limits on Power.

Probably the biggest policy challenge for regulating digital asset securities[9] is clarity.[10] By clearly defining non-security tokens as assets not regulated by the SEC, it will ensure that opportunity can remain for open-source software projects developing blockchain technologies and digital assets. For example, adopt the following clear policy: digital assets which are not intended to represent an interest in equity or an interest in debt are not securities.

Most digital assets are not securities because most digital assets do not produce any profits solely from the efforts of others and often lack a common enterprise. In the case of decentralized assets not on a centralized exchange, any profits coming from the asset are only derivable from active

[8] The most recent legislation relating to blockchain technology is the Lummis-Gillibrand Responsible Financial Innovation Act, which was introduced to the Senate Finance Committee by Senators Lummis and Gillibrand. See Lummis-Gillibrand Responsible Financial Innovation Act (2022), https://www.congress.gov/bill/117th-congress/senate-bill/4356/all-info.

[9] There are two types of securities: equities and debt. Most cryptocurrencies and digital assets more generally are not securities, money, or debt. Instead, this new asset class is something completely new that cannot be forced e*x post* into an existing framework of legal analysis.

[10] The Lummis-Gillibrand Responsible Financial Innovation Act defines a new class of assets called ancillary assets. Ancillary assets are a specific type of security token, which have additional properties that yield additional regulation.

participation in a decentralized protocol.[11] One problem is ultimately that the SEC has a financial interest in arguing most digital assets are securities.[12] The more the SEC has authority to regulate, the more money Congress will appropriate to the agency, but SEC spending is already out of control. Between 2011 and 2021 the SEC overspent on its congressionally appropriated funds by more than 275 million dollars.

By arguing more things are securities, such as digital assets,[13] the SEC hopes to aggrandize its authority and budget.[14] Unsurprisingly, the SEC is citing regulating digital assets to support requesting a budget increase for the year 2023 to a total over $2.17 billion.[15] Yet, security tokens are actually few and far between.[16] The SEC should be incentivized to reduce spending and improve performance through the use of compliance automation technology, rather than increase spending for unconstitutional selective enforcement schemes. Moreover, the SEC should be incentivized to respect and promote the public good rather than its own bottom line.

C. Innovation is Important.

It is important that there exists incentive for America to support innovation and technical excellence in cryptography. Some straightforward mechanisms for supporting innovation include:

1. Incentive for patenting post-quantum security mechanisms.
2. Allocating small research and development grants under to open-source developers for research at the confluence of quantum computing, cybersecurity, and blockchain.
3. Milestone based performance contracts to small businesses for research and development.

There is a significant national security interest in the development of quantum security. Indeed, cyberwarfare is a global and daily battle and if the United States loses the edge, it could have catastrophic consequences.

---

[11] This is a lot of work and not consistent with traditional conceptions of securities, such as buying stock – which can be inherently passive.

[12] Fiscal Year 2023 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2021 Annual Performance Report (March 28, 2022), https://www.sec.gov/cj.

[13] For most digital assets, there is and should be no inherent expectation of profits. This is particularly true for on-chain assets, where users are only able to access new assets through direct participation in decentralized protocols, which is very different than interacting with the blockchain through a centralized exchange for example. It's important to respect the fact that utility tokens are used for specific applications and technical purposes irrespective of profits.

[14] But the collective is a network of individuals with their own respective interests and motivations. *See* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION 7 (1971). (Arguing the State's members often have interests separate and apart from the people.)

[15] Fiscal Year 2023 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2021 Annual Performance Report (March 28, 2022), https://www.sec.gov/cj.

[16] Indeed, only digital assets offered through an express ICO should be considered security tokens. An ICO is a specific type of action where a project backs a new asset with equity and then sells the asset to the public. Very few projects use an ICO, and they are generally vulnerable to much higher regulatory scrutiny for good reason. In fact, most projects decentralize assets through other mechanisms removing any common enterprise or any expectation of profit.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Cornell SC Johnson College of Business

CORNELL SC JOHNSON COLLEGE OF BUSINESS & FINTECH AT CORNELL

Response to 2023 OSTP Request for Information

SOURCE: 6/22 Cornell Convenes Roundtable Report on Digital Assets

Excerpt 1: Addressing RFI Topics 1-6

BACKGROUND ON CORNELL ROUNDTABLE REPORT:

In March of 2022, US President Joseph R. Biden issued an Executive Order on Ensuring Responsible Development of Digital Assets. Citing "profound implications for the protection of consumers, investors, and businesses, including data privacy and security; financial stability and systemic risk; crime; national security; the ability to exercise human rights; financial inclusion and equity; and energy demand and climate change," the order impels expert insight and direction on policy and research objectives and coordination, with a specific focus on the proper design and adoption of a US central bank digital currency (CBDC), establishing concepts of relative value of digital assets versus sovereign money.

Directives and schedules for government reporting are included in the full Executive Order here.

In response, Fintech at Cornell, an initiative of the Cornell SC Johnson College of Business, identified the pressing need for focused, ongoing dialogue amongst **three sectors: academics, regulators, and industry professionals**, and organized the Cornell Convenes forum described in this report. Since March, government entities have agreed with this approach [FSOC Warns Crypto is Possible Systemic Risk) (Responsible Advancement of US Competitiveness in Digital Assets] recommending focused discussions like this as valuable tools for the proper understanding and regulatory response to the rapid advent of digital assets activity.

The Cornell Convenes group was the first of its kind to address this specific agenda. Meeting for a half-day on June 6, 2022, in Washington, DC, 26 experts in academia, industry, and regulation gathered in an open discussion observing Chatham House Rule to promote openness of discussion (all in attendance may use information from the discussion but agree not to identify any speaker by name). This focused, open, same-place discussion among academics from three of the nation's top business schools, three former US regulators, and twenty current and past industry leaders achieved a forceful conferring of informed insights, respectfully working to wrangle clarity from the competing and shared priorities.

This report is authored by the Cornell FinTech Initiative together with help on the Chapters sections from many of the Cornell Convenes participants. It follows the structure of the Cornell Convenes discussion, which arranged the Executive Order's section topics into four "chapters" addressing variegated issues within digital finance, with the group identifying priorities and areas for further study. After each chapter discussion, participants had opportunities to contribute additional commentary via poster boards. The full report also provides graphics illustrating the various sector perspectives on key ideas discussed within each chapter. After the meeting, many of the assembled divided into three chapter-focused working groups which provided summaries contributing to the deep level perspectives and recommendations. Those summaries are included in the Appendix of the full report.

This excerpt reflects the Chapter 1 discussion.
To read the full Cornell Convenes Digital Assets Roundtable Report, click here.

The report works to capture and share the group's live discussion, with its free-flowing connections and associations. The goal was to encourage a bold and vigorous discussion rather than to reach broad agreement, but where strong agreement appeared, we note it here. Future discussions are planned.

Note: The contents of this work do not represent the views of Cornell University or the Cornell SC Johnson College of Business, but simply those of the individuals participating in the Cornell Convenes Roundtable.

Cornell
SC Johnson College of Business

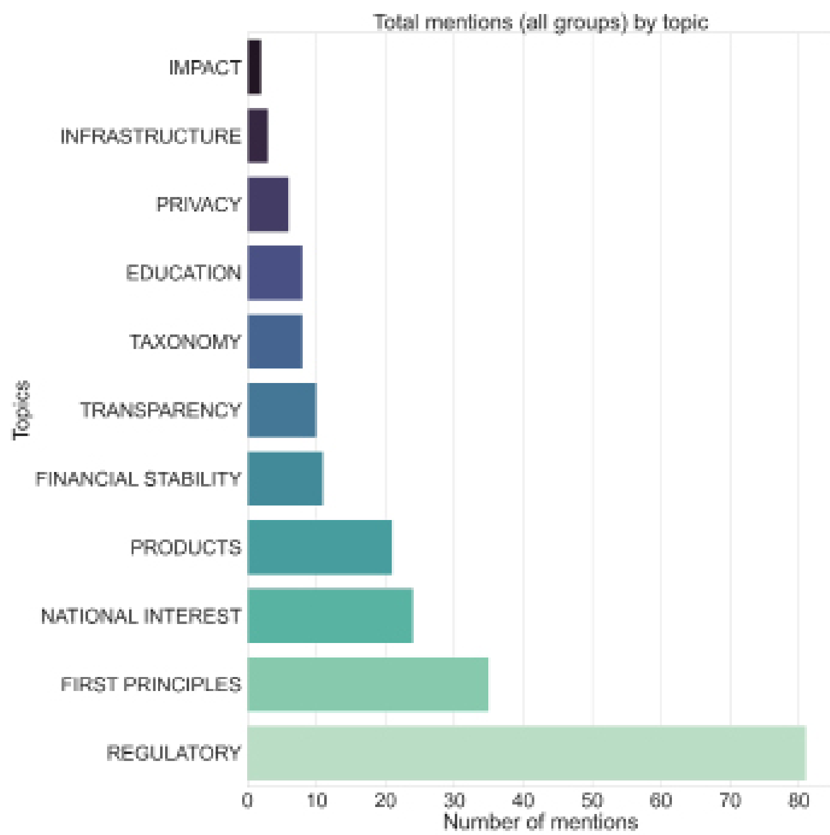
Discussion Perspectives: Breaking down group attitudes by their priorities

The group represented experienced perspectives from the fields of academia, regulation, and industry, enjoying a vivid discussion of the various considerations at play in the establishment of practices, protocols, standards, and policy regarding the development and implementation of digital currency and decentralized financial products. The discussion's specifics are summarized in this paper.

The editors extracted key ideas from each statement and classified them by topic. Using these idea- and topic-level mention counts by sector (academia, regulatory, industry), we are able to identify priorities and the level of agreement among them. We discuss a number of stylized effects in the main body of the paper, leaving the rest to the full report's APPENDIX.

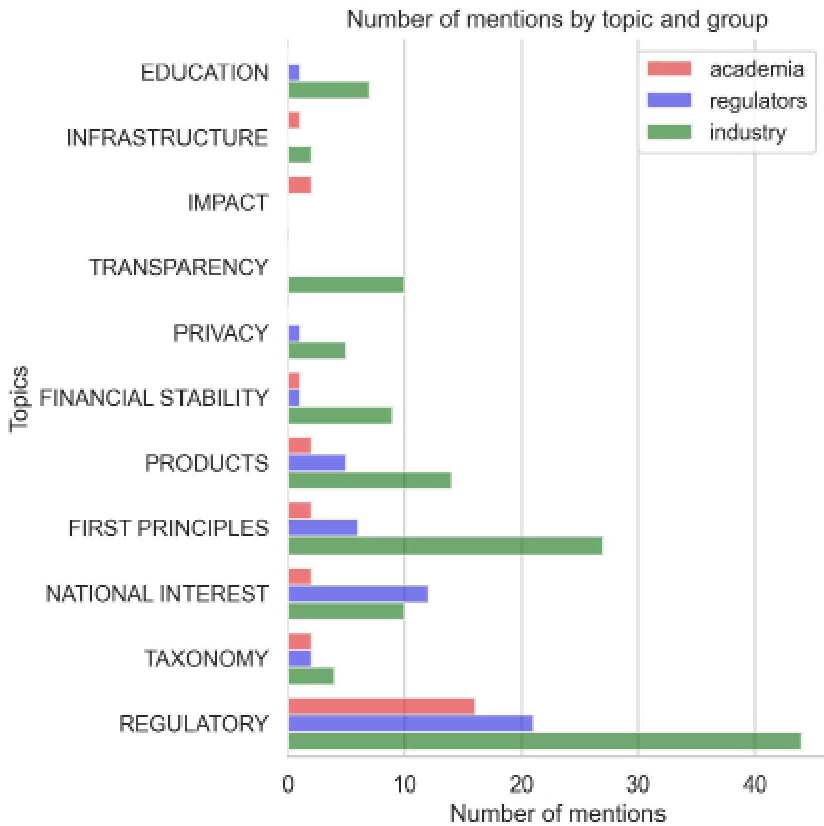
Figure 1 presents the total number of mentions by topic with the top three topics being regulatory, first principles, and national interest. Regulation considerations (when, how regulation applied and to what, with a light enough touch to encourage innovation and a strong enough hand to discourage bad actors) were at the crux of the discussion.

Fig. 1: Percentage of mentions for each group by topic



Discussion Perspectives: Breaking down group attitudes by their priorities

Fig. 2: Number of mentions (all groups) by topic and group



In Figure 2 we decompose the total topic-level mentions into counts by sector. As follows from this figure, the industry sector led in its thinking about regulatory considerations and first principles, in addition to products, transparency, national interest, and financial stability. The regulatory and academic sectors, on the other hand, showed less interest in transparency but shared as their top two priorities regulatory considerations and national interest. The third priority topic for regulators was national interest, for academia taxonomy placed third. While these indices are interesting, they must only be considered within the context of this particular conversation, and do not indicate an exclusive focus of a given sector. Note that privacy was a top priority for academics as a subset of first principles as a topic.

In the interest of exploration, we compute Pearson and Spearman correlation coefficients between idea-level mention count series for each sector. Pearson correlation measures the degree of co-movement (in terms of number of mentions), while Spearman correlation estimates the ranking agreement (how much rankings of ideas co-move between sectors). Both coefficients range from -100% to 100% with a larger magnitude indicating a stronger effect. We find that the Pearson correlation is 71%, 73% and 62% for academia-regulators, industry-regulators and academia-industry pairs respectively, while Spearman correlation coefficients are respectively 38%, 70% and 20%. Practically speaking, this indicates the highest level of agreement between the regulatory and industry sectors, while academics were closer to regulators, but had a somewhat different priority of ideas from the other two sectors.

THE DISCUSSION **INTRODUCTION**

The Cornell Convenes roundtable discussion was moderated by a professional **facilitator**, who introduced a widely-published **economist** to begin the day's discussion.

Affiliated with Cornell University and global NGOs, the economist dialed the focus toward the "transformative changes in money and influence" taking place, and emphasized this gathering as an opportunity to provide clarity.

The economist then stated that, in order to create regulatory frameworks, it is necessary to define assets, tokens, and regulatory apparati dealing with new assets and products. One of several former regulators present was instrumental in creating a taxonomy on varieties of tokens, and the economist cited this work specifically.

The economist went on to frame broader fundamental questions:

- Should the US tweak existing frameworks so that they can encompass new products, or create a new regulatory architecture?
- How can US regulators and industry make sure they can manage regulatory arbitrage?
- How does the US lead responsibly? By setting standards useful to the rest of the world?

He allowed that many sides to this question exist, some advocating for the wait-and-see approach, others arguing that since the opportunities for leadership are waning ("tech doesn't know borders and other countries are advancing; Japan is already defining its stablecoin, for instance"), waiting too long might allow a status quo to be set in unfavorable ways. "The questions of choosing issuing bodies and parameters frustrate regulators, but also point to possibilities in the technology. There's a fundamental need for systems at international level. How do we create a framework that allows innovation?"

The economist identified sticky conundra as well, summarized here:

· Crypto already has "quasi-legitimacy," since crypto holders need to report these to the IRS without the benefit of consumer protection (thus far).

· Decentralization, bitcoin mining, and ownership and decentralized finance can be characterized as "another centralization" which "could lead us to more inequities."

· Regulation will be important in terms of broader objectives. "We want new tech to lead us to a better world with more access, better-scaled rather than leading to more inequality and defining issues. What sort of regulation is best to serve markets and society?"

The economist then set the tone:

> **"It's incumbent on us to think about how we can meet these objectives and create an ecosystem that can support benefits."**

CHAPTER 1
Protecting Consumers, Investors, and Businesses (from EO Section 5)

The Cornell Convenes group delved deeply into questions on disclosure, definition, and regulation, as suggested in EO Section 5 provided below.

> **Topics strongly identified**: taxonomy, definitions, products; existing vs. new regulations (when traditional rules apply and when they don't); regulatory responsibilities balanced with protecting freedom for innovation; disclosure best practices; infrastructure; impact; leadership and competition/national and International expertise and relationships; education

THE EXECUTIVE ORDER STATES:
Sec. 5. Measures to Protect Consumers, Investors, and Businesses. (a) The increased use of digital assets and digital asset exchanges and trading platforms may increase the risks of crimes such as fraud and theft, other statutory and regulatory violations, privacy and data breaches, unfair and abusive acts or practices, and other cyber incidents faced by consumers, investors, and businesses. The rise in use of digital assets, and differences across communities, may also present disparate financial risk to less informed market participants or exacerbate inequities. It is critical to ensure that digital assets do not pose undue risks to consumers, investors, or businesses, and to put in place protections as a part of efforts to expand access to safe and affordable financial services.

Directives and schedules for government reporting are included in the full Executive Order HERE.

CHAPTER 1 DISCUSSION

The industry facilitator began the Chapter 1 Discussion, which addressed the sometimes-aligning, sometimes-competing efforts to protect consumers, investors, and businesses, **with a question:**

"Where to start? With principles, or with asset definitions?"

Industry led the response, stressing **clarity and disclosure** as imperative, central elements of consumer and investor protection.

> NOTE: Disclosure was an important topic for many, so much so that at one point the facilitator redirected the group to be more broadly focused on regulation.

An industry leader emphatically expressed the need to build trust with investors and consumers. "Nothing is more core to consumer protection than disclosure." This person said that disclosure needs to happen when things are changed, pushing information to investors where they prefer it (give access in a variety of ways), that the disclosure should be understandable, and should be frequent and consistent, and should help the reader make decisions. "If done properly, smart disclosure establishes a foundation to help this marketplace."

A former regulator replied: "When we talk about crypto, we see it as another new investable asset class, so we go to the forms we usually use. In my work on the last decade, crypto is about a new protocol, about establishing the ownership of value; internet of value: broader; I suggest we need to think about it more as an investable asset class." He argued that this approach would focus the national interest in exploring the full range of this growing field. "We need to think about investor protections in a new way."

* Disclosure: what info, to whom, by whom, for whom; education; developers; different kinds for different assets and different recipients (tech-savvy and non-tech-savvy); use cases; keeping up with changes; education working with developers on communication; enforcement AI and ML is activity based rather than entity-based but is not transparent to the non-tech-savvy; if a license is required, how is that defi? Difference between consumer protection and investor protection

An industry representative displayed that industry's particular interest in preserving openness. "This ties into a conversation about what tokens are, but what are the activities? We regulate currency because insiders have information that investors need. When you think about crypto, projects are developing protocols and issuing tokens; platforms offer trading to retail customers. The principles should start where there are information asymmetries, disclosure should be necessary, and then."

A former regulator weighed in that definitions should be the starting point, that once assets are defined, "all the jurisdictions will follow. Hybrid assets will share qualities with some things we recognize, but not completely." This person urged that all involved should "always identify: what does it look like, what kind of regulation might come into play (money laundering) but what about it is so unique that the historic way of treating it won't work?"

This jump-started the next block of discussion.

> **Editors' note:** Definitions and categorizations should consider economic functionality, legal aspects, as well as technical specifications, together with rigorous empirical analyses of existing data. To date, no common taxonomy or classifications exist.

An industry representative shared about disclosure practices – on the abundant accessibility of transaction information and the need for disclosures to be surfaced in an easy-to-find way, but in a way that is sorted and presented to be effective for the user. Implying that traditional ways won't work here, this person suggested **a different form of disclosure relevant to digital assets,** and introduced **the importance of education as a part of disclosure.** "By surfacing it with educational information, the digital asset developer can aggregate the information, and have protocols that surface with the asset."

Another industry representative stated, "Crypto is financialization of the internet; Crypto is radically transparent. I can see every elemental action with crypto, but I can't in traditional finance. This is the future of the internet: the land-grab around ownership." In later parts of the discussion, others presented additional argumentation and evidence that crypto is or can be used for other, non-financial, purposes.

Another industry expert argued that in order to develop fully-appropriate first principles, it would be necessary to "break it down into use cases, because the technology is so broad it won't fit under one framework." Again, activity is identified as a structural feature of digital finance.

TWO SYSTEMS? A lawyer reflected on the assets and the ecosystem's rapid pace of innovation, positing that perhaps two realms will evolve: "a completely separate governmental agency regulating the parallel universe."

> **Editors' note:** When relying on use-cases, definitions and activities must be clearly detailed and defined. Recent use cases for consideration include AirBnB and Uber, which challenged existing industries, leading to competition that brings more choice and better service to consumers. This is not an unknown principle in innovation, two systems evolving at the same time, to allow the market to choose what's best.

An industry representative argued, "We need to make this more accessible for consumers. Last week I spent time with **tech-savvy and non-tech-savvy.** The tech savvy say we don't need regulations; the non-tech savvy group has no idea -- doesn't understand this. There's a strong need for investor protection: the **what,** the **who**, the **how.** Perhaps (we can distinguish) a difference between the asset and the technology. So from that point of view, we can pursue the **who,** which of those players have to be a part of this process." The officer posited that the **how** could be the development of a way to deliver the technology to people. (These are) all disparate questions to take on, but we can't lose the lens of investors. The majority are not tech-savvy."

Editors' interpretation: Investors need to be educated, and disclosure needs to be made accessible to them.

An industry representative wondered whether the lawyer's comment on the fast pace of industry growth brings up an enforcement question. "Maybe the principle from the educational perspective: artificial intelligence and machine learning are useful, can identify anomalies, patterns, etcetera. We can leverage those technologies rather than policing people inside but evaluating markets in real time."

Central question: identity vs. activity

Currently regulation is based on the common approach of using individuals' identity (know your customer, identify bad actors before they can behave badly). Can regulators use the new technology for enforcement, if they base the applications on activities rather than identities/individuals? Can this enable regulators to do their work differently, more efficiently?

An industry representative recommended learning from the existing payment system, identifying what the instruments do and how they're used, and then tailoring regulation to that activity. This person agreed about leveraging technologies for enforcement. "Create crypto frameworks that are forms of payment but divided into the separate mechanisms used," they suggested.

A legal expert enforced the concept that **education is essential** to fully-functioning markets. "Consumers don't know what's under the hood of machine learning mechanisms." She recommended caution with artificial intelligence, arguing that if disclosure is automated, and consumers can't understand what's in the black box of the algorithm, then disclosure still hasn't been achieved.

A former regulator weighed in.
"Regulators in an analogue world asked, 'where are intermediaries, gatekeepers, bottlenecks?' We'll license and regulate them, will give them monopolies. This is also true in financial services; you get licenses in return for giving information to regulators. As we go into a digital world, where intermediaries are being disintermediated, what do regulators do? Traditional regulators don't know what to do. **They need to, rather than resist, accept that the same technology is going to give them tools they haven't had before, to move from an entity-based model to an activity-based model.** Start monitoring activities; that's what Amazon and eBay do – it's being done. Watching data analysis: if regulations become nodes on blockchains, they can do a better job...It will take regulators to move away from the entity-based to an activity-based system."

An IT expert suggested that lessons could be learned for this transition from the transition to e-commerce several years ago.

Editors' note: The Internet quickly became a fast growing technology. Questions regarding taxation, intellectual property, consumer protection, user agreements, privacy, and even management of the Domain Name System (DNS) immediately became topical and were addressed in a joint effort by regulators globally, industry professionals, and international organizations. For instance, in a 1997 white paper, the US Department of Commerce proposed transferring the management of the DNS to a not-for-profit private corporation. The 1999 E-Commerce OECD Guidelines provided a pathway to ensure consumer protection, while the US regulators passed the Anticybersquatting Consumer Protection Act (ACPA) and the Electronic Signature in Global and National Commerce Act protecting the flow of commerce in cyberspace. That same year, the World Intellectual Property Organization (WIPO) produced a set of rules for the Uniform Domain Name Dispute Resolution (UNDR) in an attempt to strengthen intellectual property rights in e-commerce by providing a domain name dispute resolution framework. As for taxation, in 1998 President Clinton's Presidential Decision Directives were issued to provide a favorable space for e-commerce development with a focus on network infrastructure and security. The regulatory perspective was clearly one of light touch to ensure consumer protection without impeding innovation. In a modern world with a much greater number of software and technology experts arriving at a similar resolution in the digital asset space seems feasible.

An industry expert suggested a lighter touch, to allow for innovation. **"Trying to fit blockchain into the current regulatory framework will limit the power of the blockchain, as innovations continue to be developed, which may be hampered in their growth before their usefulness can be explored."**

A legal expert agreed with this, adding, "It's dangerous to compartmentalize tech before you understand what it is. What happens to data licensing? NFT? Other applications we haven't thought of yet?" This person proposed a "do no harm" approach, "with light guardrails so that we can allow experimentation and permit useful failure along the way."

Consumer, investor, institution

A policy expert argued for **a principle to be clear about the distinction between consumer protection and investor protection**, because different rules are applied to these parties.

> **The editors see this as good food for thought.** For instance, consumer protection largely revolves around education, bad actor enforcement, and market conduct. So in thinking about how to approach digital assets, consumer education might be at the forefront on the consumer side because the availability of data onchain is not sufficiently understandable by itself to disclose risks. Investor protection from the investment provider side may speak to suitability of the investment, fair dealing, and ethical sales practices. From an institutional perspective, fair dealing comes into play with regard to disclosure of charges and fees. If these disclosures already exist onchain in real time, then what further obligation might be imagined for a financial institution regarding communication of these charges and fees?

Speaking to the regulator, the industry representative noted that "the information changes that we're seeing, when you think about money laundering and consumer protection (government requires reports over $10k), now governments can see that online. How can that translate to consumer protection? Can we use tech to reach people where they are, to disclose appropriately who they are?"

An industry leader suggested that the current dynamic is analogous to the early days of the internet and websites. "We did not anticipate people selling regulated things on websites. Sites displace businesses, tokens displace assets; we had regulated activities and then had to adapt regulations to close gaps in partnership with the private sector." This person argued that "lawyers see blockchain as transparency, but it's difficult to understand. From a policy perspective, not just disclosure for disclosure's sake, but (specifying) what kind of disclosure is helpful. (There's a) false sense of security for investors when some consumers are duped anyway. This is essentially legalized fraud." This person **sees an essential information asymmetry in the listing of the token, the asymmetry between the request for information and the information that the consumer actually sees. He strongly suggested that this gap be closed.**

> **Editors' note:** Information asymmetry can lead to some truly formidable consequences. Saber, a defi protocol built on a Solana stablecoin exchange, was purportedly created by eleven developers but found to be two brothers - Dylan and Ian Macalinao – taking advantage of anonymity and social media. With this, they managed to "build protocols that stack on top of each other, such that a dollar could be counted several times," significantly inflating the total value locked (TVL) that reached $7.5 bln. in deposits with Solana's total deposits at $10.5 bln. [70% of Solana's value was created by artificial people, making it the fourth most valuable currency at the time.] These findings question the benefits of developer anonymity and use of TVL as a major metric. They also underscore the fact that a couple of bad actors can distort cryptocurrency markets.
>
> Regulatory and law enforcement consequences for the Macaliano brothers are pending; however, a somewhat similar example comes to mind from commodity markets. In 1980, by purchasing futures contracts on margin, the Hunt brothers managed to accumulate up to one third of the entire world supply of silver with a view to manipulate its price. The Commodity Exchange (COMEX) responded by adopting "Silver Rule 7" heavily restricting purchase of commodities on margin. This led to a quick unfolding of the bubble with the silver price down over 50% in a span of four days and the Hunt brothers found responsible for conspiracy civil charges. This brings home the point that the regulatory and disclosure practices being considered and developed now for cryptocurrency assets will be crucial for creating stability in this new space and why it is so critical to have broad participation in the discussion.
>
> **TO READ MORE:** The Fake Team That Made Solana DeFi Look Huge, Coindesk, August 2022.

A former regulator contributed insight on privacy and compartmentalizing. “Crypto is a social technology, a way of interacting more widely; this can be limiting but also what’s unique here.” The enforcement agency took an activities approach. Noting that crypto wallets (places where traders store the secure digital codes needed to interact with a blockchain) act differently, he added, “there’s a permanence here that can be a disaster from the privacy standpoint. If you’re applying old principles, where’s the privacy? Everyone’s exposed once you have the addresses. What’s converging these principles? International Organization for Standardization?”

An industry leader said that with “old school applications, your database was the subserver, but with crypto, the database is the blockchain. The asset is transparent if it’s on the chain without any privacy shields.” This could imply that privacy protections will limit transparency.

> **EDITOR’S NOTE:** This line of inquiry begs the question, “what comes from this?” (WALLET/SIGNALING?). If an address is trading large amounts, the trader is free, but vulnerable because the information is accessible. Privacy implications are abundant here, and echoed throughout the rest of the discussion. One attendee suggested a different form of disclosure, relevant to digital assets, introducing **the importance of education as a part of disclosure.**
> “By surfacing it with educational information, the digital asset developer can aggregate the information, and have protocols that surface with the asset.”

A legal expert asserted several key ideas be kept in mind for disclosures of digital assets.
“I not only know **how** but **what** and **by whom**. The risks here are different than in traditional assets. (There is) a long list of information on management thinking carefully about how to tailor what’s important: **Who’s responsible for disclosure**? Does the issuer have the main disclosure obligation, while other parties can have information asymmetries? Active participants are sometimes not the issuer, but they drive the price.”
Implication: The traditional way won’t work here.

An academic wanted to “distinguish between crypto and other off-chain platforms. For assets that are traded on the blockchain, there’s the defi services and other applications, then there’s room for smart disclosure; you can see all the transactions. But providing the info to the right users...**you worry about whether disclosure is being done.” Suggestion: transparency does not equal disclosure.**

After this vigorous introduction to the issues of disclosure, the facilitator asked the group to consider other dimensions, inviting broader perspectives.

A legal expert stated that, from his perspective, disclosure was too narrow a lens on which to base a first principle. “Disclosure takes care of itself most of the time,” but also that “if you don’t see any disclosure, then the activity probably isn’t going right.” This person argued that the first principle should be around the main theme: “What is the nature of the asset? The nature of the asset is always important under the law and policy; if we’re not talking about the nature of the asset, we’re not doing law and policy right. But because of this unique world and its flexibility in moving forward, we can be moving toward a whole new world that’s more worth working toward rather than narrowly looking at what the old agencies should be regulating.”

The nature of the asset resonated with the group, and was generally agreed upon as a first principle to this discussion of the proper treatment of digital assets.

At the end of Chapter 1 discussion, the facilitator summoned the lingering question: “Do we leverage where we are today, or do we evaluate all this as it evolves?”

CHAPTER 1 TAKEAWAYS

"We will need Congressional action because the agencies (particularly SEC) will not create a constructive framework for innovation and are regulating by enforcement/stealth."

"Stablecoins are not just a 1:1 dollar or fiat-pegged token. Broader possibilities, such as a tokenized money market fund should be allowed to flourish outside of a bank/depositing institution."

BIG IDEAS

Regulators stress balance
The regulatory perspective clearly advocated the balancing of a light touch to ensure consumer protection without impeding innovation. In a modern world with a much greater number of software and technology experts, arriving at a similar resolution in the digital asset space seems feasible.

The nature of the asset matters: Products, classification, taxonomy, definitions.
All agreed the assets should be defined by their behavior, and not by identity. In this regard, some assets behave like traditional financial instruments, while others do not, and still others are developing quickly which defy any previous understandings.

Regulators stressed the need for uniform definitions, while academy and industry mentioned classification as "useful," not essential. An anonymous party did stress the need for agreement on definitions, suggesting a definition rule that defines tokens as those which do and those which don't act like assets or other products.

Standards, Disclosure, Privacy, and the importance of Transparency
Transparency as an ideal in decentralized finance and crypto currency refers to the availability of market infrastructure to any party, anywhere, who possesses the knowledge of the structure. It was argued by this group that transparency does not equal disclosure (nor does it equal consumer safety, added an industry person), because the skillset inherent in the system is not universally possessed or even understood. It was suggested by one person present that **"disclosure and education should perhaps go hand in hand."**

Disclosure, education, and licensing; education and standards
Similarly, education and the understanding of clear standards are key to transparency and to the development of industry expertise that can be trusted and shared.

Policy and Regulation, Enforcement and Innovation
Industry representatives stressed the desire to encourage innovation, through flexibility.

General agreement appeared on the need for bipartisan frameworks supporting innovation.

Do we leverage where we are today, or do we evaluate all this as it evolves?

CHAPTER 1 DATA VISUALIZATION

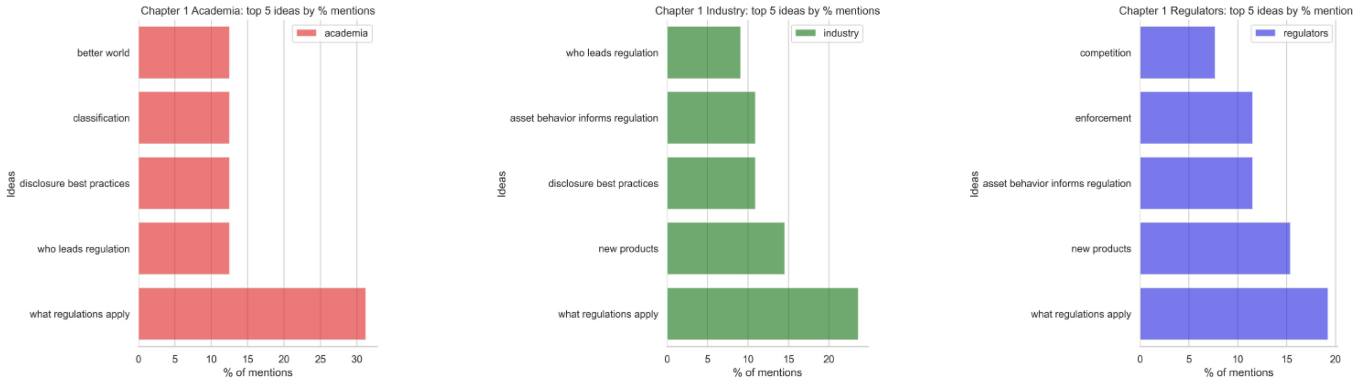


Fig. 3: Top five Chapter 1 ideas by sector

Figure 3 presents the top five Chapter 1 ideas by sector (academia, industry, regulators). The most popular idea, **what regulations apply**, is consistent across the board, while industry and regulators agree on **new products** as being the second most important. Both academia and industry consider disclosure **best practices** as the third most important idea, although that does not make the top five for regulators.

CHAPTER 1 CONCLUSION

Regulators believed strongly in the need to protect national leadership, to remain competitive, and to set policy rather than waiting for enforcement to create the guardrails. Regulators also observed the likelihood of other countries seeking to remain competitive and to be leaders; the industry noted the need for approaches unique to different countries.

CORNELL SC JOHNSON COLLEGE OF BUSINESS & FINTECH AT CORNELL

Response to 2023 OSTP Request for Information

SOURCE: 6/22 Cornell Convenes Roundtable Report on Digital Assets

Excerpt 2: Addressing RFI Topics 1-6

BACKGROUND ON CORNELL ROUNDTABLE REPORT:

In March of 2022, US President Joseph R. Biden issued an Executive Order on Ensuring Responsible Development of Digital Assets. Citing "profound implications for the protection of consumers, investors, and businesses, including data privacy and security; financial stability and systemic risk; crime; national security; the ability to exercise human rights; financial inclusion and equity; and energy demand and climate change," the order impels expert insight and direction on policy and research objectives and coordination, with a specific focus on the proper design and adoption of a US central bank digital currency (CBDC), establishing concepts of relative value of digital assets versus sovereign money.

Directives and schedules for government reporting are included in the full Executive Order here.

In response, Fintech at Cornell, an initiative of the Cornell SC Johnson College of Business, identified the pressing need for focused, ongoing dialogue amongst **three sectors: academics, regulators, and industry professionals**, and organized the Cornell Convenes forum described in this report. Since March, government entities have agreed with this approach [FSOC Warns Crypto is Possible Systemic Risk) (Responsible Advancement of US Competitiveness in Digital Assets] recommending focused discussions like this as valuable tools for the proper understanding and regulatory response to the rapid advent of digital assets activity.

The Cornell Convenes group was the first of its kind to address this specific agenda. Meeting for a half-day on June 6, 2022, in Washington, DC, 26 experts in academia, industry, and regulation gathered in an open discussion observing Chatham House Rule to promote openness of discussion (all in attendance may use information from the discussion but agree not to identify any speaker by name). This focused, open, same-place discussion among academics from three of the nation's top business schools, three former US regulators, and twenty current and past industry leaders achieved a forceful conferring of informed insights, respectfully working to wrangle clarity from the competing and shared priorities.

This report is authored by the Cornell FinTech Initiative together with help on the Chapters sections from many of the Cornell Convenes participants. It follows the structure of the Cornell Convenes discussion, which arranged the Executive Order's section topics into four "chapters" addressing variegated issues within digital finance, with the group identifying priorities and areas for further study. After each chapter discussion, participants had opportunities to contribute additional commentary via poster boards. The full report also provides graphics illustrating the various sector perspectives on key ideas discussed within each chapter. After the meeting, many of the assembled divided into three chapter-focused working groups which provided summaries contributing to the deep level perspectives and recommendations. Those summaries are included in the Appendix of the full report.

This excerpt reflects the Chapter 2 and 3 discussions.
To read the full Cornell Convenes Digital Assets Roundtable Report, click here.

The report works to capture and share the group's live discussion, with its free-flowing connections and associations. The goal was to encourage a bold and vigorous discussion rather than to reach broad agreement, but where strong agreement appeared, we note it here. Future discussions are planned.

Note: The contents of this work do not represent the views of Cornell University or the Cornell SC Johnson College of Business, but simply those of the individuals participating in the Cornell Convenes Roundtable.

Cornell
SC Johnson College of Business

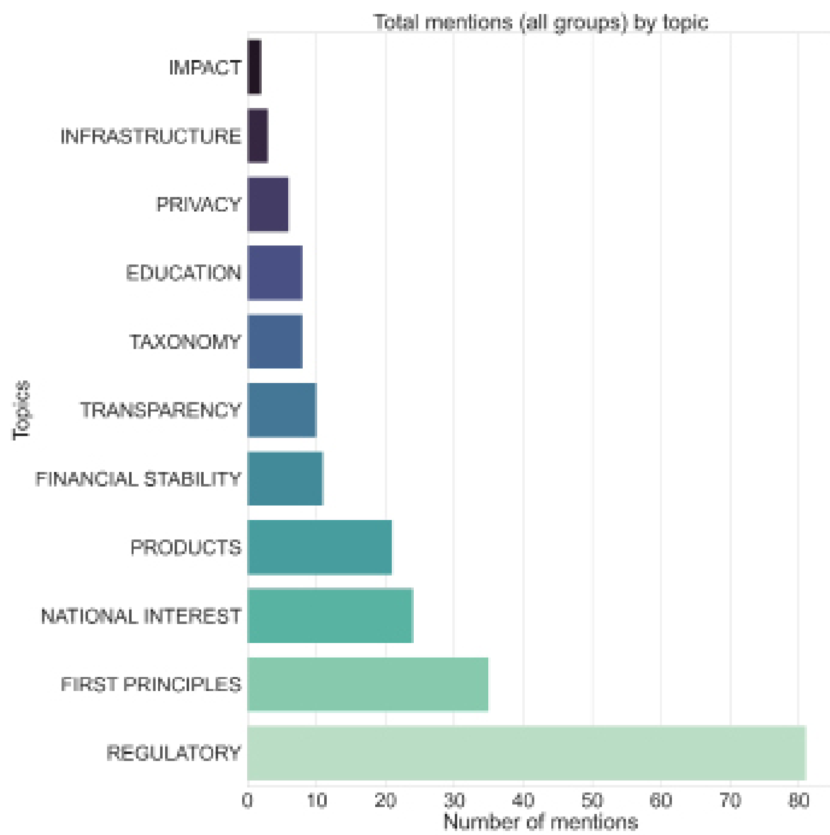
Discussion Perspectives: Breaking down group attitudes by their priorities

The group represented experienced perspectives from the fields of academia, regulation, and industry, enjoying a vivid discussion of the various considerations at play in the establishment of practices, protocols, standards, and policy regarding the development and implementation of digital currency and decentralized financial products. The discussion's specifics are summarized in this paper.

The editors extracted key ideas from each statement and classified them by topic. Using these idea- and topic-level mention counts by sector (academia, regulatory, industry), we are able to identify priorities and the level of agreement among them. We discuss a number of stylized effects in the main body of the paper, leaving the rest to the **APPENDIX.**

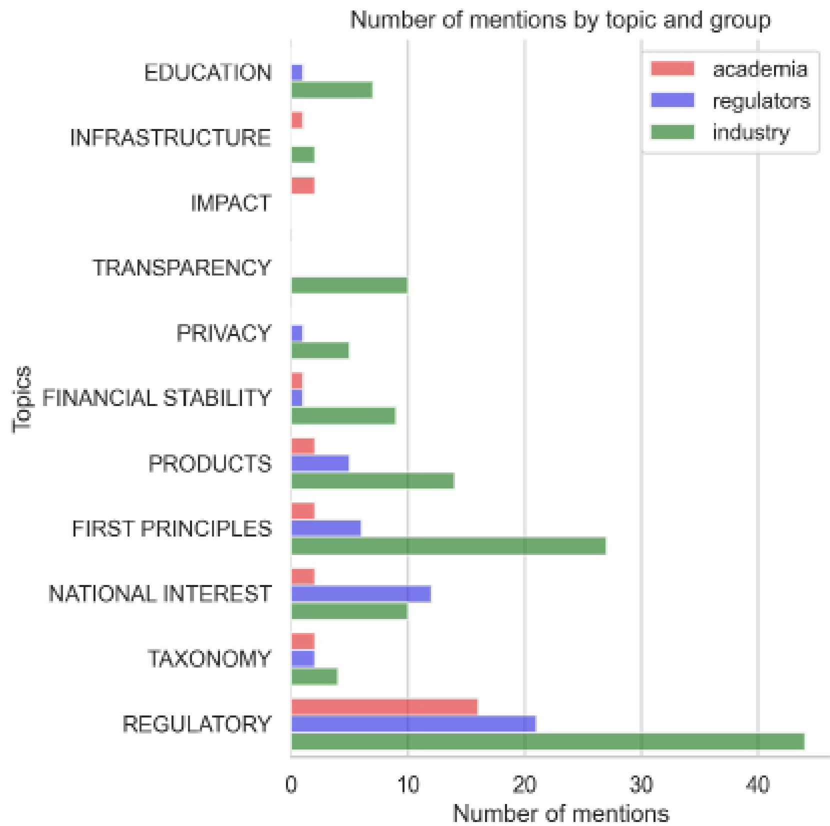
Figure 1 presents the total number of mentions by topic with the top three topics being regulatory, first principles, and national interest. Regulation considerations (when, how regulation applied and to what, with a light enough touch to encourage innovation and a strong enough hand to discourage bad actors) were at the crux of the discussion.

Fig. 1: Percentage of mentions for each group by topic



Discussion Perspectives: Breaking down group attitudes by their priorities

Fig. 2: Number of mentions (all groups) by topic and group



In Figure 2 we decompose the total topic-level mentions into counts by sector. As follows from this figure, the industry sector led in its thinking about regulatory considerations and first principles, in addition to products, transparency, national interest, and financial stability. The regulatory and academic sectors, on the other hand, showed less interest in transparency but shared as their top two priorities regulatory considerations and national interest. The third priority topic for regulators was national interest, for academia taxonomy placed third. While these indices are interesting, they must only be considered within the context of this particular conversation, and do not indicate an exclusive focus of a given sector. Note that privacy was a top priority for academics as a subset of first principles as a topic.

In the interest of exploration, we compute Pearson and Spearman correlation coefficients between idea-level mention count series for each sector. Pearson correlation measures the degree of co-movement (in terms of number of mentions), while Spearman correlation estimates the ranking agreement (how much rankings of ideas co-move between sectors). Both coefficients range from -100% to 100% with a larger magnitude indicating a stronger effect. We find that the Pearson correlation is 71%, 73% and 62% for academia-regulators, industry-regulators and academia-industry pairs respectively, while Spearman correlation coefficients are respectively 38%, 70% and 20%. Practically speaking, this indicates the highest level of agreement between the regulatory and industry sectors, while academics were closer to regulators, but had a somewhat different priority of ideas from the other two sectors.

CHAPTER 2

Limiting Illicit Finance and Associated National Security Risks Exective Order, Section 7.

Topics strongly identified: privacy, transparency, regulation, risk, unintended consequences, illicit finance

THE EXECUTIVE ORDER STATES:

(a) Digital assets have facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity. The growing use of digital assets in financial activity heightens risks of crimes such as money laundering, terrorist and proliferation financing, fraud and theft schemes, and corruption. These illicit activities highlight the need for ongoing scrutiny of the use of digital assets, the extent to which technological innovation may impact such activities, and exploration of opportunities to mitigate these risks through regulation, supervision, public-private engagement, oversight, and law enforcement.

Directives and schedules for government reporting are included in the full Executive Order HERE.

CHAPTER 2 DISCUSSION

The Chapter 2 discussion leader, an academic, began by focusing the discussion on the timing of the regulations, asking if it has so far happened "too soon, or too late?"

This led to a nuanced discussion of unintended consequences, the need for regulators to be open-minded/cooperative/knowledgeable about how to use the tech to respond to its own endemic issues and vulnerabilities, the need for information sharing and management, and recommendations for enforcement approaches. "They need to know how the tech behaves," she said.

> **The discussion leader positioned the "locus of the debate" on two questions:**
>
> a. If you regulate too soon, do regulators understand what they're regulating? Is the tech so dynamic and moving so quickly that by the time they've regulated, it's already changed?
>
> b. If you regulate too late, have the harmful consequences accumulated?

The discussion leader asserted that on this the EO is "pretty vague," but presented it as a lens for considering implications. "What's the distribution of risk? What I see is a tendency to regulate tail risk (taking our shoes off every time we fly because one person once had a bomb in their shoe)."

> **She then posed a series of questions:**
> What's the context in this digital finance realm?
> What's the risk terrain?
> What should we be thinking about in considering the problem of regulation?
> What's the risk profile in terms of what's speculated on in the EO?

The discussion leader continued: "Despite best intentions, what haven't we anticipated? Is it a question of regulation overly centralizing something whose virtue is its decentralization? **What's the tradeoff?** What now can or can't we do?"

An industry representative picked up on the issue of **unintended consequences**. He dressed down policy makers and political leaders as under pressure and "**not being careful or thoughtful enough**," and saying that their "firestorm response has created problems." As examples, this person offered activities-based regulation that has worked well until regulations created issues for the ability of law enforcement to collect information. "One thing can kill a wire fraud case," he added, referencing an **NFT fraud case** brought this year in New York's Southern District.

Continuing, this person discussed finance and the need to get the **informatio**n into the right hands. "**Regulators need to think about being open-minded in allowing the tech to solve certain problems."** Digital identity can help KYC (know your customer). "Where you don't have to have central onboarding, we can build tech that will address those problems in a way that it can operate effectively in the ecosystem. But also, with stablecoins and CBDCs, in trying to be more competitive, maybe all will operate together, but (we should be) making sure that the US is a leader here. We need to keep up with China."

First Principles Focus: Transparency and unintended consequences

Another industry representative asserted: "There's a need for this transparency. Who's perceived to be a bad actor? OPSEC SPN has six addresses; however, Chainalysis/TRM (Digital Asset Compliance and Risk Management) labs are doing heuristic scoring. Customers who are trying to move to defi want lists in order to avoid regulation…but they can't move and agencies keep the list, and only publish six addresses so people are using the government who should provide more."

An academic added that he has been personally studying intermediaries during the financial crisis, and sees a challenge to the idea of "blockchain providing a nice framework for forensic checking. The code is hard to figure out – and I have been reading this for five years – and for the regulators, too. We need to think about identity, and to protect, but the intermediaries will step in; this is the time that **the intermediary has to provide oversight regulators**." He acknowledged that this is an **identity-based approach.**

"When I talk to regulators, they're lagging behind, but the economists will think about the **unintended consequences.** Regulators don't have that much time; **it's the business schools that provide human capital to regulators**, then a positive cycle; but it's all happening so fast; regulators need more time, and I hope they're open to hiring more well-trained people."

One legal expert suggested that, while OPSEC is understood through policy, blockchain has an advantage, because you can see the chain. "You can have factors and data points and **as a former prosecutor, I'd rather have data points than one password. The whole point of the distributed social tech is that people can manage their own risk,** but also you have these different data points and you don't need to do Know-Your-Customer and can personalize their risk tolerance."

Another legal expert retorted, "I have trouble squaring the circle: bad actors are bad while privacy is good, but if we try to catch bad actors, we can ruin privacy. (And) if we don't have bad actors in mind, we're missing something. We also need to respect due process. Chainalysis, TRM do great work here. I'm not impugning their work, but **that's different than due process**, and this should be applied."

Should protocol choose the interaction, or should the individual?

TO LEARN MORE: An Anatomy of Crypto-Enabled Cybercrimes, Cong, Harvey, Rabetti, and Wu (2022)

TO LEARN MORE: Crypto Wash Trading, Cong, Li, Tang, and Yang (2020)

An industry expert added: On protocols, in illicit finance, if we make these permissions (part of the) protocol, this destroys the permissionless protocol. **How can we allow the permissionless nature to exist while protecting compliance?** Sanctions, a protocol intermediating itself, but now that an intermediary is facilitating that transaction…**every single user of the protocol can create a list of those with whom it wants to interact ("block"ing users); use TRM, insert addresses, a permissionless system, where individuals choose who they'll interact with; so that protocols don't get intermediated**.

A former regulator steered the discussion back to the discussion leader's opening about whether **regulations should come earlier or later**. "Europe goes in early, and we come in late. The two approaches show that EU has ability to export regulation. Is this an advantage? Does it cause innovators to adapt to the regulation rather than better problem-solving." This person argued that "our innovation has been better because we come in late. The downside is that crisis-based regulation is done in a rush and isn't best. **The best is for the regulations to be innovative while waiting for Congress to step in**. In 2017 there was no regulation, but bitcoin derivatives were being developed, so we hoped if we held off the innovation would advance. The two sides of this are on view now: on balance, **I agree with the US/North American approach."**

An industry voice brought the group back to the subject of illicit finance: "It's somewhat controversial: the core attribute of this technology is that it's hard to censor, hard for outsiders to regulate. **Thinking about that, the way that regulators should try to enforce rules is to focus on the on- and off-ramps, and other touch points, rather than trying to intermediate.** It's already starting: this diversion of the institutional decentralized finance (closed) but also the badlands where anonymous permissions (are happening); keeping this framework in mind."

An industry representative commented on the facilitator's point regarding geopolitics/geo-economics: "**I think the Fed turning itself into a retail bank is a good idea and that the US is losing ground and is late**." He expressed the view that, for a large stablecoin issuer, "**the air gap is a feature, not a bug**." If we're in a digital currency space, we run because political leaders provided a destination. The Europeans have a 600-page body of law. We don't have a good answer, but we should be encouraged that the US isn't waning. The dollar is the currency, the underlying rails. (This is) A critical national security objective: we moved over $6T through our pipeline, but in many countries the CBDCs obfuscate. **Who can innovate an economy?"**

> **"There are stablecoins and then there's everything else**." **-- Former SEC regulator**

This person went on to devise an approach. "Stablecoins are different from the other digital assets (we always know the issuer and algorithm, can regulate it like a fund, so some regulations are not objectionable) and then there's everything else, trading on digital exchanges. Gensler thinks they're probably trading securities, but once he thinks there's a halfway point" (as an academic had earlier asserted) **"there could be exchanges that give safe harbor. If you have something like that, you can trade there and gather and share information; but what's happening in the unregulated exchanges?"**

A proposition: "Now, you have a place where a consumer can go and buy a digital asset and at least see that the pricing is being overseen; maybe price discovery and integrity is more reliable. **Still, people can trade off-exchange…but if you want the regulated exchange, you can go there**. I **think this would address the concerns:** exchanges provide 15c2-11 seasoned securities (the recently-amended rule providing for additional disclosure by broker-dealers to potential investors, applying to both equity and fixed-income securities), and the broker/dealer certifies a certain level of information. A similar process could be put together for digital assets."

An industry representative stressed this: "The national security interest is important, but for institutions to get comfortable, we need safeguards. How risky is this? Do we outsource our understanding of this, or do we need permission? We should be striving for a world where there's consumer choice. If we can protect the privacy imperative (not assuming they're harmful or withholding information, but those who want to surrender their privacy in exchange for security). This person suggested that maybe some permissionless protocols can be preserved." **This person's firm favors the privacy imperative, "but many proactive regulations kill innovation**." He went on to show the struggle for balance, as his firm allows innovators to create best circumstances – "the things that private actors think are good for consumers and markets while also helping regulators provide protection."

Editors' note: Privacy is seen as instrumental, endangered, and fundamental

An industry representative wondered about the Web3 definition, the internet of control. "Privacy is instrumental," they put in, saying that the EU law on General Data Protection Regulation (GDPR), "is there because people don't control their information. **At what point does this data become a digital asset as well?** Then you are able to give permission. From an illicit finance perspective, education is important. Regulators could understand better."

"From the banking perspective," said one participant, "**it would be a great irony if the invention of blockchain began to realize control over the system**. It's important to balance privacy and freedom. You can't bring more than $10k in cash. There won't be a perfect regulatory solution but the idea of a government ***flowing*** every single interaction is dystopian."

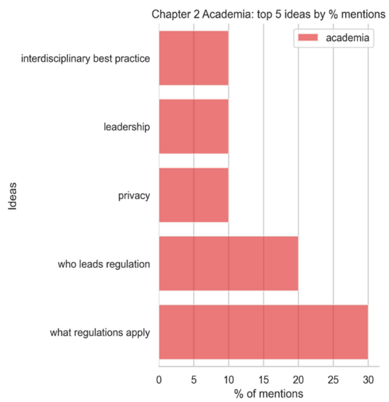
An industry expert claimed that when considering privacy and identity, "the concept of privacy is bigger than crypto. **We need to consider privacy as a fundamental right.** Europe put 600 pages into law, and we haven't thought about privacy as a right. It's limiting to see it as a trade-off. You need the overarching right, and then you apply it to different functions. Also, when you think about 24/7 markets, can we regulate in that vein, rather than just raising the hammer?"

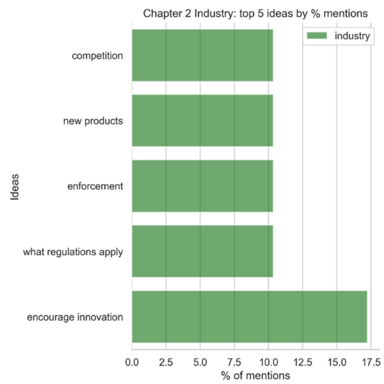
RECOMMENDED: Distinct approaches for centralized and decentralized finance.

An academic agreed about avoiding overregulation, arguing for an approach that would **distinguish between regulation for centralized and de-centralized crypto**. "There were a lot of hacks and scams on the issue of whether by regulating defi we increase the risks, but **there should be consistent systems for centralized and decentralized."**

End of Chapter 2 Discussion

CHAPTER 2: DATA VISUALIZATION





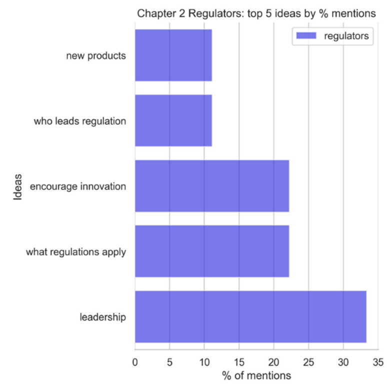


Figure 4. Top 5 Chapter 2 ideas by sector
In these figures, we can clearly see that the groups assessed the questions of illicit finance and national security from different perspectives. Ideas classified as "what regulations apply" seem to have been in focus in each group. Industry was largely interested in encouraging innovation and to a lesser extent interested in enforcement, new products and competition. Finally, central to regulators was US leadership in the field, followed by encouraging innovation.

DISCUSSION CHAPTER 2 TAKEAWAYS

General themes:

- Regulate on activity
- Provide education
- Focus on on- and off-ramps
- Be aware of surveillance potential

"Hopefully good tech will move us to activity regulation, but we need more time and education."

"Regulators should try to enforce rules is to focus on the on- and off-ramps, and other touch points, rather than trying to intermediate."

"It would be a great irony if the invention of blockchain began to realize control over the system."

CHAPTER 2: CONCLUSION

Points for further discussion include a better understanding of and control of enforcement bias. Ruling by enforcement will hamstring innovation. Industry and regulators must engage in new ways.

"When I talk to regulators, they're lagging behind, but the economists will think about the **unintended consequences.** Regulators don't have that much time; **it's the business schools that provide human capital to regulators**, then (it's a positive cycle; but it's all happening so fast. Regulators need more time, and I hope they're open to hiring more well-trained people." -- Academic

CHAPTER 3
Promote Financial Stability, Mitigate Systemic Risk, Strengthen Market Integrity (from EO Section 6)

Topics strongly identified: crisis, shocks, hacks, risk

THE EXECUTIVE ORDER STATES:
(a) Financial regulators — including the SEC, the CFTC, and the CFPB and Federal banking agencies — play critical roles in establishing and overseeing protections across the financial system that safeguard its integrity and promote its stability. Since 2017, the Secretary of the Treasury has convened the Financial Stability Oversight Council (FSOC) to assess the financial stability risks and regulatory gaps posed by the ongoing adoption of digital assets. The United States must assess and take steps to address risks that digital assets pose to financial stability and financial market integrity.

Directives and schedules for government reporting are included in the full Executive Order HERE.

CHAPTER 3 DISCUSSION

This chapter called for a shorter, more intensely focused discussion period, led by two discussion leaders.

One academic leader began by focusing on system architecture. "System risk is close to heart. I was working on it when the financial crisis happened, reflecting on two sources of systemic risk in crypto markets -- shocks, like Terra and Luna, currency which dropped in value, and then all coins are negatively affected, making transactions impossible. Then from the technological cohort: smart coins, open source -- then some softer; most of the time; the softwares can be hacked." He briefly discussed the Monox blockchain, in which 31 million dollars in digital coins were stolen. "What about relying on the importance of ensuring continuity of service? We want to transition to software where we can transition quickly." He invited the group's thoughts.

See: The Crypto World Is on Edge After a String of Hacks, New York Times, 9/28/22

The other discussion leader, bringing the industry perspective, commented on these well-known crises (hacks and thefts) and argued that regulators failed.

"Today we've prepared for big tech or Libra or China tech or gov tech. What blew up first was **Terra,** which got big quick, and failed the most basic of tests: show me the money. If you want to meet that simplest of tests, where in the payment system does it belong?" At his company, he continued, "we follow a model with no leverage. We could give custody to the Federal Reserve. Stablecoin is a lightning rod since 2019, but innovation on the margin creates correlations. (**Tether** should be discussed: an exposure to the real economy) The idea is that a stablecoin could break the buck."

Regulators are slow, that person argued. "They saw the Terra structure in 2017; didn't understand it; and where are the regulators then if everything is a security? Not only did the regulators fail, but the basic due diligence failed as well (vaporware). Since September, I talked to Terra four times; got no answers; **these are red flags I've got to believe that someone in the government should have seen.**

An industry leader added questions: "On the risk piece, we're not addressing systemic risk in stablecoin, it's just an extrapolation of what US is doing with the dollar? Are we just extending the impact into other parts of the economy that are now going to be dependent on stablecoin? How are we **dimensionalizing?"**

Another industry voice advised caution: "We have to be careful in thinking about systemic risk: contagion into traditional financial markets, interconnectivity that causes damage to the real economy, not just about individual losses."

Industry then parried:

"Stablecoins also have design flaws of financial architecture; we are talking about Terra because it collapsed. But (here's a) question: commercial paper, not backed by fiat, then: liquidity; how are we doing stablecoins –they are de-centralized in that they use blockchain but they have a centralized issuer; still not transparent enough."

"We won't understand Terra; I agree with (bitcoin developer counsel): the collapse of Terra is an example of something not systemically important --not impactful on markets or overall environment. But agree that different stablecoins are constructed differently."

"On the earlier point about systemic risk and engineering, the risk management we discuss is about regulation and bad actors, but when engineering isn't done well." Citing the Ether transaction in which $34 million became permanently locked up in a smart contract, he recommended, "**We also need to educate engineers and set up risk protocols. That kind of mistake at a systemic level could be huge and is possible."**

"Terra was comparably the size of Lehman when it fell. I was at Barclays when they bought Lehman; **I saw the rails rewritten** into a hopefully better way. Decentralized text, by design better solves systemic risk problems, intermediaries and off-ramps (can be designed) so people can participate on their own accord and account for their risk."

"Do these (open-sourced protocols) regulate risk better? If they're open-sourced, who's maintaining them? What incentives make sure these protocols are being handled properly?"

"With $1B US invested, we shouldn't dismiss algorithmic stablecoins. Terra was a mistake but shouldn't cause us to dismiss the system. How did that become a systemic risk? **Sandbox dynamic adds controls..."**

CHAPTER 3: TAKEAWAYS

"(The) challenge is that digital assets aren't just a protocol; they are used for payments and investments, which raise additional issues. Innovation by itself is not enough."

"**We also need to educate engineers and set up risk protocols. That kind of mistake at a systemic level could be huge and is possible."**

CHAPTER 3 DATA VISUALIZATION

Figure 5. Top 5 chapter 3 ideas by sector

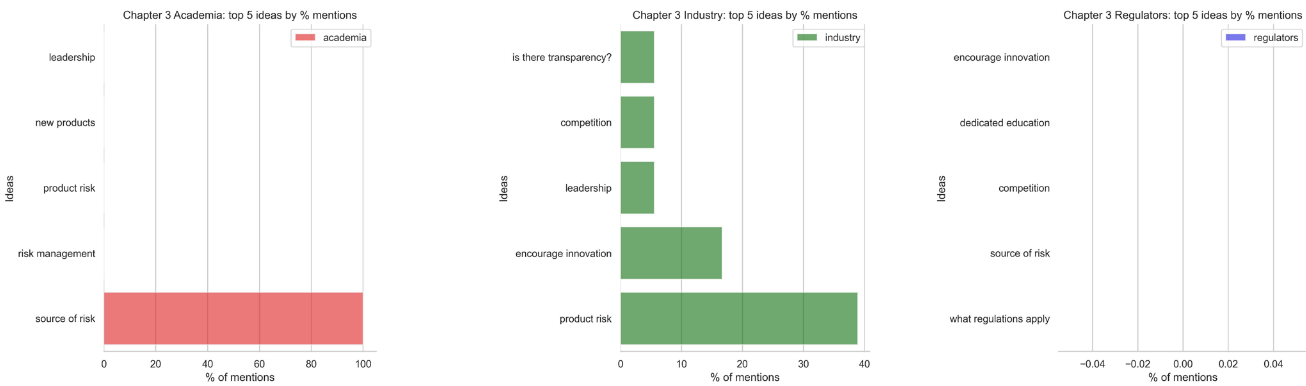


Figure 5. Summary

Figure 5 shows industry representatives focused on the ideas of product risk, innovation encouragement and leadership, while academics provided input on the sources of risk and regulators stayed silent. Industry representation greatly outnumbered academic and regulatory sectors in the discussion.

CHAPTER 3 CONCLUSION

Crypto currency is still segregated, although there is statistical evidence of contagion. The 2018 crypto crash (correlations between assets go up). Before COVID, this regression model showed correlations between stock and crypto prices (was bitcoin acting as an inflation hedge? No inflation in 2018 but an interest rate depression?), and in 2019 the term spread so the yield curve of the bond was inverting (even before COVID we knew that recession was coming).

CORNELL SC JOHNSON COLLEGE OF BUSINESS & FINTECH AT CORNELL

Response to 2023 OSTP Request for Information

SOURCE: 6/22 Cornell Convenes Roundtable Report on Digital Assets

Excerpt 3: Addressing RFI Topics 1-6

BACKGROUND ON CORNELL ROUNDTABLE REPORT:

In March of 2022, US President Joseph R. Biden issued an Executive Order on Ensuring Responsible Development of Digital Assets. Citing "profound implications for the protection of consumers, investors, and businesses, including data privacy and security; financial stability and systemic risk; crime; national security; the ability to exercise human rights; financial inclusion and equity; and energy demand and climate change," the order impels expert insight and direction on policy and research objectives and coordination, with a specific focus on the proper design and adoption of a US central bank digital currency (CBDC), establishing concepts of relative value of digital assets versus sovereign money.

Directives and schedules for government reporting are included in the full Executive Order here.

In response, Fintech at Cornell, an initiative of the Cornell SC Johnson College of Business, identified the pressing need for focused, ongoing dialogue amongst **three sectors: academics, regulators, and industry professionals**, and organized the Cornell Convenes forum described in this report. Since March, government entities have agreed with this approach [FSOC Warns Crypto is Possible Systemic Risk) (Responsible Advancement of US Competitiveness in Digital Assets] recommending focused discussions like this as valuable tools for the proper understanding and regulatory response to the rapid advent of digital assets activity.

The Cornell Convenes group was the first of its kind to address this specific agenda. Meeting for a half-day on June 6, 2022, in Washington, DC, 26 experts in academia, industry, and regulation gathered in an open discussion observing Chatham House Rule to promote openness of discussion (all in attendance may use information from the discussion but agree not to identify any speaker by name). This focused, open, same-place discussion among academics from three of the nation's top business schools, three former US regulators, and twenty current and past industry leaders achieved a forceful conferring of informed insights, respectfully working to wrangle clarity from the competing and shared priorities.

This report is authored by the Cornell FinTech Initiative together with help on the Chapters sections from many of the Cornell Convenes participants. It follows the structure of the Cornell Convenes discussion, which arranged the Executive Order's section topics into four "chapters" addressing variegated issues within digital finance, with the group identifying priorities and areas for further study. After each chapter discussion, participants had opportunities to contribute additional commentary via poster boards. The full report also provides graphics illustrating the various sector perspectives on key ideas discussed within each chapter. After the meeting, many of the assembled divided into three chapter-focused working groups which provided summaries contributing to the deep level perspectives and recommendations. Those summaries are included in the Appendix of the full report.

This excerpt reflects the Chapter 4 discussion.
To read the full Cornell Convenes Digital Assets Roundtable Report, click here.

The report works to capture and share the group's live discussion, with its free-flowing connections and associations. The goal was to encourage a bold and vigorous discussion rather than to reach broad agreement, but where strong agreement appeared, we note it here. Future discussions are planned.

Cornell
SC Johnson College of Business

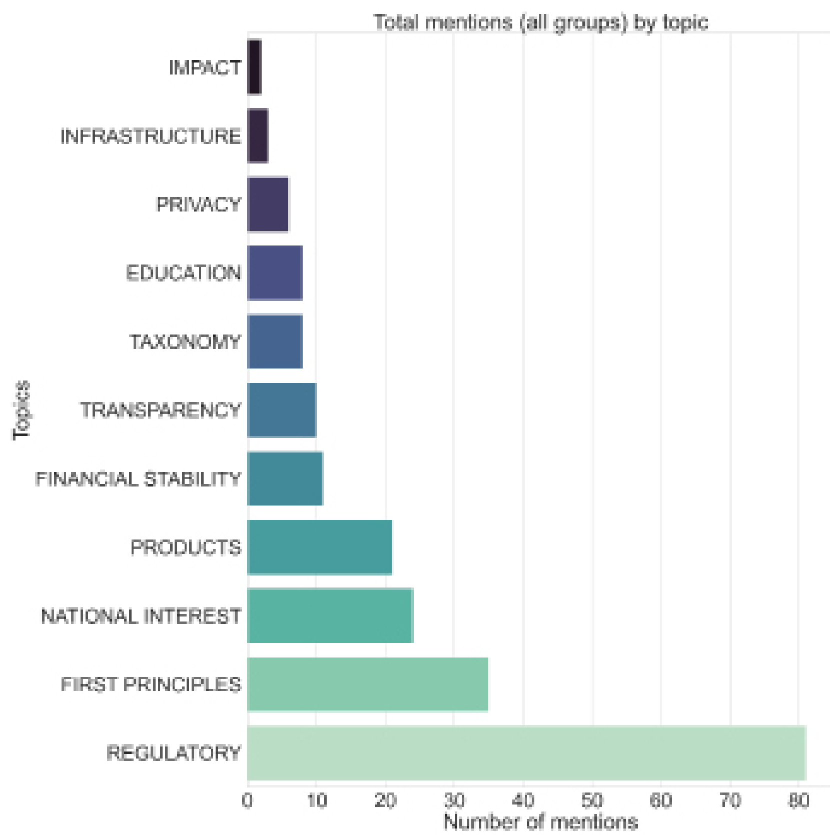
Discussion Perspectives: Breaking down group attitudes by their priorities

The group represented experienced perspectives from the fields of academia, regulation, and industry, enjoying a vivid discussion of the various considerations at play in the establishment of practices, protocols, standards, and policy regarding the development and implementation of digital currency and decentralized financial products. The discussion's specifics are summarized in this paper.

The editors extracted key ideas from each statement and classified them by topic. Using these idea- and topic-level mention counts by sector (academia, regulatory, industry), we are able to identify priorities and the level of agreement among them. We discuss a number of stylized effects in the main body of the paper, leaving the rest to the **APPENDIX.**

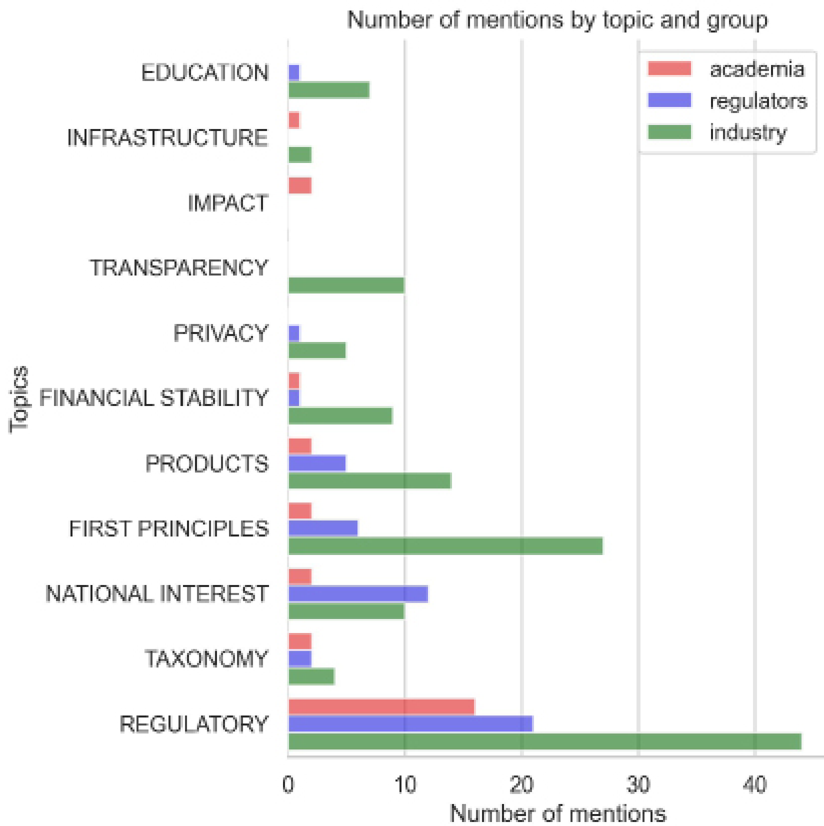
Figure 1 presents the total number of mentions by topic with the top three topics being regulatory, first principles, and national interest. Regulation considerations (when, how regulation applied and to what, with a light enough touch to encourage innovation and a strong enough hand to discourage bad actors) were at the crux of the discussion.

Fig. 1: Percentage of mentions for each group by topic



Discussion Perspectives: Breaking down group attitudes by their priorities

Fig. 2: Number of mentions (all groups) by topic and group



In Figure 2 we decompose the total topic-level mentions into counts by sector. As follows from this figure, the industry sector led in its thinking about regulatory considerations and first principles, in addition to products, transparency, national interest, and financial stability. The regulatory and academic sectors, on the other hand, showed less interest in transparency but shared as their top two priorities regulatory considerations and national interest. The third priority topic for regulators was national interest, for academia taxonomy placed third. While these indices are interesting, they must only be considered within the context of this particular conversation, and do not indicate an exclusive focus of a given sector. Note that privacy was a top priority for academics as a subset of first principles as a topic.

In the interest of exploration, we compute Pearson and Spearman correlation coefficients between idea-level mention count series for each sector. Pearson correlation measures the degree of co-movement (in terms of number of mentions), while Spearman correlation estimates the ranking agreement (how much rankings of ideas co-move between sectors). Both coefficients range from -100% to 100% with a larger magnitude indicating a stronger effect. We find that the Pearson correlation is 71%, 73% and 62% for academia-regulators, industry-regulators and academia-industry pairs respectively, while Spearman correlation coefficients are respectively 38%, 70% and 20%. Practically speaking, this indicates the highest level of agreement between the regulatory and industry sectors, while academics were closer to regulators, but had a somewhat different priority of ideas from the other two sectors.

CHAPTER 4

Fostering International Cooperation and United States Competitiveness (EO Section 8) PLUS Coordinating Regulators (EO Section 3)

Topics strongly identified included education, leadership,

THE EXECUTIVE ORDER STATES:

Sec. 8. Policy and Actions Related to Fostering International Cooperation and United States Competitiveness. (a) The policy of my Administration on fostering international cooperation and United States competitiveness with respect to digital assets and financial innovation is as follows:

(i) Technology-driven financial innovation is frequently cross-border and therefore requires international cooperation among public authorities. This cooperation is critical to maintaining high regulatory standards and a level playing field. Uneven regulation, supervision, and compliance across jurisdictions creates opportunities for arbitrage and raises risks to financial stability and the protection of consumers, investors, businesses, and markets. Inadequate AML/CFT regulation, supervision, and enforcement by other countries challenges the ability of the United States to investigate illicit digital asset transaction flows that frequently jump overseas, as is often the case in ransomware payments and other cybercrime-related money laundering. There must also be cooperation to reduce inefficiencies in international funds transfer and payment systems.

(ii) The United States Government has been active in international fora and through bilateral partnerships on many of these issues and has a robust agenda to continue this work in the coming years. While the United States held the position of President of the FATF, the United States led the group in developing and adopting the first international standards on digital assets. The United States must continue to work with international partners on standards for the development and appropriate interoperability of digital payment architectures and CBDCs to reduce payment inefficiencies and ensure that any new funds transfer and payment systems are consistent with United States values and legal requirements.

(iii) While the United States held the position of President of the 2020 G7, the United States established the G7 Digital Payments Experts Group to discuss CBDCs, stablecoins, and other digital payment issues. The G7 report outlining a set of policy principles for CBDCs is an important contribution to establishing guidelines for jurisdictions for the exploration and potential development of CBDCs. While a CBDC would be issued by a country's central bank, the supporting infrastructure could involve both public and private participants. The G7 report highlighted that any CBDC should be grounded in the G7's long-standing public commitments to transparency, the rule of law, and sound economic governance, as well as the promotion of competition and innovation.

(iv) The United States continues to support the G20 roadmap for addressing challenges and frictions with cross-border funds transfers and payments for which work is underway, including work on improvements to existing systems for cross-border funds transfers and payments, the international dimensions of CBDC designs, and the potential of well-regulated stablecoin arrangements. The international Financial Stability Board (FSB), together with standard-setting bodies, is leading work on issues related to stablecoins, cross-border funds transfers and payments, and other international dimensions of digital assets and payments, while FATF continues its leadership in setting AML/CFT standards for digital assets. Such international work should continue to address the full spectrum of issues and challenges raised by digital assets, including financial stability, consumer, investor, and business risks, and money laundering, terrorist financing, proliferation financing, sanctions evasion, and other illicit activities.

(v) My Administration will elevate the importance of these topics and expand engagement with our critical international partners, including through fora such as the G7, G20, FATF, and FSB. My Administration will support the ongoing international work and, where appropriate, push for additional work to drive development and implementation of holistic standards, cooperation and coordination, and information sharing. With respect to digital assets, my Administration will seek to ensure that our core democratic values are respected; consumers, investors, and businesses are protected; appropriate global financial system connectivity and platform and architecture interoperability are preserved; and the safety and soundness of the global financial system and international monetary system are maintained.

Sec. 3. Coordination. The Assistant to the President for National Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP) shall coordinate, through the interagency process described in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System), the executive branch actions necessary to implement this order. The interagency process shall include, as appropriate: the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Labor, the Secretary of Energy, the Secretary of Homeland Security, the Administrator of the Environmental Protection Agency, the Director of the Office of Management and Budget, the Director of National Intelligence, the Director of the Domestic Policy Council, the Chair of the Council of Economic Advisers, the Director of the Office of Science and Technology Policy, the Administrator of the Office of Information and Regulatory Affairs, the Director of the National Science Foundation, and the Administrator of the United States Agency for International Development. Representatives of other executive departments and agencies (agencies) and other senior officials may be invited to attend interagency meetings as appropriate, including, with due respect for their regulatory independence, representatives of the Board of Governors of the Federal Reserve System, the Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and other Federal regulatory agencies.

Directives and schedules for government reporting are included in the full Executive Order HERE.

CHAPTER 4 DISCUSSION

During this final segment, the assembled discussed the interactions between regulatory entities and practitioners, and the need for coordination among US agencies.

A former regulator opened the discussion with the observation that the world sits at "a thought-provoking moment"on international competitiveness and the development of a global system of regulation. "High-level" conversations are happening, he said, with the SEC inviting people to talk, but these discussions have yet to effect an approach. "Crypto venture capitalists can talk with policymakers in DC but these conversations **won't help for safe harbor**. He described evidence that some developers are keeping their work offshore in order to avoid US jurisdiction (naming Reddit and Discord). In all, he said, **"Those who are trying to get it right are getting information requests, (but) this makes people feel like they'll be better off if they avoid the regulators, which is too bad because regulators need insight from people's experience**."

An industry representative dismissed the level of discussion between regulators and industry thus far. "I don't think the regulators and policymakers are walking the walk. We need to push for substantive, lengthy discussion. **These meetings where industry gives a presentation aren't enough; industry needs to follow on the Executive Order.** Consult with industry, rather than (our) trying to force our way in, asking for substantive helpful conversations, and to shape the conversations. We need to have lengthy conversations; people like us need to be having these conversations, to give solutions to the regulators."

Another industry representative is optimistic about international cooperation and US competitiveness. "T**he obituary of my former project needed to be written in order to take this more seriously. This is not a process in vain: it expands the conversation.** The states will bring some sensibility. California, the fifth largest economy in the world, also has an Executive Order. **It's a fintech constitutional crisis**: US will win the Web3. Regulatory harmonization (France has licensed Binance; other countries are leaning heavily)**. Just because we're a little late, it's an advantage. Industry needs to look in the mirror; some aspects of our trade need improvement; industry needs sensible leadership."**

Former regulator admitted: "It's disappointing to hear about the challenges of going into our regulatory structure (that's a step back); CFTC and SEC were open to learning, but in this regard we've gone backward. On the international angle, I served at IOSCO (International Organization of Securities Commissions), and this has been recognized by overseas counterparties. I will say that it's not always the best approach; the world is looking to the US to lead, and once we have and have set some standards, we can do that**. We need to get our head out of the sand**. Early in the internet, the US leadership was a net-good. Banking would like to stifle this. If we balance traditional-finance with this, it'll be good for the US. **US should lead first, then sit down. Cooperation later. Further innovation, be open-minded."**

An industry member agreed with the former regulator. **"Get it right before harmonizing.** If enacted as written, the Solana blockchain goes down, and this would not encourage innovation. We need to think through US leadership, but we also need more detailed conversations. On the Hill, **we need to separate Defi from Cefi**, because custodians might do things differently. Better discussion of crypto asset classes and frameworks for use cases; and then bespoke, targeted changes for DeFi. The **wrong question is: How do we regulate crypto assets?** Our peers are proposing things that don't work for our models."

> **EDITORS' NOTE:** Internationally, it may require the US to lead before harmonizing. But domestically, coordination and communication among regulators and policymakers remain a key issue that the Executive Order aims to explore solutions for. A case in point is that when crypto tax policies and crypto market wash sales rules are not in sync, the efficacy of regulatory actions is severely reduced.
>
> **READ MORE:** Tax-Loss Harvesting Using Cryptocurrencies

Cryptography in defense

Another former regulator wanted to re-iterate that decentralized privacy is a "competitiveness and defense issue." This person said that crypto suffers from being treated as financialization when it's an infrastructure issue. "The ability to get aid to Venezuelan healthcare workers was because we were able to use cryptography."

International cooperation and bureaurаcy

An academic complained that "International cooperation was a straitjacket, a gesture of the willing-esque, lowering trade barriers and providing an alternative to China's digital sovereignty firewall. **I associate international cooperation with more bureaucracy**, (but) I think the TPP and digital trade agreement are going to increase the flow, that something in that vein might be productive."

An industry representative added, "Digital assets are trading around the world. In the US, we participate; FTX (crypto derivatives exchange) has better risk management."

> **EDITORS' NOTE:** FTX filed for bankrupcy on November 18, 2022. At the time of this publicaion, its risk management and other practices are under examination.

A legal expert: Yes, crypto is a comms tech and infrastructure tech, PLUS: it enables convening in so many ways and putting this in a box makes it hard to protect innovation.

DAOs and the Constitution

An industry representative added: Looking at DAOs (Decentralized Autonomous Organizations), in terms of the Constitution: What do you use IFT (interbank fund transfer) for? **This tech crosses borders so fast that how can you control what you need to**? Any ideas on how this gets done?

Another industry member chimed in: On the market infrastructure and 24/7 exchange issue: we've helped exchanges to push their infrastructure into the cloud for 24/7 trading. T**ech providers and market can serve as a bridge between traditional exchanges and crypto exchanges**. Until we do that, most institutions will respond the same. Look at the request to change the risk approach and see it competitively. Market participants can help mutualize the cost of moving to 365 trading by a certain date.

"How does CME participate? Policy makers need to extend, maybe relying on AI and ML on the weekend."

Former regulator:
"We live in a democracy. **Industry needs to speak to policymakers (through contributions and conversations).** We should support candidates who support innovation; Congress needs bipartisan (cooperation?) (party-proof and well-informed). **This room of experts is struggling to communicate.** We need to give information to Congress; we need to inform Congress in a non-crisis situation to come up with something comprehensive; not be ashamed.)"

CHAPTER 4 CONCLUSION

In closing the Chapter 4 discussion, the industry facilitator offered insight.

"I'm thinking about the delusion of transparency, how hard this is to understand. As we proceed, in the interest of dispelling the myth of transparency, we should remove the pertinent and **make it understandable for the layperson.** I'm also struck by the conversation on **regulation as a tailwind or activity-based regulation;** it can be built in so many ways."

Ultimately, she concluded: "How can we envision a system that can pivot as fast as it will need to, envision a flexible, elastic innovation, moving in real-time, tech can go 24/7; how can we create the right regulatory structure?"

CHAPTER 4 TAKEAWAYS

1. Process needed for industry to help regulators;
2. Legislators and agencies both need to have open minds and sync;
3. industry follow-through on the EO is required;
4. DeFi and CeFi need to be clarified legislatively.

"My big takeaway is: how does this industry help regulators?"

"People on the Hill have a more open mind, but the agencies need to start embracing it."

"These meetings where industry gives a presentation aren't enough; industry needs to follow on the Executive Order. "

"On the Hill, we need to separate Defi from CeFi, because custodians might do things differently."

"TradFi needs to learn from crypto in protecting us from risk."

CHAPTER 4: DATA VISUALIZATION

Figure 6. Top 5 Chapter 4 ideas by sector

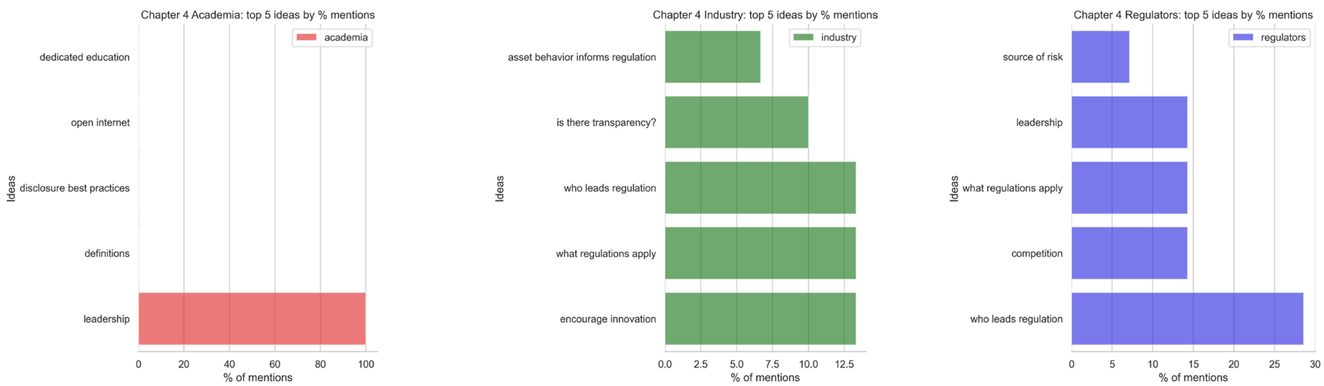


Figure 6. Summary

Industry and regulatory representatives contributed vigorously to the discussion of international cooperation and US competitiveness. The former group's top three ideas are innovation encouragement, what regulations should apply, and who should lead in regulation, while the latter focused more on who should lead in regulation, what regulations should apply, competition and leadership. Regulation-related ideas were important to both the industry and regulatory groups, while both the regulators and the academics paid attention to US leadership in the space.

EVENT CONCLUSION

The event organizer closed, expressing hope that the ensuing working groups would stay involved.

"The only wrong answer is to stop everything. This tech is broader than financial assets. Other applications for other industries might be helpful: maybe verified communications is an easier application than De-finance; maybe finance is too. This is a technology that can be used for other things. Think outside the politically-antagonizing finance box."

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Computing Research Association (CRA)'s Computing Community Consortium (CCC)

Computing Community Consortium's Response to RFI "Digital Assets Research and Development"

March 3rd, 2023

Written by: Hank Korth (Lehigh University), Rajmohan Rajaraman (Northeastern University), Catherine Gill (Computing Community Consortium), and Ann Schwartz (Computing Community Consortium).

This response is from the Computing Research Association (CRA)'s Computing Community Consortium (CCC). CRA is an association of nearly 250 North American computing research organizations, both academic and industrial, and partners from the professional societies. The mission of the CCC is to enable the pursuit of innovative, high-impact computing research that aligns with pressing national and global challenges.

This response primarily pertains to questions 1, 4, 5, and 6 from the Request for Information.

Introduction: A Framework for Digital Assets

In order to consider the technological needs, challenges, and opportunities in the domain of digital assets, it is important to assess the range of current and potential applications. Assets take many forms: money, equities, bonds, real estate (and other physical property), intellectual property (patents, books, etc.), carbon-offsets, etc. Some of these assets are largely in a digital domain. Most monetary transactions, and virtually all large, legal ones, are digitally created and stored, and operate over digitally represented assets. The link between physical assets and their digital representation is created, managed, and maintained by some (usually centralized) authority, such as a registrar of deeds for real estate.

Beyond a traditional view of assets is the concept of information as an asset. Whether that information is health data, financial data, or data shared on social media, those data are indeed assets with real value. As is the case with other assets, information is managed in most cases by a central authority, with the individual about whom the information pertains possibly losing control of its use.

The connection between digital assets and blockchain technology[1] rests in the use of cryptographically secure methods to replace some or all of the centralization with a trust based

[1] We use the term *blockchain* here rather than *digital ledger*, though both terms are applicable in most of our contexts. The term *digital ledger* is used, often in an enterprise setting, for a blockchain with no cryptocurrency and some degree of centralized access control.

upon code, typically, though not necessarily, open-sourced and publicly verifiable. The design of a blockchain framework can enable a degree of decentralized control versus a central authority. There is a full spectrum of control – from highly centralized to purely decentralized. Where a specific deployment of a framework rests in this spectrum varies among current blockchains. Some existing blockchains mandate a particular mix of decentralization and centralization. Others allow a degree of flexibility that is subject to parameters set by policy makers. Who those policy makers are and how they make their choices is beyond the scope of this paper, which focuses on technology and the need for investment in research. Taken as a whole, blockchain technology can serve as an efficient enabler of policy choice and can empower both governments and enterprises to operate in accordance with their core values. To ensure that digital assets and blockchain technology enable fair and equitable systems, these technologies must be employed in a trustworthy fashion. We recommend a framework emphasizing three properties: *privacy*, *transparency*, and *regulatability*.

Supporting a Mix of Privacy, Transparency, and Regulatability

While privacy and transparency may sound like antithetical goals to implement in a single system, the unique properties of the blockchain allow for each to be achieved without compromising the other. Blockchains can offer privacy and transparency simultaneously using zero-knowledge (ZK) proofs, a breakthrough technology in cryptography that allows a party to prove a guarantee to another party convincingly (hence offering transparency) without revealing any private information (hence maintaining privacy). ZK proofs were introduced in 1985[2] and formed a body of contributions to cryptography leading to the 2012 Turing Award being presented to Shafi Goldwasser and Silvio Micali. The underlying mathematics is highly complex but the concept has been illustrated in a highly intuitive way using interactive examples in a human domain rather than code[3].

In our context of digital assets, ZK proofs allow proof of compliance while preserving privacy. Consider the example of a sanction list from the US government. A financial institution could use ZK to prove that no transactions in a set of transactions interacts with any party on that list without having to reveal anything more about the transactions themselves. Later, if due process allows for audits, that institution could reveal a transaction and show that it was a part of the set for which the ZK proof applies without having to reveal the entire set of transactions[4].

While many ZK systems exist, they fall short of the scale needed to support both mass adoption and application to large-scale datasets, both of which are important to maximize societal

---

[2] Goldwasser, S., et al. "The Knowledge Complexity of Interactive Proof-systems." *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85*, USA, ACM Press, 1985. *Crossref*, https://doi.org/10.1145/22145.22178.

[3] "Computer Scientist Explains One Concept in 5 Levels of Difficulty | WIRED." *YouTube*, 18 Jan. 2022, www.youtube.com/watch?v=fOGdb1CTu5c.

[4] The full technical details include cryptographic data structures such as Merkle trees.

benefits. The challenge here is that ZK proofs, though relatively easy to verify, are computationally hard to generate, and that difficulty grows with the complexity of the computation about which a proof is being generated. Many of the mathematical computations needed to generate ZK proofs are highly parallelizable but also require large amounts of memory. Considerable research is needed in cryptography and cryptographic algorithms, and also in the design of highly scalable parallel hardware and software systems in order to enable broad deployment of ZK technology.

Trustworthy Markets and Financial Leadership

The US' post World War II leadership role in financial markets has benefited the nation in many ways. The continuance of the leadership depends on the US maintaining its trustworthy markets in the face of advancing technologies that may enable new leaders to emerge. China is clearly pursuing a leadership role with its e-Yuan and various Western nations, including those in the European Union, are developing digital-asset prototypes and policies. Continued US leadership will require a prudent mix of policy and regulation that both protects investors and supports continued experimentation and technical innovation. Prudent regulation requires a deep understanding of how policy goals can be achieved with minimal impact on positive, useful aspects of markets and industries. The ability of blockchain systems to create trust among untrusting parties and the power of zero-knowledge to prove compliance while maintaining privacy can combine to create a regulatory framework that is both transparent and privacy-preserving. The impact of such a framework is a continued faith in the fairness of markets while enjoying the benefits of technological advances. A technologically-aware approach to regulation that supports both trustworthy markets and further innovation is of particular importance for blockchain and cryptocurrencies, since those technologies and the markets they enable have a high degree of global mobility.

Information: The Foundational Digital Asset

Much of the discussion on digital assets thus far has focused on the applications of digital assets and the blockchain in financial markets and cryptocurrency. The term “digital assets” itself may imply a financial leaning in its application area, but we believe that this focus is unnecessarily limiting, and biases the discussions surrounding the potential impacts of these technologies. Blockchain technology is not simply about currency. Blockchain technology is about information and the privacy and transparency thereof. Information that supports a digital currency is only one such application. Efforts are underway to employ blockchain technology to a variety of information management applications both in government and in enterprises. Most of the latter applications do not even have an associated cryptocurrency. We are aware of ongoing projects and products in secure health records, verifiable accounting, supply chain, real-estate registration and transfer, academic transcripts, and more. Certainly, central-bank digital currencies are an extremely important application, but that and other currency-based applications can all be viewed from the standpoint of a blockchain being an information-management system handling data about the currency and transactions in that currency.

It is important to distinguish between the concept of information management as in a typical enterprise database and information management within a blockchain setting. A database system facilitates storage, retrieval, update, and sharing of information. Applications run on top of the database possibly using stored procedures within the database that applications can call. Blockchains enable code to run with partial or total autonomy. Such code is called a *smart contract*[5]. This enables a business contract to be coded as a smart contract that implements the terms of the agreement. A simple example is a weather insurance contract that pays a farmer if the contract-specified period of no rain occurs. The real-world information about rainfall would be provided by a trusted real-world provider (say the National Weather Service) or a crowd-sourced "oracle" implemented by another smart contract. The tamper resistant properties of blockchains protect against a party to a contract reneging; rather the smart contract directly enforces the contract.

Smart contracts are a powerful concept. They enable publicly verifiable implementation of agreements, automated "organizations" providing services, and the ability to replace high-fee centralized services with code. That power comes with challenges. Bugs in a smart contract are forever due to the immutability of blockchain data. Careful code verification can reduce this threat. However, unless the deployer of a smart contract includes calls to control the contract's operation after deployment, the contract is autonomous, leading to the term *decentralized autonomous organization* (DAO). Even if autonomous, smart contracts can provide proof of compliance with regulations if so coded, making them valuable resources for efficient management of complex agreements.

Much discussion surrounding digital assets and cryptocurrency recently has been tainted by scandals such as the FTX collapse, the direct loss of billions of dollars of investor's money, and follow-on collapse of other centralized firms that relied on FTX. While these examples display a clear misuse of cryptocurrency, they do not point to faults in the digital-asset technologies, but rather the risks of these technologies being used by bad actors in nefarious schemes. The technologies we suggest here for our three-part goal of privacy, transparency, and regulatabilty have the ability to mitigate and, ultimately, eliminate the financial and accounting fraud behind the FTX scandal.

The true value of digital assets and blockchain technology lies in their ability to establish trust between the untrusting. An example of this is in the healthcare industry. According to a 2016 report by Johns Hopkins University[6], the 3rd leading cause of death in the United States is due to medical errors, "resulting from poorly coordinated care, such as planned actions not

[5] Or, in the terminology of Hyperledger, *chaincode.*
[6] Makary, Martin A., and Michael Daniel. "Medical Error—the Third Leading Cause of Death in the US." *BMJ*, BMJ, May 2016, p. i2139. *Crossref*, https://doi.org/10.1136/bmj.i2139.

completed as intended or errors of omission in patient records"[7]. Various reports since that study provide evidence that the problems are not diminishing despite a move to electronic health records. Although records may be electronic, access to those records is limited even in cases where there is a clear medical necessity to access them. The root cause of this problem is that health records are stored in separate repositories that have their own data access controls and authentication framework. A single central national health data repository would raise numerous privacy concerns. A solution to this problem would be creating a blockchain-based medical-records system, which could store patient information while also only being accessible if the patient gives consent (directly or via an authorized representative or a personally carried access code). This would allow all patient information to be accessible through one system, enabling medical practitioners to provide better informed care and limit errors in a patient's medical history due to omission of records. Ultimate ownership of medical data would be with the individual, with each entry digitally signed by the health provider involved.

This example of health information is one of many that detail the need for blockchain technology use and competency in the United States, and also prove the risk of not furthering R&D in this area. By simply listening to popular debate of blockchain technologies and the misuse of cryptocurrency in nefarious financial schemes, it is easy to view these technologies negatively, and even become jaded against allocating them further funding towards research and development. However, it is also important to realize the risks of limiting this research in the United States, and allowing foreign nations to become dominant in this field. Said differently, it is important to recognize that technologies of all types have both uses and misuses. Policy goals should seek to maximize positive use and minimize misuse. Simply running from a valuable technology because misuses exist is not likely to be the best policy choice; rather it leads to the benefits from positive use accruing to other nations.

The earlier discussion of smart contracts is another illustration of the need and value of further R&D in blockchain technology. Autonomous smart contracts (DAOs) are, by design, immune from external control post-deployment. That provides a high degree of valuable functionality, but presents challenges for regulatabilty. Integrating the power of smart contracts in an open, global blockchain setting with a trustworthy market framework remains a challenging problem. Placing legal and regulatory constraints on DAOs risks limiting their benefits and creating added risks for individual participants, yet lack of regulation presents participants with other potentially serious risks. Creating a framework for effective incorporation of this technology in a modern market remains an area of research that crosses the barriers between computing, finance, and the law. The nation that leads in research in that space will be the one best positioned to mix policy and technology in a way that allows that nation to win the global competition to create the most attractive markets. Here, too, running from a technology because of possible misuses is not the best policy choice.

[7] "5 Blockchain Healthcare Use Cases." *STL Partners*, stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases.

Innovation and Leadership: Technology, Commerce, Social Values

Those countries that innovate tend to benefit the most from their innovations. From the days of the innovative use of assembly-line technology in manufacturing through to the invention of the technologies underlying the internet, US technical leadership in innovation led to US industrial leadership. So, tying back to the topic of digital assets, we are left with one question: are we willing, as a nation, to take a backseat and let foreign nations innovate in the field of digital assets, leading us to scramble to catch up, or should we lead the way and reap the benefits?

Leadership in the blockchain space has value beyond the specific examples cited here. As the Internet developed into a decentralized utility providing a communication-link for commerce and society, blockchain technology promises to be a decentralized trust-utility for commerce and for society. Recent supply-chain challenges show both the importance and potential frailty of the way businesses depend upon each other. Blockchain technology offers a means for timely, reliable sharing of supply-chain data enabling smoother supply chains. Blockchain's key contribution in this space is that members of a supply chain can collectively validate information that is digitally signed by firms, creating a trusted source of information spanning all firms participating in the supply chain and integrating with those firms enterprise databases and ERP systems. While this automation and auditability cannot prevent physical disruption to a supply chain, it can not only smooth normal operation, but also enable accurately informed rapid response to disruption. In an economy driven by long, complex supply chains, leading-edge technology in supply-chain infrastructure and its effective use becomes a competitive advantage. Several leading US technology firms are already active in this space and foundational research can provide the basis for continued US leadership in supply-chain systems.

Because blockchain-based information systems encode and automate policy decisions, leadership in blockchain is not only the economic issue that we noted above, but also one of advancing national values, including the rights and freedoms of individuals, and the access of the most disadvantaged to information-based services, most importantly the financial system. Blockchain technology can bring access to the financial system to the unbanked (this is already happening in the developing world and played out dramatically at the time of Russia's invasion of Ukraine). Blockchain technology can provide cryptographic proof of payment of a fair wage to workers along with a conveyance of that proof along the supply chain to the consumer, thus ensuring fair treatment of workers and reducing the chance of corruption. All these possibilities exist or are being prototyped. Systems of this sort can go beyond just wages to include certification of working conditions, not only in farms but also along the supply chain delivering products to end users. At each step, digital signatures combined with digital identities enable documented public assertion regarding the path products take from raw materials to store shelves.

The value of blockchain technology for social good and financial inclusion is perhaps an even stronger justification for the US to seek R&D leadership in this space. While blockchain technology *can* be used for good, it can be used in other ways. The structure of the e-Yuan has a more centralized and less private design that could enable a stronger surveillance state and stronger access restrictions. Several prototype central-bank digital-currency systems instead enable maintenance of the decentralized ("two-tier") framework of today's western financial systems, with parameters that grant policy-makers a strong degree of policy choice. Technologies of this sort need continued R&D so that these positive properties can scale to the level of global finance and commerce.

Training the Next-Generation Workforce

The position of the US as the world's industrial and financial leader rests to a large degree on its leadership in data management and computing. The global nature of information and of digital assets implies that leadership entails not only technological leadership but also a world-class workforce trained to use (and extend) this technology. Historically, US leadership in computing technology in all its varied aspects has rested heavily on the contributions of academic research in the US, research that in large part has been funded by Federal agencies (NSF, DARPA, and others). Another significant source of support has been US-based firms in the computing field. That R&D funding enables not only research but also an educational framework to train the next generation of researchers and workers.

Earlier, we noted the foundational role of federal R&D support for the Internet. In 2011,[8] the CRA participated in an event showing how federal R&D support enabled the game-changing innovation in the iPad. In 2019, the CCC released "*A 20 Year Community Roadmap for Artificial Intelligence Research in the US*," which presented recommendations for increased funding of AI research and cited successful examples, such as the NSF and ARPA funding of the Linguistic Data Consortium (LDC), which created a repository for natural language datasets to train AI technologies in speech recognition[9]. The recent federal support for research in Artificial Intelligence (AI) and its impact on society, through grants, National AI Research Institutes, and initiatives such as the National AI Research Resource, is enabling US leadership in AI. Today, the nation has a similar opportunity to stimulate not only research but also the skilled human infrastructure needed for effective development of research into digital-asset products and the deployment of those products in the market.

The computing technology underpinning blockchain includes many areas already strongly supported by Federal initiatives, including distributed computing, parallel computing, cryptography, among others. Blockchain systems combine these technologies in unique ways that create new programming paradigms and new user-computer interaction paradigms. Translating technology to impactful practice requires educational excellence at all levels: user experience, application design (especially novel and disruptive applications), along with the

---

[8] Melissa Norr. “Deconstructing the iPad.” *GovAffairs*, 20 Sept. 2011, cra.org/govaffairs/blog/2011/09/deconstructing-the-ipad.

[9] Y. Gil et al. “A 20 Year Community Roadmap for Artificial Intelligence Research in the US.” *Computing Community Consortium*, August 2019, https://cra.org/ccc/wp-content/uploads/sites/2/2019/08/Community-Roadmap-for-AI-Research.pdf

system internal structure itself (cryptographic mathematics and algorithms, verification of blockchain smart contracts, high-performance systems, etc.). At present only a modest fraction of universities offer a strong set of courses in blockchain systems, technology, and applications. In the 2022 CoinDesk ranking of the top 50 universities in blockchain only 1/3 are US-based. US-based schools typically occupy at least half of top-50 rankings of universities in general. Anecdotal evidence suggests that blockchain education remains largely absent below the top "elite" universities in the US. College and university student clubs focus more on trading than on the technology and its impact.

Most discussion of technology and workforce development focuses on the "STEM" disciplines, and the CRA's focus certainly reflects that. However, blockchain education is not just a STEM issue. As noted above, blockchain-based information management enables richer enterprise collaboration, better targeted monetary and fiscal policy, and documentable values-based social policies. While leadership in business and policy may not need training in the mathematics of esoteric technologies like zero-knowledge proofs, leaders do need a strong factually grounded understanding of the capabilities of the technology not just to do old things better but rather to do things that could not be done effectively before. Though there are a few examples of knowledgeable leaders on these topics in business and government, such leaders are still sorely lacking in these fields. A spinoff effect of investment in R&D in an academic setting is an increased amount of training for the next-generation workforce.

Arguably, federal R&D support for research in technologies underlying digital assets should be partnered with support for development of courses and experiential learning addressing both the technologies themselves and their applications. Much of the mathematics underlying blockchain is from branches of mathematics that tend to be less-covered in computing curricula (groups and fields, cryptography). The computing subdomains of parallel consensus and software verification need greater emphasis. Relatively few business curricula cover blockchain and its applications in supply chain, finance, etc. Beyond the technical and business disciplines, the applications of blockchains for social good could inspire new generations of policy leaders.

Conclusion

At present, the US is behind the world as a whole in blockchain technology research, education, and policy. There is a strong industrial and entrepreneurial presence that needs to be nurtured and developed. Past experience with R&D investment and supportive policy at the government level in computing technology has, and is paying dividends. This has been demonstrated with the internet, digital commerce, chips, personal devices such as the iPhone, and most recently, AI. The area of digital assets is the next open frontier for innovation in computing and information technology.

The largest open question is who will be the leader in this next frontier for innovation in computing and information technology? Will it be the US, as it has largely been in the post World War II era? The answer depends on how the US reacts both in its policy decisions and in its investment decisions. This report focuses on the second of those two: investment. The US tradition of strong federal R&D investment at an early stage has paid huge dividends both in the economy and in world leadership. At key points in the past, federal investment in education and workforce development has allowed the nation to be the first-mover in taking advantage of the research developed in the US.

There are concrete steps that the federal government can take to help ensure that the era of digital assets is led by the US:

- Direct support for research and development in the blockchain technologies that support digital-asset management, particularly investment in academic research.
- Encouragement of the development of digital-asset systems that enable a mix of privacy, transparency, and regulatabilty by creating a framework that enables policy choice and appropriate levels of decentralization.
- Augmentation of R&D support with support for educational initiatives and expansion of educational offerings in blockchain and digital-asset technologies both in the STEM disciplines and in the disciplines impacted by digital-asset technology.
- Promotion of positive-use-case examples in the digital-asset space to inspire projects to enhance national economic competitiveness and social good.

A recurring theme in a discussion of digital assets is decentralization. Examples above have shown how such decentralization and disintermediation can positively impact many aspects of society. Open, accessible systems that use blockchain technology to combine that openness with the critically important properties of privacy and regulatability offer the potential of creating fairer, freer, and more just systems from finance to healthcare. But that potential can be achieved only if the leadership in the technology comes from nations with such traditions and values.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Consumer Technology Association (CTA)

Consumer Technology Association™

[redacted]

March 3, 2023

The Honorable Dr. Arati Prabhakar
Director
Office of Science and Technology Policy
Executive Office of the President
Washington, DC 20500

RE: Request for Information; Digital Assets Research and Development (88 FR 5043)

Dear Director Prabhakar:

The Consumer Technology Association appreciates the opportunity to respond to the Office of Science and Technology Policy's (OSTP) request for information on "*Digital Assets Research and Development*." CTA members view the Administration's March 8, 2022 Executive Order on "*Ensuring Responsible Development of Digital Assets*" as an important government acknowledgment of a new technology, much the way the Clinton administration's 1997 Framework for Global Electronic Commerce set the stage for the growth of the commercial Internet. CTA is happy to provide our perspectives on the importance of regulatory certainty and a robust trade policy for digital assets.

CTA represents the $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. A strong majority of our members are small and medium-sized enterprises (SMEs). They and our larger members are innovators, manufacturers, service providers and employers of Americans. CTA also owns and produces CES®—the most influential technology event in the world – which showcases and serves as a forum for discussion of blockchain and digital asset technologies.

The consumer technology industry stands at the intersection of blockchain and digital asset technologies. Consumer tech companies manufacture the hardware and devices that facilitate the use of blockchain and exchange of digital assets and innovate the software underpinning the digital assets themselves, digital asset transactions, and the cross-border flows of data and information that enable them. Our views and principles in this area are informed by our considerable experiences in the development and commercialization of Web 2.0 technologies, which we believe are critical to any U.S. government initiatives concerning Web 3.0.

This history tells us that a neutral and reliable framework for regulation of blockchain and digital asset technologies – at a higher level than the infrastructure underpinning them – is the key to U.S. digital finance innovation and the participation of individuals in the digital economy. Such a framework is also essential to leveraging blockchain and digital asset technologies to accomplish urgent domestic and international policy objectives, which we outline below. More, the Biden-Harris Administration's focus on blockchain and digital assets is a significant opportunity for the United States to increase U.S. competitiveness for these technologies and to explore new ways to deploy technology to address risks, while protecting the security and privacy of individuals.

CTA welcomes OSTP's interest in the significant potential for responsible blockchain and digital assets innovation to grow the economy. Our members with experience in these technologies are largely consumer-facing businesses, small and medium-sized enterprises, and startups. Our comments below reflect their perspectives and experiences. As OSTP considers an overarching research and development agenda for blockchain and digital assets, we urge it to consider the enabling factors for a successful and competitive industry in the United States (e.g., regulatory transparency; strong internal coordination of regulatory work across the government; greater regulatory certainty; voluntary, market-driven standard-setting in areas such as cybersecurity and privacy; robust and sustained public-private cooperation).

More, we urge OSTP to develop an R&D (research & development) agenda for blockchain and digital assets that prioritizes scalability. For example, the existing financial system operates at economies of scale which leaves many merchants, SMEs, and consumers paying higher transaction costs for trade and things like FX transfers. Digital assets have the potential to lower transaction costs, both at scale and at the individual and business levels, thus increasing efficiency, reducing barriers to customer growth, and allowing access to more markets overseas. Regulation for payments and development of a uniform federal government technical framework (e.g., terminology, regulatory leads, and determination of whether standard-setting lies with the federal government vs. private sector,) are fundamental and key factors in U.S. competitiveness in digital economy.

Regulatory Certainty with Flexibility Can Spark U.S. Innovation in Digital Assets

Above all, U.S. regulation of digital assets should enhance U.S. technology leadership by prioritizing innovation and legal clarity while protecting users and consumers. U.S. companies innovating and using digital asset technologies benefit from the certainty that U.S. law provides. For example, under the Banking Secrecy Act, any company providing covered digital financial services must comply with the same core anti-money laundering (AML) requirements that a U.S. bank would under this Act. Additionally, U.S. blockchain and digital assets firms benefit from other high U.S. regulatory standards covering the financial services industry, including with respect to corporate conduct, prudential risks, and operational management.

Continuity and clarity in regulation will provide space for start-ups and SMEs to innovate new digital asset technologies, scale them up, and commercialize them quickly for the benefit of U.S. and global consumers, particularly those who to date have been unable to participate in the global financial system at all or only in limited ways. It will also leverage U.S. comparative advantages in intellectual property and technology development and provision of globally competitive digital services through cross-border data flows.

A welcoming and enabling regulatory environment that creates more certainty and enforces existing U.S. law is our strong preference. Instead, what we are seeing is U.S. regulators using enforcement actions to regulate in novel ways. They may not have the authority to take these actions, as it is not clear that

Congress has granted it. This dynamic creates even more uncertainty for firms innovating and deploying digital asset technologies.

The ultimate result if this trend continues is that they choose to innovate in other global markets – not the United States. And this trend may have the opposite impact of the what the three regulators intend, namely the heightening of threats to U.S. economic competitiveness, national security, and technological development. OSTP instead should prioritize an R&D and regulatory agenda designed to retain digital assets firms in the United States and dissuade them from moving to international jurisdictions.

For technologies at the early stages of development and commercialization, regulatory certainty provides what innovators need to facilitate the investment and capital that drive innovation. For digital asset technologies, the U.S. regulatory system should be certain but not overly prescriptive. Flexibility is key. U.S. regulations concerning digital asset technologies should not make new market entrants subject to enforcement actions for failing to comply with unclear regulations.

The certainty provided by pro-innovation government guidelines has previously proven helpful in promoting new financial technologies. For example, the Consumer Credit Protection Act of 1968 provided a legal and regulatory framework that encouraged the widespread use of credit cards**.** Any regulation should be clear, transparent, and focused on protecting consumers from actual and demonstrable – not theoretical – harms.

Regulatory Certainty with Stronger Enforcement in the United States Will Enhance U.S. National Security and our Comparative Advantage

The U.S. regulatory and national security interests together have a significant impact on the international environment and markets for U.S. blockchain and digital asset technologies. Any U.S. regulation of blockchain and digital asset technologies should recognize that developing digital assets in the United States - and regulating them appropriately - is connected to U.S. national security interests. The movement of assets around the world relates to U.S. primacy over financial flows. For example, remittances of assets from the U.S. to other countries are critical to their financial health and development. Digital asset technologies may make remittances even more potent development tools.

For these reasons, enforcement of current U.S. laws, particularly against those known to be engaging in hacks or scams, is paramount. The greatest illicit finance risk regarding digital assets is lack of enforcement. If U.S. regulators choose to enforce our laws only lightly, offshore entities will then increase their scale and arbitrage capacity through foreign digital asset exchanges – to the detriment of U.S. competitiveness, innovation, and consumers. Stronger enforcement of existing U.S. laws will level the playing field both domestic and foreign companies and enhance U.S. competitiveness.

To strengthen their enforcement efforts, U.S. regulators should:

1. Incentivize companies to improve existing technology or innovate new compliance tools, such as combining traditional compliance tools with blockchain analytics to increase the transparency of parties and transactions;

2. Prioritize broad dissemination of these compliance tools across the private sector and promote ways to develop them further; and
3. Enhance information sharing between industry and government to alleviate the paperwork burden of both. Due to the transparent nature of blockchain, much of the information that would allow governments to identify and trace illicit transactions is already available via public blockchain. Qualified analysts (e.g., at Chainalysis) work with industry and government to interpret and make accessible information already available on-chain.

These innovations at home can have a significant impact on U.S. interests abroad. Any regulatory proposal should not impact product design as innovators and suppliers need to provide a single product that can meet the demands of digital payments in multiple markets. Businesses design products for multiple markets and customers. The ability of U.S. innovators to participate and hold leading positions in the global marketplace is key to facilitating the cycle of private-sector research and development investments. CTA recommends that policy considerations should not impact how U.S. firms provide multiple payment solutions for global customers and conduct R&D activities.

Blockchain and Digital Asset Technologies Can Address Urgent Domestic and International Policy Objectives

CTA members are quickly innovating new use cases for blockchain and digital asset technologies. These use cases can improve identify verification, cross-border payments, environmental conservation, and transmission of healthcare data. We offer examples below:

- One set of technologies that will yield security and innovation dividends in the future is "digital identity", blockchain, and "zero knowledge proof", which will better optimize privacy and security features of our current (and outdated modes of authenticating and communicating identify. Consumers with an independently verified digital identity are more likely to use and store digital assets to hold value on the Internet. Digital identity technologies can increase the efficiency and effectiveness of existing AML regulations and companies' compliance efforts, for example through streamlined "know your customer" procedures. CTA encourages OSTP to work with U.S. regulators on understanding the benefits of "digital identity" to responsible development of digital assets.

- Another financial innovation that will further integrate our financial system are payment stablecoins. OSTP could examine how to creating the conditions for stablecoins to mirror the accessibility of physical cash (e.g. ability to transact without internet connectivity or a bank account; use of near-field-communications; and interoperability across technologies and blockchains).

- OSTP could support the robust work on cybersecurity standards under the National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework[1] and the development of standards under it will help the U.S. government and the private sector safeguard funds across digital assets and adopt stronger data protection standards.

[1] https://www.nist.gov/cyberframework

U.S. Trade Policy is Critical to the Future of Blockchain and Digital Asset Technologies

The United States should write the trade rules concerning blockchain and digital asset technologies. Through the digital trade chapters of the U.S.-Mexico-Canada Agreement and the U.S.-Japan Agreement Concerning Digital Trade, the United States has become a leader in writing the rules of digital trade for the Web 2.0 era. As Web 3.0 technologies evolve and become more widespread, their decentralization will ensconce them in the international environment. International trade agreements will affect the pace and scale of deployment of digital asset technologies worldwide.

For this reason, it is in the national interest of the United States to continue its digital leadership and write rules that reflect long-standing international trade principles, such as national treatment and most-favored nation. More, core rules regarding digital trade, for example prohibitions on restrictions on cross-border data flows and the location of computing facilities, should be essential elements for any new provisions on digital asset technologies in trade agreements. Regulatory cooperation provisions would also be important as governments determine when and how to regulate blockchain and digital asset technologies, to avoid regulatory misalignments and market segmentation.

Conclusion

As the Biden-Harris Administration implements the Executive Order, we encourage OSTP to work with U.S. regulators and other relevant federal agencies on creating a more certain and pro-innovation regulatory environment for blockchain and digital asset technologies while enforcing existing U.S. laws to create greater regulatory certainty. We urge OSTP to collaborate closely with Treasury, the Office of the U.S. Trade Representative, the Department of Commerce, and relevant U.S. regulators on writing new rules in free trade agreements that promote broader adoption of blockchain and digital asset technologies and secure and advance U.S. technology leadership across the globe. We look forward to serving as a resource for you and your staff as you consider input and recommendations from stakeholders.

Sincerely,

[redacted]

Michael Petricone
Senior Vice President of Government Affairs
Consumer Technology Association

[redacted]

Ed Brzytwa
Vice President of International Trade
Consumer Technology Association

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Georgetown University

CyberSMART Research Center

March 3rd, 2023

Submitted to the Science and Technology Policy Office

Georgetown University, CyberSMART Research Center

Respondent type: Academic Institution

Response to "Request for Information; Digital Assets Research and Development"

We appreciate the opportunity to comment on "Request for Information; Digital Assets Research and Development" as published by the Science and Technology Policy Office on January 26th, 2023. We welcome the opportunity to be part of the ongoing dialogue.

Introduction

Cyber SMART is a National Science Foundation (NSF) Industry-University Collaborative Research Center (IUCRC). Initially established at Georgetown University in 2019 in response to industry demand for a new approach to cyber research and training; the Center's name, standing for Science, Management, Applications, Regulation, and Training, reflects a new holistic approach. Cyber SMART has since expanded to include the University of Notre Dame, and in 2021 was accredited as an IUCRC by the NSF. Cyber SMART is the first IUCRC to strategically combine computer science (CS), with all related NSF social and economic sciences (SES) and behavioral and cognitive sciences (BCS) to the full spectrum of cyber research.

Cyber SMART's unique capabilities in law, economics, finance, management, forensics, neuroscience, psychology, behavioral science, and ethics, and its world-leading expertise in computer science, combine to provide much more effective cyber solutions that address real-world needs. This multidisciplinary approach produces research that is focused and directly relevant to the public and private sector organizations that are the Center's Members and their constituents and customers.

The main research area of the center is CBDC, blockchain, and its application, which include, smart contract security, layer 2 and bridge security, digital identity and privacy, decentralized oracle and game theory, decentralized governance, CBDC, and stablecoins.

RESPONSES

1. Goals, sectors, or applications that could be improved with digital assets and related technologies.

Three Key Features of Digital Assets

Digital assets have three key features that differentiate them from traditional financial assets, even those held in electronic form.

First, they are digital bearer assets or account-based assets. This means that anyone with a private signing key can transfer ownership around the clock and around the world at almost no cost. Such a decrease in transaction costs has clear benefits for almost any type of transaction. Digital assets can also facilitate efficiency in the internet of things. For example, a solar panel on one roof can auction electricity in real-time, either to a factory or an electric vehicle, and the owner can get paid in real-time.

Relative to existing real-time settlement solutions, including those offered by the Federal Reserve (e.g. FedNow), a central bank digital currency (CBDC) and other private forms of digital assets could be considered advantageous due to easier accessibility through existing retail payment networks. Real-time gross settlement systems are interbank systems, while CBDC and privately issued digital coins could offer peer-to-peer payments.

Second, these assets could be programmable. That means that they could incorporate many types of functionality in addition to payment and settlement. This includes payments whose amount and timing are controlled by the digital asset itself. For example, a venture capital funding arrangement could automatically release the next round of financing when certain milestones are met. A security could automatically check to determine whether a lockup period has expired permitting its sale, or whether a prospective purchaser is an accredited investor. It could even automatically withhold the right amount of taxes from a dividend and pay them to the appropriate government agency.

Third, digital transactions could be stored in a distributed ledger that might provide a secure record without a single point of failure. This provides the opportunity for very high levels of accountability and transparency.

Potentials of Central Bank Digital Currency (CBDC)

An important consideration in developing a central bank digital currency (CBDC) is establishing its clear purpose as a financial tool. The main reasons supporting the implementation of digital currency which is the liability of the central bank are (1) financial inclusion, (2) the creation of a digital substitute for the declining use of cash[1], (3) the creation of a public alternative to privately issued digital assets, (4) reduction in cross-border payment frictions (speed and cost), (5) introduction of CBDCs as monetary policy tools to address the new financial environment[2]. In addition to (1) to (5), from a U.S. standpoint, a U.S. CBDC could help preserve the international trust and role of the U.S. dollar. If the U.S. dollar does not keep up with modern payment technology, then it will lose relevance as competing currencies, digital currencies or foreign CBDCs will provide better, faster, cheaper payment and store-of-value solutions. Furthermore, there are also positive implications such as higher economic growth, higher employment, and increased income equity; all associated with enhancing financial inclusion. CBDCs have the potential to make digital banking more accessible to a greater share of the population, which could help reduce the significant number of unbanked and underbanked households in the U.S[3]. Assuming greater financial

---

[1] CBDCs are likely to speed up the transition to a paperless and cashless economy. The use of CBDC in ordinary transactions would contribute to further digitalization of the economy, associated with lower costs and increased efficiency of the banking system.

[2] The development of poorly regulated digital currencies and crypto assets has caused many central bank officials to be concerned that such a development could ultimately lead to the loss of control of the money supply. The increasing popularity of digital assets might mitigate the central bank's ability to conduct monetary policy.

[3] According to "National Survey of Unbanked and Underbanked Households" conducted by the Federal Deposit Insurance Corporation (FDIC), 4.5% of U.S. households (approximately 5.9 million) were "unbanked", 14.1% (approximately 18.7 million) were "underbanked". The "underbanked" is defined as the household that was banked

inclusion, financial intermediaries, including private banks, could more effectively extend credit to an increased number of individuals and organizations. In fact, there is some evidence that high level of financial intermediation has a positive correlation with economic growth, employment and reducing income inequality[4].

2. Goals, sectors, or applications where digital assets introduce risks or harms.

Taking Risks into Account

Just like any new and powerful technology, there are risks as well as benefits. The bearer nature of digital assets presents clear issues with money laundering as well as the safety of the custody of assets. However, just because these risks exist does not mean that this technology should not be developed.

For example, many bridges have collapsed over the centuries, but that does not prevent us from building new bridges with better technology, design, and measures. We learn from our engineering mistakes and move forward with better designs.

The ICO bubble and the FTX disaster demonstrate the potential harms from fraud.

Balancing Privacy and Enforcement of AML/CFT Measures

CBDC will become widely adopted only if it preserves the anonymity of its users. One of the main reasons why many people do not choose online payment methods is the lack of trust in financial institutions associated with privacy concerns[5]. Even a partial anonymity in the domain of finance represents a significant risk associated with the potential for fraud, money laundering, and violation of sanctions policy. Anti-Money Laundering/ Countering Financial Terrorism (AML/CFT) regulation will be the primary safeguard against the illicit use of digital money; however, unnecessarily restrictive regulation of digital assets, including CBDCs, might prevent achieving their potential.

Opportunities of CBDC for Effective, Efficient and Feasible AML/CFT Measures

CBDCs bring a new opportunity for AML/CFT measures. Sidorenko et al. (2021) and Soderberg et al. (2022) expect that CBDC will be a useful tool to combat any crime related to money settlements because of its traceability as compared to cash which is anonymous and therefore lacks an audit trail. Mahari et al. (2022) suggest CBDC to be resistant to money laundering and financing of terrorism by leveraging strong forms of digital identity connected to customer due diligence, ongoing algorithmic transaction monitoring, and inter-operable record keeping. Kakebayashi et al. (2023) analyze the current cost of AML/CFT measures of the stakeholders (government, financial institutions, and users), and suggest that the AML/CFT system associated with CBDC should consider a tiered approach based on the level of assurance, collective customer due diligence (e.g. cross-industry), automated analysis and evaluation, capacity building of human resource for judgment and reporting, and an efficient streamlined process.

Offline Transaction Capability and AML

A CBDC ideally would need to be available offline and have appropriate data privacy protections

---

but in the past 12 months used at least one of the nonbank transaction or credit products or services that are disproportionately used by unbanked households to meet their transaction and credit needs. (https://www.fdic.gov/analysis/household-survey/)

[4] The role of financial intermediation in economic growth has been widely recognized in theoretical and empirical research. Finance can stimulate the main drivers of growth such as capital and total factor productivity (https://deepblue.lib.umich.edu/bitstream/handle/2027.42/132992/wp1091.pdf?sequence=1).

[5] Based on an article from the San Jose Spotlight (December 31st, 2022): "According to a survey conducted by the Federal Deposit Insurance Corporation (FDIC), the rate of unbanked households, or homes that do not have at least one bank account, jumped from 1.9% to 13.2% between 2019 and 2021 in the San Jose metro area, far more than any other metropolitan region in the country. … People from Mexico and Latin American countries don't generally trust the banks." (https://sanjosespotlight.com/why-do-san-jose-residents-avoid-banks/)

in place to achieve financial inclusion, accessibility, and broad usability. CBDCs will require features optimal for the timely tracking of illegal activity and enforcing economic sanctions, even in an offline environment. However, offline transaction capability is very difficult to achieve in practice and requires further research.

Cross-Border Payment Frictions

Contrary to the objective of cross-border payment facilitation, if cross-border payment becomes easier with the CBDC, protective measures, such as AML screening and enforcing trade sanctions by the Foreign Assets Control office, are likely to increase frictions in cross-border payments. Therefore, related regulations that would influence the efficiency of cross-border payment must be considered very carefully to mitigate unnecessary friction as much as possible.

There would also have to be further considerations on the capital restriction, limit on the transaction amount and the holding limit. Capital restrictions associated with CBDC are beneficial for AML/CFT regulation and for preserving commercial bank money, but have a negative effect on achieving system efficiency with economies of scale and on the efficiency of CBDC as an effective monetary policy tool.

Threat to the Stability of a Private Banking System

A CBDC has the potential to threaten the stability of the private banking system by draining deposits from the system in a crisis. A CBDC where the central bank offers full-service general, non-intermediated, purpose accounts would be the most disruptive from an economic perspective. A direct CBDC could pose a threat to commercial banks by reducing the need for depository institutions associated with a potential decline in the deposit base. Private bank deposits are routinely used to extend credit to consumers and firms. Even an intermediated CBDC that preserves the role of depository institutions in providing accounts to the public might severely impact the intermediation process in times of financial panic due to the flight to quality, in this case, a flight to CBDCs.

The most popular type of digital money used in daily private transactions is commercial bank money, that is, money digitally stored in private bank accounts. It remains uncertain to what extent CBDCs will be compatible with commercial bank money. In this respect, CBDCs might disrupt important functions of financial intermediaries. Banks hold demand deposits for consumers; they conduct money transfers; they facilitate the distribution of money from the central bank to consumers.

It is important to note that when CBDC is included into this basic intermediary model, the primary objectives and functions of CBDC might compete directly with commercial bank money. From one perspective, CBDCs reduce the credit and liquidity risk in the financial system. However, at the same time, commercial banks' lending and borrowing depend on commercial bank money. Even if commercial banks are involved in the intermediation of retail CBDCs, their lending services might still be compromised. Lower public demand for commercial bank money could significantly reduce the number of funds available to extend loans. Therefore, CBDCs might have a significant impact on the profitability of commercial banks. This problem arises specifically in the case of a retail CBDC in which clients would have the option to choose to hold their money in the form of CBDC instead of commercial bank money. In a CBDC model, where payroll and savings would be accumulated in a CBDC balance, commercial banks would not be able to use these CBDC balances for investment. They could offer higher interest than the CBDC in order to attract deposits, increasing their cost of operation. This is one of the main arguments for introducing limits on the potential use of CBDC. Limits on the transaction and holding amounts are designed not only to comply with AML/CFT regulation but also to control the shares of publicly- and privately-issued money in the financial system.

Excessive Segmentation of the Money Market

Different forms of digital money, including CBDC, are increasingly organized into closed-loop systems. This occurrence creates a risk of excessive segmentation of the money market, causing digital payment platforms to be poorly interoperable and digital money not easily transferable[6]. Publicly issued money must guarantee that it is universally accepted as payment, equally valued regardless of its digital form, location, and regardless of the identity of the user. One of the main reasons for developing a CBDC is to preserve the role of public money in a digital economy, emphasizing the use case of CBDC as the primary medium of exchange. The uniformity of money and its role as a medium of exchange are the two components of public currency that define monetary sovereignty and which must be preserved in the CBDC.

3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

Good Regulation to Achieve Objective

One of the biggest challenges to mitigating risks from digital assets is regulation. Regulation that is too permissive opens the door to fraudsters and other criminals. Regulation that is too restrictive suppresses valuable innovation. A naive approach is to say: “same activity, same regulation.” However, this does not always make the most sense. For example, Uber and Lyft provide a service similar to traditional taxis but are very different. New York City taxi drivers are frequent robbery targets, so they are required to have bulletproof partitions to protect the driver. Uber and Lyft drivers in the U.S. don’t carry cash, so they are not robbery targets. Thus, they don’t need bulletproof shields. This illustrates that even if it is “the same activity” (i.e, providing a riding service from the place the users are to the place where instructed), it does not have the same risk (i.e., robbery) and therefore does not apply the same regulation (i.e., the requirement of bulletproof partitions).

The same thing applies to digital assets. Standard regulatory objectives include the prevention of fraud, preventing the failure of critical intermediaries, reduction of systemic risk, and supporting economic growth. There is much research that needs to be done in order to figure out the right way to achieve these objectives in the digital asset space.

Up-to-Date Tools (Regtech and Suptech) and Capacity Building for Effective Enforcement

There is also a need for regtech research into the use of digital asset technology itself to achieve regulatory objectives. The transparency and programmability of blockchain technology create the opportunity to use the technology to prevent and prosecute fraud.

At the same time, supervisory technology to enhance financial supervision must be developed. With a large number of transactions and regulatory technology to better detect illicit activities, law enforcement, and investigators will also have to evolve in a timely manner. Empowering the government to have sufficient tools to react to the constantly evolving situation is necessary to secure effective enforcement.

In addition, as Kakebayashi et al, (2023) pointed out, AML/CFT measures are costly, and human resources are limited for both the government and the private sector. The tools are crucial to detect suspicious financial activities, but the investigation and the judgemental process cannot be fully automated. Therefore, capacity building on human resources, which can effectively use Regtech and Suptech, is a necessary action for both the public and private sectors.

Maintaining availability of offline payment

As a result of experiments of open-loop e-cash systems conducted by the Bank of Japan in 1999 and 2000, it turned out that perfect open-loop and offline payment is impossible, considering communication errors. This is a technical restriction resulting from network theory. At that time, a user’s wallet (a smart card) and a bank need to maintain and synchronize status information to process reimbursement when a payment error happens. In the case of Mondex, there was a special agreement that

[6] Based on a report published by the ECB (Jan 2022) available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703337/IPOL_STU(2022)703337_EN.pdf

the organizing company didn't have any responsibility to return the money when there was some communication error or wallet trouble. The availability of offline payments is an essential merit of CBDC against other digital financial means. Combining state-of-the-art technology such as (not-scalable) permissionless blockchain with the above simple and matured payment protocols to achieve both scalability and maximum availability is a key area of technology research and development.

Mitigation of cyber security risks

In 2022, there was a $3.04B loss due to security incidents at blockchain platforms and their applications [19]. Although blockchain technology and cryptography fulfill some security requirements, they don't cover all security requirements of the entire money system. Unfortunately, the security management process depends on each specific system, and we need to execute the ISMS (ISO/IEC 15408) process for each system design and implementation to manage security risks. There are many aspects to consider to ensure the security of the entire digital money/asset system: (1) cryptographic algorithms (e.g. ECDSA), (2) cryptographic protocols (e.g. TLS), (3) application protocols (secure transaction and privacy protection), (4) security of implementation of business logic (e.g. smart contract), (5) implementation of hardware and software (supply chain risk), and (6) operations (e.g. cryptographic key management). This is a role of a federal governmental institution like NIST to establish a comprehensive framework to facilitate system security for digital assets leveraging existing international standards (e.g. ISO/IEC 27000 series, ISO/IEC 15408, and ISO/IEC 29128), and federal standards.

Wallet and its governance

A wallet, regardless if it is software-based or hardware-based, is an important point of failure in the digital asset ecosystem. It is a device/software to securely manage private cryptographic keys and securely conduct cryptographic operations. At the same time, a wallet provides functionalities to authenticate a human and authorize users to use designated online services. Hence, a user wallet is the intersection of security, privacy, identity, AML/KYC/CFT, and business model. In general, security design and implementation of a device/security are managed using ISO/IEC 15408, CMVP, and FIPS140-3 for cryptographic modules. However, there is no ISO/IEC 15408-related work like security targets and protection profiles that are not defined for wallet hardware/software. Research and development on secure wallets are required.

Wallet governance is another essential issue. A trusted Execution Environment (TEE) and Secure Enclave (SE) are the core technology in securing the wallet. However, the design of such secure hardware is dominated by a very small number of companies that can design processors for smartphones and PCs. It implies that those companies are a point of failure in the digital asset ecosystem, even if we use permissionless blockchain for decentralization. Building a comprehensive framework for wallet governance is important for responsible development.

Cryptographic key management and its life-cycle

The most complicated part of the operations of systems based on cryptography is cryptographic key management. It is difficult even for experts. We cannot assume that general users of digital assets and CBDC manage cryptographic keys securely. Thus, we need to establish technologies and operation frameworks for any case of cryptographic key operations. It contains a key management life-cycle for the digital assets and CBDC. Generally, the key operation model for blockchain is different from the key management model for public key infrastructure (PKI), which is documented by NIST SP800-57. It is required to establish such a key management model and methodology specialized for digital assets.

Design principles for cryptographic tools in a CBDC

There are many different ways to design a CBDC, and there is a need for more research to explore the best option. A properly designed CBDC will be efficient, secure, low-cost, and environmentally friendly. Secure incorporates protecting financial privacy while also preventing money laundering.

However, it is not entirely clear how best to achieve all of these objectives. A well-diversified research program utilizing researchers with a variety of backgrounds and affiliations will help to identify universal standards. Whether or not the U.S. issues a CBDC, having 90% of central banks actively exploring the development of CBDC (Kosse and Mattei, 2022), it is crucial from an economic and national security perspective to establish a domestic reservoir of expert researchers to collaborate with the government. This would serve the best interest of the people who will be exposed to a new financial system with a CBDC directly or indirectly.

There are unmitigated risks related to fraud, money laundering, and system attacks that are posed by advanced transaction functionality like programmability and offline access. These advanced features of CBDC present significant technical complexity to ensure system security and reliability. There are risks related to fraud, money laundering, and system attacks. CBDCs require more than just integration to the banking system. They require expertise in AML/CFT, cryptography, and governance to ensure compliance with existing laws and regulations. New features present risks to implementation and operation because they are relatively new and not yet well controlled. Designing the advanced transaction functionality of CBDC will be the most time-consuming component of the CBDC system.

The development and application of appropriate cryptographic tools in a CBDC setting is vital to ensure optimal security features of CBDC. There is a tradeoff between user privacy and transaction transparency. Privacy-enhancing technologies can also be used to enhance transaction confidentiality. In conducting a CBDC transaction, information on private transactions should be recorded only for auditing purposes. Private transactions should be conducted without unauthorized third parties interpreting the transaction information. A cryptographic commitment could be designed to ensure the settlement of transactions without revealing basic transaction details to unauthorized ledger participants. In this context, zero-knowledge proof tools could be designed to create confidential transactions, information about which could be verified without revealing it. In more general terms, privacy-enhancing technologies could be applied to restrict the sender/receiver information visible on a public transaction ledger. Each privacy-enhancing technology has a different effect on the visibility and interpretability of transaction-related data. Using multiple privacy-enhancing technologies in combination may ensure a higher level of confidentiality.

However, enhanced cryptography complicates Know-Your-Customer (KYC), AML compliance by limiting access to transaction information. In that case, information for auditing (i.e. to comply with regulations) would need to be obtained through alternative data sources. These trusted sources could become third parties conducting the implementation of cryptographic tools, possessing the necessary information that the auditor could use to interpret the transaction information with certainty.

Trusted ledger participants would be required to cooperate with the auditor following regulations with an enforcement mechanism. If the auditing process consumes an excessive amount of computational power, it may even be considered infeasible to implement cryptographic tools.

4. R&D that should be prioritized for digital assets

(1) Security

Security of digital-asset and CBDC systems is an essential foundation for why everyone uses such new financial means. At the same time, if some vulnerability is found, the adversary can utilize it to steal a huge amount of money in a very short time. It is a specific financial risk in digital asset systems. Thus, having a common framework to analyze, design, implement, and operate security mechanisms is the most important first step.

(2) Wallet: the intersection of Identity, privacy, and key management

As written before, the user wallet is the intersection of security, privacy, identity, AML/KYC/CFT, and business model. It is necessary to consider appropriate security and privacy technology for the user wallet, as well as management of supply chain risks. Governance mechanisms for wallet design, implementation, and operations are decided by multi-stakeholders.

(3) Incentive mechanisms and business models to encourage all stakeholders for responsible development.

The digital asset and CBDC-powered digital money system cannot be established by only central banks and the government. Cooperation with private sectors and a large amount of exploration and investment of resources by private sectors are necessary. In this regard, designing good incentive mechanisms and business models to encourage all stakeholders, including the private financial sector, to buy-in is essential for responsible development.

(4) Scaling regulatability by leveraging Regtech and Suptech

Appropriate regulation of digital assets is a major priority. Clearly, this technology has great potential, but achieving that potential will require intelligent regulation. Current regulators are valiantly attempting to apply old laws designed in a different era to this new technology. Unfortunately, this has resulted in a chaotic and incoherent approach that is chilling the appropriate development of this technology. As the old saying goes, they are trying to put new wine into old wineskins, which does not go well.

(5) Reconsidering the role of intermediation

Other than the policy implications of CBDCs, there are major technical hurdles associated with building an efficiently functioning digital system infrastructure. There exist major technical limitations associated with the level of intermediation, interoperability, use restrictions, off-ledger functionality, cryptographic method, hardware interface, offline functionality, authentication method, programmability, method of data storage, accessibility of the core ledger, and unit fungibility. Each of these elements requires technical specialization, which influences the entire CBDC system structure and in many cases, these technical adjustments restrict the primary CBDC objectives. CBDC has the potential to improve transaction processing, further reduce transaction costs and add advanced functionality in the form of programmability. However, it must be emphasized that many desirable features of CBDC are currently not easy to implement in practice due to technical constraints, high costs, or the early stage of development.

Intermediation functions include distributing CBDC, providing custody and wallets for CBDC balances, validating transactions, settling transactions, providing user interfaces, offering customer service, and ensuring AML/CFT compliance. All of these functions require appropriate technology infrastructure, experience in providing the service, and compliance with regulations. Private service providers other than commercial banks are likely to also be involved in providing CBDC services. This form of extended intermediation could help increase financial inclusion, encourage specialization in specific intermediary functions, increase competition among CBDC service providers, and promote innovation in payment technology. An intermediary model of CBDC would ensure private sector participation, fostering coordination between multiple organizations, the central bank, commercial banks, and third parties to provide interoperability with existing payment systems.

(6) Proper use of blockchain and distributed ledger technology

Many CBDC models remain to be based on a distributed ledger design, wherein network participants operate private nodes through which transactions are processed and where transaction information is stored. However, there are serious operational limitations and security issues associated with a decentralized model. In the first phase of the MIT Project, Hamilton concluded that distributed ledger technology in its current form does not satisfy CBDC operational requirements: a transaction time of fewer than five seconds and a transaction rate of more than 100,000 transactions per second[7].

Decentralized ledger issues are associated with scalability, interoperability, and security issues.

[7] Project Hamilton is studying the design of a transaction processor to be part of a large retail payment system (https://dci.mit.edu/opencbdc).

Existing digital payment platforms (e.g. Visa) can process up to 24,000 transactions per second. In comparison, existing blockchain networks (e.g. Ethereum) can process only up to 20 transactions per second. This fact underscores the stark scalability limitations of a blockchain-type design. There is evidence that distributed ledger technology does not effectively support retail payment networks. A trial conducted by the Japanese Digital Currency Forum demonstrated that a prototype decentralized interbank network offers limited interoperability between *The Common Area* decentralized ledger and *The Business Process Area* coordinating the distribution of digital currency, linking payments with simultaneous delivery of goods and services, and recording payment instructions[8].

(7) Interoperability

More broadly, CBDC interoperability is associated with private interface connectivity. International banking and private platform connections to the CBDC system have experimented in the form of asset swaps and interconnected CBDC ledgers, which are difficult to implement and also introduce limitations to the functionality of existing payment platforms. Differences in governance and regulation standards across different payment methods are the key impediment to CBDC interoperability. A basic example of interoperability is the possibility of direct convertibility between CBDC and bank deposits. This function is important to improve liquidity transfers between CBDC and commercial bank money to ensure the stability of the financial system and to enforce holding limits on CBDC with the possibility of transferring excess balances to a bank account.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem

Importance of leading international standards

Assuming that one of the prime benefits of digital assets is for cross-border payments, creating careful international standards is essential to ensure secure operations regarding digital assets and CBDC. Now, ISO TC68, ISO TC307, and ITU-T are working on international standardization in this area. Generally, the central bank community focuses on ISO TC68 standards, and ISO and ISO/IEC JTC1 have many relevant international standards. Thus, focusing on creating a series of ISO standards by leveraging existing standards should be an effective way forward. Before launching U.S. CBDC, it is assumed that over 10 new international standards will be needed to ensure the security and privacy of money systems. Designing a strategy and a roadmap for those groups of standards is needed.

Leading multi-stakeholder dialogue for proper regulations and supervision.

With a proper and supportive regulatory framework, the private industry will continue to work in applying digital asset technology in various applications. To realize such a regulatory and supervisory framework, collaboration among all stakeholders is required. In 2019, G20 agreed to welcome the FSB report [5,6] on decentralized finance to encourage the establishment of multi-stakeholders dialogue. Blockchain Governance Initiative Network (BGIN)[9] was established to organize such a multi-stakeholder dialogue in 2020. It is necessary to leverage this organization to make the U.S. a leader in the multi-stakeholder dialogue.

6. Other information that should inform the R&D Agenda

Learning good and bad experiences from past experiments

In the 1990s, there were several national-level and private-sector level digital money projects. They included an experiment by the Bank of Japan, called "Internet Cash," Mondex (by Master Card), and Visa Cash (by Visa). Their protocols are over 25 years old, and they didn't cover AML/KYC/CFT

---

[8] The first phase of the DCJPY digital currency project was conducted by the Japanese Digital Currency Forum (https://www.decurret-dcp.com/.assets/forum_20211124wp_en.pdf).

[9] https://bgin-global.org/

requirements because they were invented before September 11, 2000. However, these experiments produced many good experiences and bad experiences (impossibility results). To avoid refinding the same problems and reinventing the wheel, we should learn from past similar experiments.

Diversity in design principles

When attempting to estimate the resources required to launch a CBDC, the government must recognize different sets of design choices which prioritize different CBDC objectives. A minimally complex design of CBDC sidelines concepts associated with offline payments, programmability, and privacy-enhancing technology, instead focusing on the simplicity of development, administration, and delivery. If the government decided that it was absolutely beneficial to launch a CBDC as soon as possible for economic and social benefit, it would be essential to identify relevant stakeholders and participants in the CBDC system. In order to support a relatively fast timeline of implementation, financial intermediaries would have to develop sufficient technical CBDC functionality; a legal framework for the minimum viable CBDC operations would have to be devised by appropriate regulatory agencies; and public research funding and private investment would need to be secured. Having said that, currently, the development speed of CBDC is not a significant policy objective. Through academic research, it is more important to recognize the risks and opportunities associated with a CBDC product and identify specific use cases where CBDC is a preferred digital method compared to existing payment solutions.

This summary recognizes that while CBDC has the potential to provide social and economic benefits in the areas of financial inclusion, transactional efficiency, and national security, the immediate advantages of CBDC in relation to other privately issued digital assets, assuming their appropriate regulation, are not obvious and require further exploration. That includes carefully assessing the necessary layers of technology comprising the CBDC infrastructure. As we have mentioned previously, while there exist creative proposals of the CBDC technical framework (e.g. distributed ledger technology), most of these are poorly interoperable with the existing highly centralized central bank payment systems. Establishing a cohesive technical framework for a CBDC requires a more targeted approach focusing on expanding the existing system rather than envisaging a new parallel payment platform.

Sincerely,
Georgetown University, CyberSMART Research Center

Dr. James Angel (Georgetown University, McDonough School of Business)
Dr. Shin'ichiro Matsuo (Georgetown University, Department of Computer Science)
Gerard P. Presto (Georgetown University, Department of Economics)
Michi Kakebayashi (University of California, Berkeley, Goldman School of Public Policy)

References

[1] Bank of Japan & ECB. *Project stella: BoJ and ECB Joint Report on DLT : 日本銀行 Bank of Japan*. Retrieved March 3, 2023, from https://www.boj.or.jp/en/paym/fintech/rel200212a.htm

[2] Barrdear, & Kumhof, M. (2022). The macroeconomics of central bank digital currencies. *Journal of Economic Dynamics & Control*, *142*, 104148. https://doi.org/10.1016/j.jedc.2021.104148.

[3] Digital Currency Forum. *DCJPY*. Retrieved March 3, 2023, from https://www.decurret-dcp.com/.assets/forum_20211124wp_en.pdf

[4] Federal Deposit Insurance Corporation (FDIC). November 14, 2022 "National Survey of Unbanked and Underbanked Households" https://www.fdic.gov/analysis/household-survey/

[5] FSB, "Decentralised financial technologies: Report on financial stability, regulatory and governance implications." https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications/

[6] G20, "G20 OSAKA LEADERS' DECLARATION." https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

[7] Howey, B. (2023, January 5). "*Why do San Jose residents avoid banks?"* San José Spotlight. Retrieved March 3, 2023, from https://sanjosespotlight.com/why-do-san-jose-residents-avoid-banks/

[8] *The Digital Euro: Policy implications and perspectives - europarl.europa.eu*. The digital euro: policy implications and perspectives. (n.d.). Retrieved April 11, 2022, from https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703337/IPOL_STU(2022)703337_EN.pdf.

[9] The Clearing House. (2021, July 27). *On the Road to a U.S. Central Bank Digital Currency*. Retrieved March 3, 2023, from https://www.theclearinghouse.org/payment-systems/articles/2021/07/07272021_us_central_bank_digital_currency

[10] The Federal Reserve. *FedNow service*. Retrieved March 3, 2023, from https://www.frbservices.org/financial-services/fednow/about.html

[11] Institute and Faculty of Actuaries. *A Cashless Society - Benefits, Risks and Issues*. Retrieved March 3, 2023, from https://www.actuaries.org.uk/system/files/field/document/A%20Cashless%20Society%20in%202019.pdf

[12] Kakebayashi, Michi and Presto, Gerard P. and Yuyama, Tomonori and Matsuo, Shin'ichiro, 2023. "Policy Design of Retail Central Bank Digital Currencies: Embedding AML/CFT Compliance." Available at SSRN: https://ssrn.com/abstract=4366778 or http://dx.doi.org/10.2139/ssrn.4366778.

[13] Mahari, Robert, Thomas Hardjono, and Alex Pentland. 2022. "AML by Design: Designing a Central Bank Digitalcurrency to Stifle Money Laundering." MIT Science Policy Review 3 (August), 57–65. https://doi.org/10.38105/spr.j0hildxtyi.

[14] MIT Digital Currency Initiative. (n.d.). *A High Performance Payment Processing System Designed for Central Bank Digital Currencies*. Retrieved March 3, 2023, from https://dci.mit.edu/opencbdc

[15] Náñez Alonso, S. L., Echarte Fernández, M. Á., Sanz Bas, D., & Kaczmarek, J. (2020, May 26). *Reasons fostering or discouraging the implementation of central bank-backed digital currency: A Review*. MDPI. Retrieved March 3, 2023, from https://www.mdpi.com/2227-7099/8/2/41

[16] Sidorenko, E.L., Sheveleva, S.V., Lykov, A.A. 2021. "Legal and Economic Implications of Central Bank Digital Currencies (CBDC)." In Innovative Economic Symposium. Springer. 496-502.

[17] Soderberg, Gabriel, Marianne Bechara, Wouter Bossu, Natasha X Che, Sonja Davidovic, John Kiff, Inutu Lukonga, Tommaso Mancini Griffoli, Tao Sun, Akihiro Yoshinaga. 2022. "Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons." IMF FinTech Notes No 2022/004.

[18] Yusifzada, L. (n.d.). *Financial intermediation and economic growth*. Retrieved March 3, 2023, from https://deepblue.lib.umich.edu/bitstream/handle/2027.42/132992/wp1091.pdf?sequence=1

[19] White, Molly. "Web3 is Going Just Great." *Web3 is Going Just Great*, 2022, https://web3isgoinggreat.com. Accessed 3 March 2023.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Damilola Arowolaju

DEMOCRACY IN OUR NEW WORLD:

Utilizing Blockchain Technology to Digitize Government Functions

Abstract

If the question is what government can do, the answer is your imagination. Blockchain technology possesses many applications for wealth generation in the financial sector. First adopters pursued use cases that generated profits, which funded their work. They established the rails and digital infrastructure that governments can utilize to improve government functions. Instead of seeking to tamper innovation, governments should utilize the infrastructure developed by first adopters to improve the functions and services they offer to their citizens. This paper addresses the use cases of blockchain technology in government.

Arowolaju, Damilola G.

Brown, Devron

I. Introduction

Jospeh Schumpter coined the term creative destruction, which occurs when innovative technology improves (or destroys) old processes. Today, automation and globalization drive creative destruction. Technological advancements allow firms to automate domestic manufacturing; whatever cannot be automated, globalization enables companies to outsource—at low costs. While some decry this process and focus on the losses resulting from it, technological innovation and creative destruction are inevitable. So rather than focusing on preventing the inevitable, attention should focus on minimizing harms when losses occur—and maximizing the gains.

On the horizon of another technological revolution is 5G technology, enabling faster wireless connection with larger bandwidth. Proponents of 5G Technology confidently claim that it will render blockchain technology ubiquitous: from devices connected to the internet of thing, to smart cities, and more. This claim is buttressed by lawmakers, who recently encouraged utilizing blockchain solutions to respond to the coronavirus pandemic.[1] But lawmakers are also growing antagonistic towards blockchain, because they are yet to appreciate the use cases for every-day people.[2]

As governments advance, they seek solutions to meet new demands. COVID-19 forced governments across the world to rethink the functioning of government to best meet citizens' needs. Technological innovation improved the functioning of businesses across the world. So, too, can technological innovation improve the functioning of government. McKinsey estimates that "government digitization, using current technology, could generate over $1 trillion annually worldwide."[3] This digitization can occur utilizing blockchain technology. Governments are already establishing a framework to digitize functions with blockchain, such as Illinois in 2018, with the final report to the General Assembly from the Illinois Blockchain and Distributed Ledger Task Force. [4]

This paper first describes the best case study of what digitizing governmental functions with blockchain technology looks like in practice: Estonia. From there, it provides a background on blockchain technology and describes how it functions. Then, it addresses the use cases of the technology that governments should pursue. Finally, it addresses inherent concerns digitization brings—particularly privacy and loss jobs due to automation.

II. Estonia Case Study

Estonia is a Baltic nation once known for its logging industry, but is now known as a digital democracy that even automates the counting of logs.[5] Estonia is a case study for what a digital democracy can look like.[6] Estonia's transition into a digital-democracy is housed under a project called *e-Estonia*, which is "a coördinated governmental effort to transform the country from a state into a digital society."[7] Under *e-Estonia*, the country digitized governmental functions such as legislation,

---

[1] Letter from Darren Sotto, Member of Congress & Tom Emmer, Member of Congress, to Steven T. Mnuchin, Secretary of the Treasury (Apr. 23, 2020).

[2] Letter from Elizabeth Warren, United States Senator, to Janet Yellen, Secretary of the Treasury (July 26, 2021).

[3] Bjarne Corydo, Vidhya Ganesan, and Martin Lundqvist, *Transforming government through digitization*, MCKINSEY.COM, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/transforming-government-through-digitization#, Nov. 16, 2016.

[4] Cab Morris, John Mirkovic & Jennifer M. O'Rourke, *Illinois Blockchain and Distributed Ledger Task Force Report to the General Assembly* (January 31, 2018), https://www2.illinois.gov/sites/doit/Strategy/Documents/BlockchainTaskForceFinalReport020518.pdf; *see also*, Illinois House Joint Resolution 25.

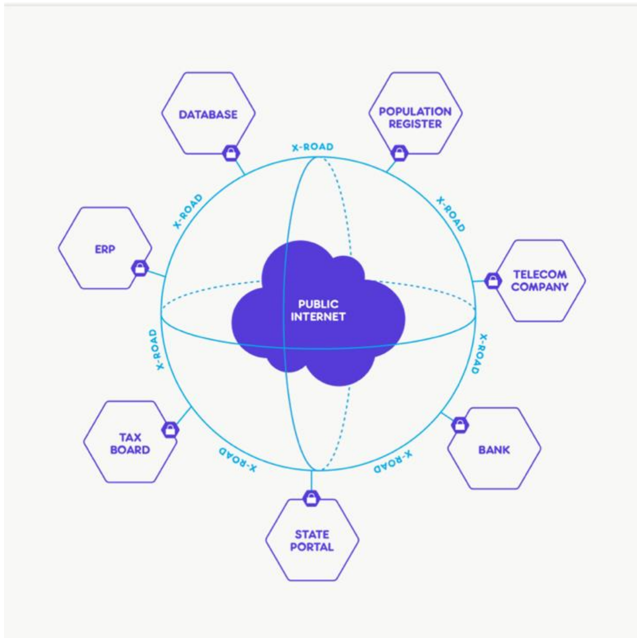
[5] Nathan Heller, *Estonia, the Digital Republic*, THE NEW YORKER, December 11, 2017.

[6] *Id.*

[7] *Id.*

justice, policing[8] voting, education,[9] healthcare, banking, taxes[10], and more.[11] In fact, "apart from transfers of physical property, such as buying a house, all bureaucratic processes can be done online."[12] This process cuts down bureaucracy—saving the country 2% in G.D.P. a year.[13]

Here's how the program works. Basically, Estonia's data exchange platform, X-Tee (formerly known as X-Road) allows registered users to access data.[14] Once registered, every Estonian citizen owns a digital id card, allowing citizens to decrypt files, affix digital signatures on files, and engage within the digital society.[15] And in Estonia, you only need to enter data once. Once Estonian citizens



log their data, that information is stored locally at the specific institution. For example, your primary doctor maintains your medical records. But should you transfer to another institution and switch primary doctors, your new doctor can request access for your medical records on X-Tee. But not all data citizens enter is necessarily accessible. Citizens can choose to hide the data they enter. And that is because Estonia has decided that "[a] key tenet of [*e-Estonia*] is that an individual owns all information recorded about him or her."[16]

Looking at Estonia's digital success: The European Union developed its own digital strategy—working towards a digital government.[17][18] And the EU is already known for its progress in data

---

[8] *Security and Safety*, E-ESTONIA, https://e-estonia.com/solutions/security-and-safety/e-law/ (last visited Oct. 3, 2021).
[9] Sally Weale*, Lessons from Estonia: why it excels at digital learning during Covid*, GUARDIAN, Oct. 30, 2020, https://www.theguardian.com/world/2020/oct/30/lessons-from-estonia-why-excels-digital-learning-during-covid.
[10] *Business and Finance,* E-ESTONIA, https://e-estonia.com/solutions/business-and-finance/e-banking/ (last visited Oct. 3, 2021).
[11] Heller, *supra* note 5.
[12] *Id.*
[13] *Id.*
[14] *See generally*, Republic of Estonia Information System Authority, *Data Exchange Layer X-tee*, Republic of Estonia (last accessed May 13, 2020), https://www.ria.ee/en/state-information-system/x-tee.html.
[15] *Id.*
[16] Heller, *supra* note 5.
[17] *Id.*
[18] *See generally*, European Commission, *Shaping Europe's Digital Future: The European Digital Strategy*, European Union, (last accessed May 13, 2020) https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy.

regulation and protection, with their General Data Protection Regulation (GDPR).[19] Whereas, the U.S—according to Marten Kaevats, Estonia's national digital adviser—is a digital mess.[20] "Data architecture [in the U.S.] was too centralized. Citizens didn't control their own data; it was sold, instead, by brokers. Basic security was lax. . . . The U.S. had backward notions of protection . . . and the result was a bigger problem: a systemic loss of community and trust."[21]

In 2007, Estonia faced a massive cyber-attack from Russia that destabilized the digital society.[22] As a result: the NATO Cooperative Cyber Defense Center of Excellence was formed, which serves as a think tank and training facility.[23] Estonia also integrated K.S.I.—a blockchain platform—into its digital system to improve security.[24] The state also built a server closet in Luxembourg, with a backup of its systems.[25] So, if a digital invasion occurs, government officials can log on remotely—using digital signatures—to issue orders and run the government remotely through the cloud.[26] The following section will now describe how blockchain technology works. It is not a hyper-technical description, because a technical understanding is not necessary to utilize blockchain technology. For example, many people send emails and utilize the internet without a technical understanding of how it works.

III. Blockchain Technology Background

a. Origination of Blockchain

Before understanding how blockchain technology works, it is import to understand its genesis. Blockchain technology was originally created as a platform for Bitcoin, a cryptocurrency.[27] Bitcoin's goal: making electronic payments to other parties without third parties, like a bank—a peer-to-peer transfer of money.[28] When people engage in financial transactions through third parties, there are "inherent weaknesses."[29] The "inherent weaknesses" rest in relying on third parties and the transaction costs associated with these transactions.[30] For example, when sending money overseas, there are usually large transaction costs associated.[31] Further, the key issue is ensuring the purported seller is who they say they are and actually have the bargained for good or service.[32] For our electronic payments and transactions to occur, we must bare these transaction costs and trust the parties involved.[33] But at times, transaction costs are too high and we cannot trust parties. Bitcoin—a decentralized peer-to-peer payment network—reduced these transaction costs and the amount of trust one must have with the transacting party.[34] Through Bitcoin, parties can make payments without relying on banks and automatically verify the authenticity of the purported seller and their goods or

[19] Matt Burgess, *What is GDPR? The Summary guide to GDPR compliance in the UK*, WIRED, March 24, 2020.
[20] Heller, *supra* note 5.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] Heller, *supra* note 5.
[25] *Id.*
[26] *Id.*
[27] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).
[28] *The great chain of being sure about things*, THE ECONOMIST, Oct. 31, 2015.
[29] NAKOMOTO, *supra* note 27.
[30] *Id.*
[31] ECONOMIC IMPLICATIONS OF REMITTANCES AND MIGRATION, (Dilip K. Ratha ed., 2006).
[32] NAKOMOTO, *supra* note 27..
[33] *Id.*
[34] *Id.*

services. This is what Satoshi Nakamato, the unknown creator(s) of Bitcoin had in mind when they released its white paper on blockchain and Bitcoin in 2008, in the wake of a massive financial crash.[35]

b. How Blockchain Technology Works

Blockchain technology, at its most basic level, is a computer file used for storing data.[36] The information stored varies. For example, the data could contain information about a transaction: purchaser i.d.; seller i.d.; the good or service; self-executing contract terms. The blockchain could contain information regarding a specific item, such as the owner of the deed to real property.[37] Each file or block contains one transaction or set of transactions, engrained with identifying codes.[38] Then, each subsequently validated transaction creates another block that links the earlier transaction and codes—creating a chain, a blockchain or electronic ledger.[39] This allows parties to trace transactions and items from their origin and verify authenticity because a block will not be added to the blockchain unless the transaction is validated as authentic.[40] When each block is added, every user or node's blockchain is updated to reflect it, thus, creating an open network of information.[41]

There are three key characteristics of blockchain technology: (1) decentralization, (2) cryptography, and (3) openness.[42] We will take them in turn.

i. Decentralization

Most computer files are stored only on a single computer. With blockchain, however, the files are distributed amongst any computer (or node) connected to a single network.[43] In this way, Blockchain technology is like a shared drive. But unlike a shared drive no single owner controls or edits the files (depending on if it is a public or private blockchain). Instead, changing or editing a file—altering—a block in the chain—requires achieving consensus amongst the users in the network that store their own separate and identical files on the blockchain.[44] If there is no consensus, no change can occur. In a blockchain platform that utilizes proof of work, this concept is called mining. It is energy intensive because it requires miners to guess the corresponding hash value first to validate the block, so they use fast computers guessing millions of numbers that require immense computing power. And the reward for mining is cryptocurrency.[45] But there is less energy intensive consensus protocol called proof of stake, which requires random groups or "committees" of users or "validators" to stake cryptocurrency before confirming individual transactions, risking losing the staked cryptocurrency for confirming invalid transactions, but gaining cryptocurrency by confirming valid transactions.[46]

---

[35] The great chain of being sure about things, *supra* note 3.
[36] Bernard Marr, *What Is Blockchain? A Super Simple Guide Anyone Can Understand*, BERNARD MARR & CO.
[37] The great chain of being sure about things, *supra* note 3.
[38] NAKOMOTO, *supra* note 27.
[39] The great chain of being sure about things, *supra* note 3.
[40] JAMIE BERRYHILL, THEO BOURGERY & ANGELA HANSON, *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector*, OECD WORKING PAPERS ON PUBLIC GOVERNANCE, 13 (2018).
[41] *Id.* at 18.
[42] MARR., *supra* note 36
[43] *Id.*
[44] *Id.*
[45] *See generally* Andrew Tar, *Proof-of-Work Explained*, COINTELEGRAPH, https://cointelegraph.com/explained/proof-of-work-explained, Jan. 17, 2008.
[46] *See generally The Beacon Chain Ethereum 2.0 explainer you need to read first*, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/, May 23, 2020.

ii. Cryptography

Blockchain technology uses asymmetric cryptography to encrypt and authenticate data within the chain, creating inherent security.[47] Asymmetric cryptography is an encryption mechanism where the sender uses one key to encrypt and recipient uses a different key to decrypt. This is different from symmetric cryptography where the same key is used to encrypt and decrypt. Imagine Alice wants to pay Bob for a sandwich using Bitcoin. Bob has a private key attached to his wallet and uses the private key to generate a public key for the specific transaction. Bob sends his public key to Alice. Alice uses her private key to encrypt the Bitcoin and transaction information, which creates a digital signature and a digest of the information. Digital signatures are like thumbprints or signatures unique to a party that bind a party to a specific transaction. (The transaction information also includes the earlier transactions or blocks associated to the cryptocurrency.) Then Alice uses Bob's public key to encrypt the digest and sends it to Bob. Bob uses his private key to decrypt the digest and authenticate whether the transaction is a valid transaction on the blockchain. If it is valid, nodes on the network confirm the transaction. The transaction would be invalid if Alice altered any of the information about the cryptocurrency, including any of the past transactions, because this would create a different digest. So, when Bob's private key authenticates the transaction, it will see that someone altered the transaction and reject the transaction.

Another way to conceptualize how asymmetric cryptography works is to think about Alice paying for the sandwich by depositing money to Bob in a locked box with an open slit. Bob gives Alice the locked box, but he does not give her the key to the box. Alice deposits the money in the box and a ledger detailing this transaction and past transactions. Then, she gives the box back to Bob. Bob then uses his key to open the box and takes the money and checks the ledger. Bob then cross references his ledger to make sure all the transactions match up. If the ledgers do not match, Bob will know something is wrong with the transaction.

This security protects against fraud and prevents someone from altering or fabricating the blockchain (or ledger). Blockchain, however, is not immutable or tamper proof—it is tamper evident. A "51 percent hack" can alter a blockchain.[48] This occurs when 51 percent of the users or nodes on the network are used to alter a particular chain.[49] First, however, in a public blockchain, it is nearly impossible for this to occur because it would require millions of unknown users to collaborate.[50] Second, in a private blockchain, only authorized users can make changes, so it is possible to identify who made the change. Lastly, if the changes did occur in a blockchain: Whether public or private, the blockchain would reflect a change in the blocks.

iii. Openness

The most important characteristic of blockchain is openness.[51] In a public blockchain every transaction made is visible to all users on the blockchain.[52] Since anyone with an internet connection can join a public blockchain—it is open to the world. In a private blockchain, anyone with permission to view the blockchain can view the transactions.[53] This openness increases transparency, thus increasing accountability.

---

[47] *Id.*
[48] BERRYHILL ET AL., *supra* note 40, at 18.
[49] *Id.*
[50] *See Id.*
[51] MARR., *supra* note 36
[52] BERRYHILL ET AL., *supra* note 40, at 19.
[53] MARR., *supra* note 36.

c. Public v. Private

Public and private blockchains effectively function the same way. The difference lies in who can engage in transactions, as well as who can view and edit the blockchain. In a public blockchain, on one hand, anyone with an internet connection can view, engage in transactions, and edit the blockchain. Moreover, all participants are pseudo-anonymous—each identifiable only by public keys. Public blockchains usually have an incentive system to encourage users to join and validate transactions. The largest public blockchain to date is Bitcoin.

Private blockchains, on the other hand, can be programmed to require permission to edit or view the blockchain and make transactions. Moreover, private blockchains require less energy output to operate, because they do not need mass consensus from a multitude of nodes (computers) to authenticate transactions. Private blockchains may offer the best use for the public sector because they "can greatly enhance accountability, as transactions can be transparent to everyone, while only authorized users are able to actually record new transactions."[54] In a private blockchain, all the users are known. Thus, a private blockchain can serve as an effective and reliable electronic ledger—tracing transactions and the parties conducting them from the inception to the present. Thus, allowing the owner to keep track of their transactions and identify irregularities.

d. Current Uses of Blockchain Technology

Blockchain technology can fundamentally alter how private parties, businesses, institutions, and governments transact. The following sections address some, but not all the current uses of blockchain technology.

i. Cryptocurrency

It is important to make the distinction between blockchain technology and cryptocurrencies like Bitcoin. In its inception, blockchain was a platform used to support the cryptocurrency Bitcoin, which launched in 2009.[55] Other cryptocurrencies soon followed suit, particularly after Bitcoin amassed immense value. Blockchain is to cryptocurrencies, as is the internet is to email—a platform. Cryptocurrencies are a means of conducting peer-to-peer payments without a third-party intermediary, like a bank. Cryptocurrencies, however, are not blockchain's only application.

ii. Smart Contracts

Blockchain technology can revolutionize government functions with smart contracts. Karim Lakhani and Marco Iansiti, professors at Harvard Business School, claim "'[s]mart contracts' may be the most transformative blockchain application at the moment."[56]

Smart contracts are contracts that self-execute once the conditions of the contract are met. Smart contracts retain all the benefits of blockchain technology while also fostering greater efficiency

---

[54] BERRYHILL ET AL., *supra* note 40, at 19.
[55] MARR., *supra* note 36.
[56] Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (2017), https://hbr.org/2017/01/the-truth-about-blockchain (last visited Oct 28, 2018).

by diminishing the processing time associated with the execution of a contract or transaction. Ethereum is the most developed blockchain platform for smart contracts to date.[57]

iii. Tokens

Some blockchain platforms, like Ethereum, allow users to develop tokens that operate on the platform. Tokens vary based on their function. Some tokens function as securities or "digital assets" because they meet the definition of an investment contract under the Howey test.[58] Other tokens are utility tokens. Utility tokens—most commonly ERC-20 tokens—are analogous to arcade tokens.[59] Once someone places an arcade token in a machine, they can use the functions of the machine. Similarly, when someone acquires an ERC-20 token and pays a fee (gas), they can run the decentralized application programmed by the token on Ethereum. Lastly, there are non-fungible tokens (NFTs). NFTs represent a real-world item recorded or tokenized on a blockchain. They are an effective tool for record keeping.

iv. Stablecoins

Stablecoins are cryptocurrencies with a value fixed or pegged to a real-world currency, like the U.S. dollar. As its name suggests, Stablecoins do not fluctuate in value. Some Stablecoins are backed by bonds or other assets. Stablecoins present the solution to the problem Bitcoin cannot solve due its fluctuation in price—engaging in transactions without a bank or other intermediary.[60] Tether is a Stablecoin operated by Bitfinex that is pegged to dollar U.S. dollar, backed by large amounts of commercial paper, and maintains the largest market capitalization of all Stablecoins.[61] And Dai is a fascinating Stablecoin pegged to the U.S. dollar but is completely decentralized, collateralized by various cryptocurrencies, and is issued by one of the earliest decentralized applications (dapps) on the Ethereum blockchain—MakerDAO.[62] Dai presents a conundrum to regulators: how do you regulate a decentralized autonomous organization?

v. Decentralized Finance (DeFi)

Decentralized finance ("DeFi") displaces traditional finance and banking by maintaining a decentralized financial market accessible to anyone with an internet connection. According to the World Bank: "Globally, 1.7 billion adults remain unbanked, yet two-thirds of them own a mobile phone that could help them access financial services."[63] DeFi presents an opportunity to provide liquidity to those out of reach of the traditional financial systems due to systemic inequities or faulty

---

[57] BERRYHILL ET AL., *supra* note 40, at 19.

[58] *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. Securities and Exchange Commission, Apr. 3, 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[59] *See generally ERC-20: The Definitive Ethereum Token Standard*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/erc20-token-standard-ethereum, May 17, 2021.

[60] *See generally* Christian Catalini and Jai Massari, *Stablecoins and the Future of Money*, HARV. BUS. REV., Aug. 10, 2021, https://hbr.org/2021/08/Stablecoins-and-the-future-of-money.

[61] *Why regulators should treat Stablecoins like banks*, THE ECONOMIST, Aug. 7, 2021, https://www.economist.com/leaders/2021/08/07/why-regulators-should-treat-Stablecoins-like-banks.

[62] *How MakerDAO Pioneered Decentralized Finance*, CRYPTOPEDIA, March 12, 2021, https://www.gemini.com/cryptopedia/makerdao-defi-mkr-dai-coins.

[63] *Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows*, WORLD BANK, Apr. 19, 2018, https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows.

credit underwriting processes. Under various DeFi protocols, users can transfer funds, provide loans, receive loans, invest, swap tokens, and more.[64]

IV. How Governments Should Utilize Blockchain

Blockchain initially gained prominence through the financial sector because of cryptocurrencies.[65] But blockchain is now spreading through the public sector. In fact, "at least 46 countries around the world have launched or are in the planning stages to launch over 200 [b]lockchain-related initiatives."[66] For example, Dubai partnered with IBM to develop the world's first government-backed blockchain platform.[67] Sheikh Hamdan Bin Mohammed Al Maktoum wants Dubai's entire government to operate on blockchain.[68] The first areas where Dubai will implement blockchain are in health records, securing the diamond trade, title transfers, business registration, digital wills, tourism engagement, and improved shipping.[69] In addition, American agencies are also seeking to implement blockchain to enhance various operations—particularly in procurement.[70] In a speech at the Blockchain Forum on October 10, 2017, Deputy Secretary of State, John J. Sullivan stated,

> "Blockchain has the potential to become a transformative technology of our lifetime. . . and is expected to play a major role in trade, business, healthcare management, and finance, and we hope at the State Department as well. . . . [S]peaking on behalf of the U.S. Government, we want to educate ourselves about how we can better leverage Blockchain technology. . . . [W]e're excited about the many ways Blockchain technology could also increase transparency and accountability here at the State Department and across the federal government."[71]

The following sections present opportunities for governments to digitize their functions utilizing blockchain.

a. Procurement

Public procurement or government contracting refers to the process of acquiring goods and services from private parties by a government agency [72]In other words, public procurement occurs when governments acts as a consumer.[73] Procurement is the life blood of developed nations. In fact, the 35 members of the Organization for Economic Co-operation and Development ("OECD") spend nearly 12 percent of their GDP on public procurement.[74]

---

64 Alyssa Hertig, *What is DeFi?*, CoinDesk, Sep. 18, 2020, https://www.coindesk.com/tech/2020/09/18/what-is-defi/.
65 BERRYHILL ET AL., *supra* note 40, at 20.
66 *Id.*
67 Alkesh Sharma, *From 45 days to seconds: Smart Dubai, IBM introduce Middle East's first government-backed blockchain platform*, THE NATIONAL, Oct. 31 2018.
68 Saqr Ereiqat, *Blockchain in Dubai: Smart cities from concept to reality*, BLOCKCHAIN UNLEASHED: IBM BLOCKCHAIN BLOG, Apr. 10, 2017.
69 Pete Rizzo, *Dubai's Global Blockchain Council Unveils First Pilot Projects*, COINDESK, May 30, 2016.
70 *See generally*, Selva Ozelli, *US Government Implements Blockchain Programs to Improve Transparency and Efficiency*, COINTELEGRAPH, Jan. 23, 2018; HOUSE SCIENCE, SPACE, AND TECHNOLOGY SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY AND OVERSIGHT HEARING, (2018).
71 JOHN J. SULLIVAN, *Remarks at the Blockchain Forum*, http://www.state.gov/s/d/17/274725.htm (last visited Nov 20, 2018).
72 *Public procurement*, OECD, http://www.oecd.org/gov/public-procurement/ (last visited Jan 21, 2019).
73 Procurement, however, can sometimes embody the sale of government assets by a government.
74 74 Public procurement - OECD, *supra* note 73..

Procurement has such a large impact on the United States that during the government shutdown in 2018–19: The United States lost $200 million a day and its economic growth reduced by 0.13 percent every week the shutdown lasted.[75] And during the shutdown, more than 1 million government contractors were furloughed.[76] Since procurement is such a crucial component of a nation, the OECD states that governments are expected to carry out public procurement "efficiently and with high standards of conduct in order to ensure high quality of service delivery and safeguard the public interest."[77] This means that good procurement requires efficiency, transparency, and integrity, which blockchain can help promote. The best use for blockchain technology in procurement is through a private blockchain that allows the public to view but not edit the blockchain.

The following sections will address how blockchain technology can enhance procurement supply chain transparency and traceability. And how it can improve the contract awarding process.

i. <u>Supply Chain Transparency/Traceability[78]</u>

Utilizing blockchain technology in procurement will enhance the supply chain traceability and transparency of transactions between a government and private contractors, as governments can track goods and transactions from their origin.[79] One example of this in the private sector is Walmart: the store used blockchain technology to locate the source of romaine lettuce that caused an E. coli outbreak in the United States.[80] There are many steps in the supply chain that make it hard to track down one food item.[81] It usually takes at least seven days to find a contaminated food item—but with a blockchain system, it took as little as 2.2 seconds to find the source of the contamination.[82]

The enhanced traceability that blockchain technology brings surely can serve any government well—so can the added transparency. Since all transactions are permanently logged on the blockchain, the government and the public—depending on the setup of the blockchain—can trace exactly which parties were awarded contracts, what good or services the contracts were awarded for, and the amount of money awarded for the contracts. This increased transparency can lead to increased bid protests, which serves as another method of procurement accountability. As disappointed bidders have more clear and public information regarding the awarded contract, this clarifies and speeds up the bid protest process.

ii. <u>Improve Contract Award Process</u>

Information is powerful, particularly information that is easily and readily available. With more readily accessible information, governments can ensure they are engaging in transactions with responsible parties, particularly in countries like the United States, where the responsibility of the contractor is a factor considered in awarding a contract. The United States federal government has a database called the Federal Awardee Performance and Integrity Information System ("FAPIIS") that holds data like "contract terminations, past performance, responsibility determinations, administrative

---

[75] Ari Natter, *Government Contractors to Lose Out on Shutdown Pay, Dragging Down Economy*, BLOOMBERG, Jan. 17, 2019.
[76] *Id.*
[77] Public procurement - OECD, *supra* note 73.
[78] A natural byproduct of enhanced transparency and traceability in a procurement system is enhanced integrity.
[79] BERRYHILL, ET AL., *supra* note 40.
[80] Matt Smith, *In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens*, WALMART https://news.walmart.com/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens (last visited Jan 19, 2019).
[81] *Id.*
[82] *Id.*

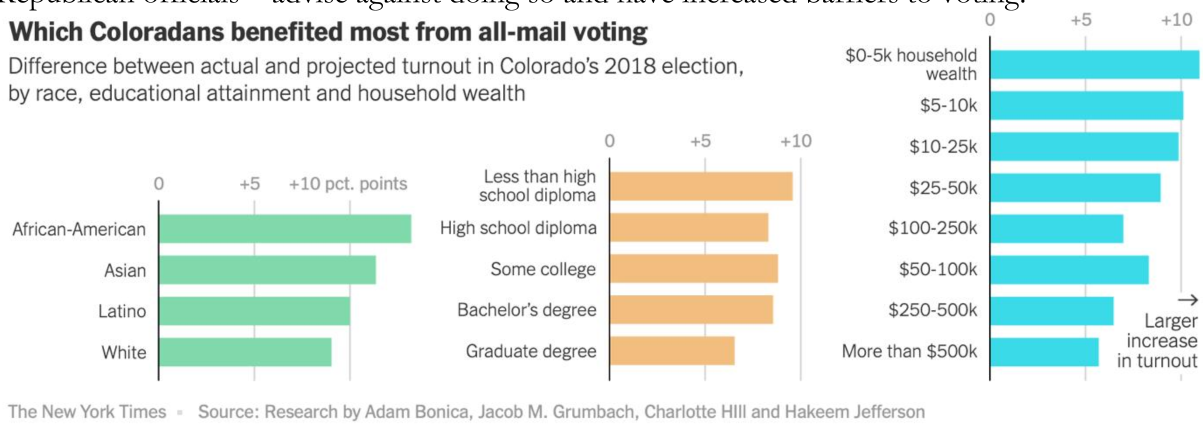
agreements, or criminal, civil, or administration actions involving the contractor."[83] Governments can incorporate the data on databases like the FAPIIS into a blockchain so the government and the public will have everything they need to know about a contractor. Faster responsibility determinations lead to faster contract awards. This also will increase efficiency, another important goal of good procurement.

The General Services Administration ("GSA")—a United States agency that oversees the management and operation of other government agencies—believes blockchain technology can shorten the time frame for its contract award process.[84] Smart contracts can drastically shorten the contracting process—allowing governments to engage in more contracts. Governments can configure the terms of a smart contract to automatically execute once the good or service is received in accordance with the specifications. The enhanced efficiency created will also save governments a tremendous amount of money, because it will cut down transaction costs. In sum, blockchain technology can lead to a more efficient and cost-effective procurement process.

The U.S. Department of Health and Human Services ("HHS") has launched Accelerate, a system to manage contracts and billing, utilizing blockchain, artificial intelligence, machine learning, and process automation.[85] This is one of the first federal blockchain applications and it has saved HHS over $720M.[86]

b. Voting

Voting for representatives are the foundations of any democracy. The coronavirus pandemic forced democracies around the world to contend with conducting voting from a distance. In America, state governments are grappling with whether to increase voting by mail, but some officials—mainly Republican officials—advise against doing so and have increased barriers to voting.[87]



A study done on voter information in Colorado (where ballots are mailed to all registered voters) shows mail ballots increased voter turnout for all groups—reducing inequities in voter

[83] Jessica Tillipman, *THE FOREIGN CORRUPT PRACTICES ACT & GOVERNMENT CONTRACTORS: COMPLIANCE TRENDS & COLLATERAL CONSEQUENCES*, BRIEFING PAPERS 25 (2011).
[84] Joe Kim, *Blockchain: A Path to Unblocking Government Procurement Processes*, THE AMERICAN CITY & COUNTY; PITTSFIELD (2018).
[85] Clavin, Erickson, Li, et al., *Blockchains for Gov. Use Cases and Challenges*, 1 DIG. GOV.: RES. AND PRACT. 3, Article 22, 8-9 (Nov. 2020), https://dl.acm.org/doi/pdf/10.1145/3427097.
[86] *Id.* at 10.
[87] *See* Charlotte Hill et al., *We Should Never Have to Vote in Person Again*, NEW YORK TIMES, May 4, 2020, https://www.nytimes.com/2020/05/04/opinion/coronavirus-vote-by-mail.html.

representation.[88] Increasing the number of potential voters is ideal for democracy.[89] So, if nations want to increase democratic representation, they should pursue methods for casting votes that achieve just that. The study from Colorado demonstrates mail ballots provides an opportunity to do just that.

Although "fraud is exceptionally rare, hard to commit without getting caught and nearly impossible to do on the scale necessary to affect [American] election results,"[90] mail ballots are admittedly susceptible to at least some degree of fraud. And because mail voting leaves behind a paper trail—which election officials can audit to verify that votes were counted as cast—it may actually be even more secure than in-person voting."[91] But for some, the risk of fraud (regardless of how minimal) is too large for comfort. This risk is heightened in emerging democracies were voter fraud already runs rampant.

Blockchain voting can create the same benefits of voting by mail but with decreased risks of fraud. In fact, West Virginia, Utah and the City of Denver have all utilized a blockchain voting application in elections.[92]Blockchain voting works like the transaction between Alice and Bob described above.[93] But instead of Alice giving Bob money, Alice gives Bob her vote. Let us imagine Alice is a voter and Bob is a state clerk. Prior to the election, Alice registers to vote with the clerk's office. Alice gives the clerk's office personal identifiable information (PII) that confirms she is eligible to vote. This then creates an ID for Alice that is not attached to her PII, which will allow her to vote on election day. On election day: Bob gives Alice a secured box, and Alice places her vote and ID into the secured box. Alice sends the box back to Bob. Bob unlocks the box and checks to see if the ID is a valid voter ID, which has not cast a ballot, and if it is valid—he records the vote. This process occurs through a mobile application or on a government website.

Like mail in ballots, blockchain voting would leave an electronic trail of votes that election officials can audit. The one concern, though, is the vulnerability of the devices individuals use to cast their votes and security of the server that holds the voting data. For example, in principle someone could hack a voter's phone and access it remotely. But a government could configure the system to require biometric recognition (face id or finger print) to proceed on the application. Also, the wide scale cyberwarfare required to hack enough phones to disrupt an election would indicate a larger issue requiring government intervention. If the servers were attacked, the hackers could not change the votes because they are encrypted and would not have permission to make changes on the blockchain. If, however, they were able to hack a user that had permission to edit the blockchain, any changes would be recoded on the blockchain and revealed by an audit.

c. Taxation

Since early civilization, governments struggle with decreasing the gap between taxes owed and taxes collected—the "tax gap." Each year, governments lose billions of dollars in potential revenue because many individuals and business fail to file and pay taxes. In fact, from 2011 to 2013, the Internal Revenue Service estimates the tax gap was $441 billion *per* year.[94] The taxation process requires

---

[88] *Id.*

[89] *But see* Aaron Blake, *Trump just comes out and says it: The GOP is hurt when it's easier to vote*, WASHINGTON POST, March 30, 2020.

[90] HILL ET AL., *supra* note 88

[91] *Id.*.

[92] Daniel Palmer, *Utah County to Offer Blockchain Voting App in Municipal Elections*, COINDESK, July 23, 2019, https://www.coindesk.com/markets/2019/07/23/utah-county-to-offer-blockchain-voting-app-in-municipal-elections/.

[93] *See supra* Section IIb.

[94] *The Tax Gap*, IRS.GOV, Oct. 21, 2020, https://www.irs.gov/newsroom/the-tax-gap.

authenticating records from businesses and personal records from individuals, which itself bears a significant administrative cost. Blockchain technology can automate the tax collecting process, allowing tax administrators to collect financial information from businesses and individuals in real time as transactions are made, authenticate financial data quicker, reduce paperwork, and increase the speed that refunds are distributed, using smart contracts.[95] This can also free up resources, allowing tax collectors to increase their enforcement and scrutiny of individuals that attempt dodge their tax bill. The newly recovered funds can then go government programs that need it the most—like social welfare.

d. Records & Data Management

Governments store and issue records: deeds, marriage licenses, driving records, health records, financial records, birth records, death records, corporate records, permits, etc. Many records are physical documents located at specific agencies. By using smart contracts and tokens on a blockchain platform, records management processes can be revolutionized. Governments can facilitate instant recordation of deeds and titles. For example, residents can purchase real property, logging the transaction on a blockchain platform in real-time by tokenizing it, creating a chain of title that allows a third party to easily authenticate and ascertain chain of title. There are several countries across the developing world seeking to update land registries through tokenization.[96]

The biggest problem when it comes to disputes regarding real property or secured transactions is figuring out which party had the best claim to the property or asset. Recording is the process that gives notice to prevent disputes. But this process can be more efficient and transparent if the transactions are automatically recorded, instead of requiring parties to record at the agency. When it comes to other records, digitizing the process on a blockchain platform can allow citizens easier access to their records without worrying about losing physical documents. Similar to its use Estonia, a centralized collection of records will further enable governments to share information and understand who is who, from parent companies and subsidiaries to parents and children.

Managing health care data with blockchain technology is an area with increased interest over the past decade.[97] The U.S. Center for Disease Control and Prevention ("CDC") is researching using blockchain technology to track public outbreaks of hepatitis A, and with IBM, began constructing a blockchain platform to track the opioid epidemic.[98] Imagine these very applications implemented to respond to the COVID-19 pandemic. For example, tracking cases and instead of requiring individuals to carry around physical vaccine cards, it was instead logged on a blockchain platform allowing for easier verification.

---

[95] *See generally*, Kuralay Baisalbayeva, Eelco van der Enden, Valentina Ion et al., *Blockchain for tax compliance*, PwC/Microsoft/Vertex, https://clouddamcdnprodep.azureedge.net/gdc/gdcDQxrqP/original (2019).
[96] Georg Eder, *Digital Transformation: Blockchain and Land Titles*, 2019 OECD Global Anti-Corruption & Integrity Forum, Mar. 2019, https://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf.
[97] Clavin et al., at 11.
[98] *Id.* at 9.

e. Distributing Aid & Benefits

On September 16, 2020, the Director of D.C Department of Employment Services (the "Department") testified before Committee on Labor and Workforce Development that the current unemployment compensation systems requires technological improvements. The District, like other U.S. states, experienced a rapid increase in unemployment claims, which overwhelmed the Department and its operations. This is another government function that can be made more efficient utilizing a blockchain platform and smart contracts that can authenticate the benefit requestors and automatically issue benefits when the conditions for the benefits are met. This same concept is applicable to the disbursement of foreign aid. Governments could automatically condition foreign aid to governments or entities on various conditions and increase oversight on how funds are utilized.

f. Central Bank Digital Currencies (CBDCs)

Central bank digital currencies ("CBDCs") are effectively a Stablecoin issued by a state's central bank, like the U.S. Federal Reserve, which is a digital representation of the nation's fiat currency—backed by the full-faith of the government.[99] Over 81 countries, representing 90 percent of global GPD are considering CBDCs, with 5 countries already launching their own currencies—including China.[100] To fully optimize the use-cases listed above, a government could launch a blockchain platform with a CBDC as its native currency or token, which would be used to fully integrate payments and transactions on its blockchain. Launching a CBDC, however, presents a host of complications from privacy concerns to adequate control of monetary policy.[101] But there are also concerns for a country like the United States in not issuing a CBDC. The hard and soft power of the U.S. in large rests on the hegemony of the U.S. dollar. About 85 percent of all foreign exchange transactions, 61 percent of foreign exchange reserves, and 40 percent of international payments are in U.S. dollars. [102] The world is dependent on the U.S. dollar, but digital currencies, particularly CBDCs backed by a government present the opportunity for the world to wean itself from the U.S. dollar with a currency easier to transact and free from the heavy-hand of a U.S. sanctioning regime.

---

[99] *See generally Central Bank Digital Currencies*, BANK FOR INT'L. SETTLEMENTS, Mar. 2018, https://www.bis.org/cpmi/publ/d174.pdf.

[100] Central Bank Digital Currency Tracker, ATLANTIC COUNCIL, https://www.atlanticcouncil.org/cbdctracker/ (last visited Sept. 22, 2021).

[101] *Id.*

[102] *US dollar funding: an international perspective*, Bank of Int'l Settlements, CGFC Papers No. 65, at 3, June 2020, https://www.bis.org/publ/cgfs65.pdf.

V. Concerns

a. When the Private Sector Attempts Preempting the Public Sector: Libra, a Case Study

i. Background

History has dictated the path forward for fintechs. To understand the point of inflection for the United States' and the regulatory structure for Stablecoins and the like, it starts with Facebook. Facebook made all the mistakes and industry stakeholders learned how to introduce tech to congress in a productive way. For the first-time ever, the sections below provide background and overview as to how it all transpired and the gates of fintech opened up.

In 2019, the House Financial Services Committee ("HSFC") held two hearing's on Facebook's efforts to create a Stablecoin, Libra (now branded as Diem, Latin for "day" and without direct Facebook control)[103] and a digital wallet, Calibra (now branded as Novi, "a portmanteau of the Latin root words, "novus" meaning new and "via" meaning way")[104]. The Committee characterized Libra as an alternative to the U.S. dollar and viewed Calibra akin to a bank account. In June 2019, Facebook released a seven-page white paper on the Libra project without consulting Congress, key federal and state regulators, foreign regulatory bodies, or other relevant stakeholders. Facebook planned for the Libra Association ("Association") and its 27 other members to serve as an independent, not-for-profit organization headquartered in Geneva, Switzerland. And unlike most other Stablecoins built on blockchain technologies,[105] the Libra Association would be permissioned, whereby only members can validate transactions.

Shortly after Facebook's Libra plans were announced, Chairwoman Waters (D-CA), along with other members, wrote a letter to Facebook and called on it to agree to place a moratorium on any further development of Libra and Calibra until regulators and Congress had sufficient opportunity to review these products.[106]

ii. The Initial Hearing

The first hearing on July 17, 2019, entitled, "Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System" and convened two-panels: the first with David Marcus, CEO of Calibra and the second with leading monetary policy, systemic risk, and securities law experts. Committee members found the balance sheet size and management style of Facebook embarking on a monetary project of this magnitude alarming, considering the company's past failures. Facebook has more than 2.7 billion monthly active users—more customers than JP Morgan Chase, Wells Fargo, Citibank, and Bank of America combined.[107]

---

103 See Nikhilesh De, *Libra Rebrands to "Diem" in Anticipation of 2021 Launch*, COINDESK, Dec. 1, 2020, https://www.coindesk.com/libra-diem-rebrand.

104 *See* Sebastian Sinclair, *Facebook's Calibra Rebrands to Novi, Details Wallet Tie-Up With WhatsApp*, COINDESK, May 26, 2020, https://www.coindesk.com/libra-facebook-blockchain-digital-wallet-novi-calibra.

105 Christine Kim, *New Libra Fork Will Create Permissionless Stablecoin Free of Corporate Control,* COINDESK Oct. 11, 2019, https://www.coindesk.com/new-libra-fork-will-create-permissionless-stablecoin-free-of-corporate-control.

106 *See* House Committee on Financial Services, *Committee Democrats Call on Facebook to Halt Cryptocurrency Plans* July 2, 2019, https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=404009.

107 Peter Rudegeair, *Venmo Has 40 Million Users, Outnumbering Most Big Banks*, WALLSTREET JOURNAL, Apr. 24, 2019, https://www.wsj.com/articles/venmo-has-40-million-users-outnumbering-most-big-banks-11556142906.

Cryptocurrency exchanges, including those that list Stablecoins,[108] are also frequently targeted by cyberattacks and data breaches.[109] To facilitate its cryptocurrency transactions, Facebook intended to manage and hold a detailed digital repository of social (Facebook and Instagram posts), financial (purchases and spending habits), and governmental data (name, address, and driver's license number), which may further increase their hacking risks. Facebook has had issues with safeguarding its users' information in the past. For example, Cambridge Analytica, a political consulting firm had access to more than 50 million Facebook users' private data which it used to influence voting behavior.[110]

iii. Domestic and Foreign Regulatory Concerns

U.S. regulators and financial leaders raised concerns with Libra. According to Federal Reserve Board Chairman Jerome Powell, "Libra raises many serious concerns regarding privacy, money laundering, consumer protection, and financial stability."[111] Chairman Powell stated that the project "cannot go forward" without addressing those concerns. Likewise, Federal Reserve Board Governor Lael Brainard stated that "there are likely to be financial stability risks for a Stablecoin network with global reach. If not managed effectively, liquidity, credit, market, or operational risks—alone or in combination—could trigger a loss of confidence and a classic run."[112] Governor Brainard also noted, "[t]he potential for risks and spillovers could be amplified by potential ambiguity surrounding the ability of official authorities to provide oversight and backstop liquidity and to collaborate across borders."[113]

Concerns mounted from overseas. After the Committee's July hearing, international regulators also expressed analogous concerns surrounding Facebook's plans with Libra and Calibra. In August, regulators from France and Germany both agreed to block Libra from their countries; in a joint statement, the two governments stated that "no private company can claim monetary power, which is inherent to the sovereignty of nations." The G-7 and the Financial Stability Board ("FSB") called for more scrutiny and higher regulatory standards for Stablecoins, such as Libra, particularly to protect consumers and ensure cryptocurrencies are not used to launder money or fund terrorism.[114] On October, 23, 2019, the Committee convened another hearing with Facebook's CEO, Mark Zuckerberg. Notably, seven of the original Libra Association signatories abandoned the project days before the hearing.[115] The Committee invited Zuckerberg to explain, how he intended to provide a sound financial product while Facebook failed protecting user trust on the company's platform. In an analysis of Facebook's efforts, Chairwoman Waters (D-CA) stated, "I've come to the conclusion that

---

108 *See* Sebastian Sinclair, *Tether Froze $300K of Stablecoin Hacked After Victims Left Wallet Keys in Evernote*, COINDESK, Dec. 9, 2020, https://www.coindesk.com/tether-froze-300k-of-stablecoin-hacked-after-victims-left-wallet-keys-in-evernote.

109 *See also* Brian Barrett, *Hack Brief: Hackers Stole $40 million from Finance Cryptocurrency Exchange*, WIRED, May 8, 2019, https://www.wired.com/story/hack-binance-cryptocurrency-exchange/.

110 Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES, Mar. 19, 2018, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

111 Pete Schroeder and Trevor Hunnicutt, *4-Fed chief calls for Facebook to halt Libra project until concerns addressed*, CNBC (July 10, 2019).

112 Lael Brainard, *Digital Currencies, Stablecoins, and the Evolving Payments Landscape*, FED. RESERVE BOARD, Oct. 16, 2019, https://www.federalreserve.gov/newsevents/speech/brainard20191016a.htm.

113 *Id.*

114 *See* Szu Ping Chan, *Facebook's digital currency dealt another blow*, BBC NEWS, Oct. 14, 2019, https://www.bbc.com/news/business-50037223.

115 Lauren Feiner, *Facebook-led Libra project announces its 21-member council after exodus of top payments companies*, CNBC, Oct. 14, 2019, https://www.cnbc.com/2019/10/14/facebook-forms-its-cryptocurrency-council-after-key-backers-drop-out.html.

it would be beneficial for all if Facebook concentrates on addressing its many existing deficiencies and failures before proceeding any further on the Libra project."[116] Since the hearings, other stakeholders have raised a wide range of policy concerns about this project.[117] Ultimately, under the spotlight of the Committee, Facebook drastically scaled back the timeline for the Libra project, then, created more separation between the entities (staff moved to Switzerland and received "libra" domains for email address instead of "Facebook,") and started hiring anti-money laundering and veteran banking experts to help further build out the project.[118]

iv. An Unclear Regulatory Framework

Presently, it remains unclear which federal agency is leading the national discussion surrounding cryptocurrencies and digital representations of value. Former Acting Comptroller Brooks, through an interpretive letter, permitted federally charted banks and thrifts to provide custody services for cryptocurrency assets.[119] Considering the revenue generated from custody fees, institutional players are likely to benefit greatly from this interpretation. All the while, Treasury had (and still has) not provided clarity on banks taking custody of cryptocurrency assets and technically, prior to this action by Acting Comptroller Brooks, "banks were never prohibited to custody crypto assets, and there was never any transparency on the risks that might entail."[120] Prior to these actions, in late 2018, to better understand and assess the challenges posed by cryptocurrencies and digital representations of value, the Financial Stability Oversight Council ("FSOC") formed a Working Group on Digital Assets (which includes the OCC), concluding that cryptocurrencies pose risks to financial stability. Examples include how cryptocurrencies interact both directly and indirectly with banking services, financial markets, and financial intermediaries; risks to consumers, investors, and businesses associated with potential losses or instability in market prices; illicit financing risks; risks to national security; cybersecurity and privacy risks; and risks to international monetary and payment system integrity.[121]

---

116 House Committee on Financial Services, *An Examination of Facebook and Its Impact on the Financial Services and Housing Sectors* (Oct. 23, 2019), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=404487.

117 *See Banking on Surveillance: The Libra Black Paper*, Americans for Financial Reform Education Fund and Demand Progress Education Fund, June 25, 2020, https://ourfinancialsecurity.org/2020/06/fact-sheet-banking-on-surveillance-the-libra-black-paper/.

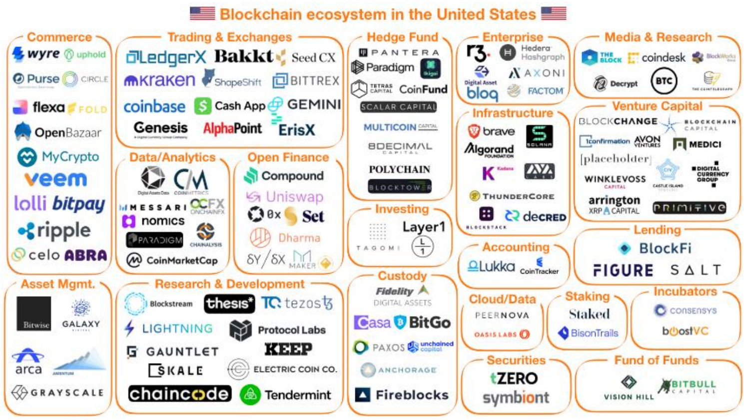
118 Alisha Roy, *Libra Association Appoints Former HSBC Exec to Move Their Project Forward*, AMBCRYPTO, Oct. 15, 2020, https://eng.ambcrypto.com/libra-association-appoints-former-hsbc-exec-to-move-their-project-forward/.

119 Office of the Comptroller of the Currency, *Federally Chartered Banks and Thrifts May Provide Custody Services For Crypto Assets* (July 22, 2020), https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html.

120 Anirudh Tiwari, *US Banks Get Crypto Custody Nod, but Instant Demand Surge Is Unlikely*, COINTELEGRAPH, July 30, 2020.

121 Dept. of Treasury, *Readout of Financial Stability Oversight Council Meeting* (Dec. 19, 2018), https://home.treasury.gov/system/files/261/December192018_readout.pdf.

US Blockchain Ecosystem Using Traditional Financial Services Terminology[122]



v. Current Oversight

Title X of the Dodd-Frank Act grants the CFPB certain rulemaking, supervisory, and enforcement authorities to implement and enforce certain laws that protect consumers from "unfair, deceptive, or abusive acts and practices."[123] These authorities apply to a broad range of financial industries and products and could apply to cryptocurrency exchanges. Although the CFPB has not exercised regulatory authority regarding the cryptocurrency industry, it is accepting cryptocurrency related complaints and has indicated it would enforce consumer financial laws in appropriate cases. In addition, the Federal Trade Commission ("FTC") has brought several enforcement actions against cryptocurrency promoters and mining operations due to potential violations of the Federal Trade Commission Act.[124] Further, all states have various laws against deceptive acts and practices, and state regulators can use their enforcement authorities against cryptocurrency-related businesses.[125]

While the federal government assesses the licensing of cryptocurrency and digital representations, the states are providing regulatory frameworks for companies to launch. In October 2020, the New York State Department of Financial Services ("NYDFS") granted Paypal (which maintains payment operations for 26 million merchants and is the parent company of Venmo, peer-to-peer electronic payment application) a conditional "Bitlicense,"[126] for a service that enables users to buy, hold, and sell cryptocurrency. In addition, Wyoming has recently approved a special purpose depository institution charter to crypto businesses, Kraken Financial and Avanti Bank & Trust, though these approvals have raised concerns from other stakeholders about the effectiveness of these

---

[122] Blockchain Association, *About Us*, https://theblockchainassociation.org/ (last visited Dec. 4, 2020).
[123] Consumer Financial Protection Bureau, *Unfair, Deceptive, or Abusive Acts or Practices* (Oct. 2012), https://files.consumerfinance.gov/f/documents/102012_cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures.pdf.
[124] Federal Trade Commission, *FTC Sends Refunds to Victims of Deceptive Money-Making Schemes Involving Cryptocurrencies* (Nov. 4, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-sends-refunds-victims-deceptive-money-making-schemes/
[125] Congressional Research Service, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, Apr. 9, 2020, https://www.crs.gov/Reports/R45427.
[126] New York Department of Financial Services, *Virtual Currency, BitLicense FAQs*, https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs (last accessed at Nov. 6, 2020).

regulatory frameworks.[127] Quick Fixes: The SEC, in consultation with the Fed for monetary policy concerns, should issue clear guidelines on Stablecoins, cryptocurrencies, and other digital representations of value, particularly ones pegged to the US dollar. FSOC should use its authority to designate any new global payment system based on a cryptocurrency or stable coin, such as Libra, that poses a threat to U.S. financial stability as either a systemically important financial institution ("SIFI") or systemically important financial market utilities ("SIFMU") and subject it to enhanced oversight.[128] But even this presents a fundamental problem: How do you regulate a decentralized autonomous organization?

b. Data Privacy & Security

As noted above in Section II, one of the hallmarks of blockchain technology is the asymmetric cryptography that encrypts the information within the blockchain. The technology is inherently secure. The issue, however, is the humans who manage the technology. If governments decide pursuing blockchain digitization, they should establish laws similar to Estonia, making it illegal to unlawfully access information (there are already federal laws to this effect)[129] Governments also need cyber security officers, which conduct security audits and ensure integrity within the infrastructure. With the increase of cyber-attacks on state and local governments,[130] increased cyber-security is a necessary component of government operations.

But most importantly, as government increase its use of technology in government, it ***must*** address ways to improve the general data-privacy protection it offers its citizens from third parties as well as the government. Data, today, is the new oil.[131]

The vast amounts of consumer information and data collected and stored by financial institutions, data aggregators, and cloud providers, among others, is commonly referred to as "big data." The "big" in big data refers to the size, complexity, and newness of any given data set. Big data is integral to modern product development because it can be used to generate insights, support decision making, and enable automation for massive growing data sets. Innovation in this sector has grown, and today, because of the internet and ability to synthesize big data quickly into rapidly applied conclusions, it is easier and less expensive for companies to collect, store, process, and sell consumer data—regardless of the data's size, type, or location.[132] In fact, this development of new products and services is largely driven by data aggregators,[133] partly because of their ability to capitalize on huge

---

127 *See, e.g.,* Bank Policy Institute, *Beware the Kraken*, https://bpi.com/beware-the-kraken/ (Oct. 21, 2020); *and also*, Bank Policy Institute, *Why a Wyoming Charter Is No Hail Mary for the Anti-Fractional Banking Team*, https://www.bpi.com/why-a-wyoming-charter-is-no-hail-mary-for-the-anti-fractional-banking-team/ (Nov. 9, 2020).

128 *See, e.g.,* Americans for Financial Reform Education Fund and Demand Progress Education Fund, *Banking on Surveillance: The Libra Black Paper* (June 25, 2020), https://ourfinancialsecurity.org/2020/06/news-release-afr-education-fund-and-demand-progress-ef-reject-recent-changes-to-the-libra-associations-white-paper-as-insufficient/.

129 18 U.S. Code § 1030

130 Todd G. Vare, *State and Local Governments Continue To Be Favorite Targets of Cyberattacks*, NAT'L LAW REV., https://www.natlawreview.com/article/state-and-local-governments-continue-to-be-favorite-targets-cyberattacks (Sept. 19, 2019).

131 *The world's most valuable resource is no longer oil, but data*, ECONOMIST, May 6, 2017.

132 Department of Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, 22-39 (July 2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

133 *See,* Consumer Financial Protection Bureau, *Request for Information Regarding Consumer Access to Financial Records*, 81 *Federal Register* 83808 (Nov. 22, 2016), https://www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records; *See also*, Consumer Financial Protection Bureau, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform The Consumer Protection Principles*

caches of data from diverse sources on the internet, compiling it into a standardized and summarized form for sale to investors and other entities.[134] These practices and others, such as webscraping and permissioned credentialing, are subject to an unclear legal framework, especially when compared to more traditional financial institutions, and raises several questions related to the existing privacy protections.

As the use of consumer data has grown, many countries implemented robust legal frameworks that grant consumers more data-use rights and protections. For example, in 2018, the European Union implemented the General Data Protection Regulation ("GDPR"), which regulates the collection, use, storage, and disclosure of personal data, and any other information through which an individual can be directly or indirectly identified.[135] In the same year, California enacted the California Consumer Privacy Act ("CCPA"), which establishes three consumer rights: (1) a "right to know" the information that businesses have collected or sold about them; (2) a "right to opt out" of the sale of a consumer's information; and (3) a "right to delete" any information a company has collected about the consumer, with some exceptions. In November 2020, California also passed Proposition 24, also known as the Consumer Privacy Rights Act ("CCPA"), to further restrict the sale of data and to create a new enforcement agency.[136]

Before increasing citizens' digital footprints, regulators must increase and modernize data privacy and consumer protections. For example, Congress should pass the "Financial Information Data Modernization Act ("FIDMA"),"[137] a proposal that would set forth minimum data security standards by clarifying "financial data" and "non-financial institutions" under GLBA to protect consumers and provide guidance that contemplates advances in technology for entities interacting with financial data. The CFPB and the FTC should explore ways to clarify enforcement authority under GLBA to better use the law to provide substantive protections for citizens. In all, firms are making decisions that affect the livelihoods of citizens with little oversight. If a government pursue the benefits of blockchain digitization, it should also seek to protect citizens and their data as well. If not, they may establish a digital democracy rooted in surveillance from both the public and private sector.

c. Job Losses Due to Automation

A foreseeable consequence of automation is job loss. If a government adopts blockchain technology, some jobs may become redundant and therefore eradicated. A mitigation strategy, therefore is necessary to contain the economic fallout. For example, a government can pursue workforce development initiatives—especially jobs resistant to forces driving automation. These jobs will find increased demand in our new digital society.

(Oct 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[134] Steven Melendez and Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, Fast Company (Mar. 2, 2019); *See also*, Lauren Saunders, *Fintech and Consumer Protection: A Snapshot*, NAT'L CONSUMER LAW CENTER, Mar. 2, 2019, https://www.nclc.org/images/pdf/cons-protection/rpt-fintech-and-consumer-protection-a-snapshot-march2019.pdf.

[135] Congressional Research Services, *Data Protection Law: An Overview* (Mar. 25, 2019), https://crsreports.congress.gov/product/pdf/R/R45631.

[136] Marketplace, *California's new privacy law could create haves and have-nots* (Nov. 6, 2020), https://www.marketplace.org/shows/marketplace-tech/california-proposition-24-consumer-privacy-rights-act-sharing-data-with-companies-inequality/.

[137] H.R.__, Safeguarding Non-bank Consumer Information Act (Discussion Draft), Cong. 116th (2019), https://financialservices.house.gov/uploadedfiles/bills-116pih-fidma.pdf.

Another growing trend in the U.S. is a gap between available jobs and qualified workers. In 2016, for example, nearly 46% of U.S. employers struggled filling jobs, citing alack of available talent.[138] The majority (roughly 53%) of the jobs in the U.S. labor market are middle-skill jobs that require more education than a high school diploma but less than a four-year degree.[139] To address this skill gap and create jobs: a pipeline program should be created, geared towards students who do not desire attending a four-year college but seek gainful employment. The pipeline should begin with students (and potentially an alternative program for high school dropouts and returning citizens pursuing a GED) gaining skills by taking career technical education ("CTE") courses and acquiring certifications.

Once students near the end of the pipeline, they will possess the skills, experience, and connections to work full-time at their site. Or at a partnering entity. In the end: the locality will develop a more skilled workforce and create a pathway to gainful employment for students immediately upon graduation.

VI. Conclusion

For governments, Bitcoin is a distraction. But the technology that underpins it presents opportunities that exceed simple financial transactions. This technology can make government operations more efficient, reducing operating costs, while improving transparency and the satisfaction of citizens in their interactions with government services. Blockchain technology can provide these benefits to governments. Thus, governments should move forward and determine how to digitize their functions with it. In moving forward, a government should establish a commission that analyzes areas—particularly the areas mentioned above—that would benefit the most from blockchain digitization. Then, engage in a cost-benefit analysis of the impact of digitizing the respective function. As far as creating their own blockchain platform, they could issue a request for production, or use a sole source contracting with Guardtime (the company that constructed Estonia's platform) or IBM (a leader in developing blockchain platforms for businesses).

In all, the world is yet to realize the opportunities provided by blockchain technology outside of the financial sector and illicit activities. There is a whole world left untapped—a new digital world. Instead of stifling innovation and taking an antagonistic approach to the technology, governments should embrace it and build on the rails already established to bring the benefits of blockchain technology to their citizens. The internet—the last greatest technological innovation—changed how people, institutions, and governments interact. Blockchain technology is doing the same for people and institutions. It is time for a paradigm shift. It is time for governments to digitize their functions with blockchain technology. But they ***must not*** do so without (1) modernizing and improving citizens' data privacy protections, and (2) investing in workforce development programs like a CTE pipeline program. If the question is what can government do, the answer is your imagination. And blockchain technology will allow governments to tap into their creativity, reforming how governments function.

---

138 Katie Brown, *Powerful Partners: Business and Community Colleges, How investments in sector partnerships can help our economy thrive*, National Skills Coalition, at 1 (July 2018).
139 *Id.*

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Data & Society Research Institute

DATA&
SOCIETY

March 3, 2023

Office of Science and Technology Policy
Submitted via email to DARD-FTAC-RFI@nitrd.gov

RFI Response: Digital Assets R&D Agenda

Data & Society Research Institute ("Data & Society" or "D&S") is pleased to submit a response to the Request for Information ("RFI") published by the Office of Science and Technology Policy ("OSTP") on developing a National Digital Assets Research and Development Agenda ("R&D Agenda"). Our organization is an independent, nonprofit research institute studying the social implications of data-centric technologies and automation. We are working to produce empirical research that challenges the power asymmetries created and amplified by technology in society.

As the Federal Government develops its R&D Agenda, Data & Society is pleased to see OSTP's commitment to "a holistic vision of a digital assets ecosystem that embodies democratic values"[1]. While technological development can bear much fruit, it can also exacerbate systemic inequality. Early proponents of the Internet described a democratic, egalitarian online society; reality has proven far different, with existing inequalities often exacerbated by digital technologies.[2] Now, proponents of digital assets and distributed systems of governance evangelize the potential for decentralized technologies to usher in a new era of human rights protections and tamper-proof economies. Supporters believe that decentralization brings the promise of a more autonomous and resilient Internet, in which people instead of corporations have control over their web architecture and experience, and powerful institutions, including in the financial world, are removed as gatekeepers, leading to greater equity in access.[3] However, the empirical evidence behind these narratives – particularly related to the expected transformative, positive societal impacts of these technologies, is largely absent. What are the factors that could lead us to different outcomes from past cycles of technological change?

Accordingly, it is essential that OSTP's R&D Agenda not only invests in research that investigates, prevents, and leads to paths of repair when harms and discrimination occur, but uses empirical methods to assess the benefits of digital assets and similar technologies–and, critically, the societal distribution of any benefits.

---

[1]Science and Technology Policy Office. Request for Information; Digital Assets Research and Development. *Federal Register*. (March 3, 2023). https://www federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets

[2] Nadler, Anthony, Crain, Matthew, & Donova, Joan. *Data & Society Research Institute*. (October 17, 2018). https://datasociety.net/library/weaponizing-the-digital-influence-machine/.

[3] Barabas, Chelsea, Narula, Neha, Zuckerman, Ethan. Defending Internet Freedom through Decentralization: Back to the Future?. *Digital Currency Initiative*. (August, 2017). https://dci mit.edu/decentralizedweb

Our comment focuses on topics 3, 4, and 5 in the RFI to propose questions to aid the Administration and agencies to develop an agenda for responsible innovation in digital assets.[4]

1. **Are digital assets as beneficial to historically marginalized communities as they have been to privileged communities?**

Supporters of decentralized digital assets have touted both their accessibility to all – even and especially the unbanked – and their leveling effects. But we know little about how communities of color and historically disenfranchised groups are engaging with these new tools, either to increase wealth or to address endemic social problems.

The R&D Agenda must invest in research that uses empirical methodologies to understand the ways in which cryptocurrency markets and tools are being deployed to and within BIPOC communities. It must empirically investigate the degree to which digital assets and related technologies shift or reify existing power structures that undergird systemic inequalities in racialized capitalism.

How does BIPOC participation in cryptocurrency markets create or foreclose other opportunities? What are the financial risks and rewards being borne by groups with long histories of income and wealth disparities as a result of economic subordination, racist marginalization, and community disinvestment? What do digital assets mean for mutual aid groups (which have surged in the COVID-19 pandemic), indigenous sovereignty movements, and other groups adopting nontraditional ways of building community resilience, solidarity, and belonging? These are but a few of the questions that OSTP should consider as it develops its R&D Agenda.

2. **How do digital assets and decentralized technologies aggravate energy consumption in an age of climate disaster?**

Our current, highly-centralized online ecosystem has meant that data is accumulated and stored in gargantuan data centers, resulting in tremendous energy consumption, but achieving some economies of scale.[5] Decentralized blockchain technologies are designed around redundant storage and sometimes, as in the case of the bitcoin cryptocurrency, energy-intensive processing that grows exponentially by design. How does Web3's carbon footprint compare to energy use in

[4]Executive Office of the President. Executive Order on Ensuring Responsible Development of Digital Assets. *Federal Register* (March 9, 2022).
https://www federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets

[5]Kez, lzar Al , Foley, Aoife M. , Laverty, David , Furszyfer Del Rio, Dylan, Sovacool, Benjamin.
Exploring the Sustainability Challenges Facing Digitalization and Internet Data Centers. *Journal of Cleaner Production*. Volume 371. (October 15, 2022).
https://www.sciencedirect.com/science/article/pii/S0959652622032115.

other sectors and how does its existence shift energy practices in other domains? How should government actors, including environmental regulators, address environmental consequences given increasingly widespread use?

The explosive growth of data and escalating demand for computation is not a foregone conclusion simply to be managed. Questions about the carbon footprint of the Internet tend to frame the issue as managing the irreversible necessity of data with maximal efficiency. But not all data has value. In the current moment, a tech 'refusal' movement is questioning whether we can sustain our current practice of data agglomeration and hoarding. What are the trade-offs and how do we gauge whether certain types of data preservation or data processing are justifiable? Data persistence also has consequences for privacy. For example, under the EU's General Data Protection Act, the "right to be forgotten" legislation recognizes the value of data deletion for protecting the anonymity and privacy of individuals.

Thank you for the opportunity to provide feedback on the R&D Agenda. We encourage OSTP to cut through the hype and hyperbole around decentralized technologies, and to instead use empirical methods to ground claims about the benefits of digital assets and to ensure that all people may equitably benefit from digital asset innovation.

Sincerely,

Serena Oduro, Senior Policy Analyst
Janet Haven, Executive Director

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Distributed Consensus: Blockchain & Beyond (DC:BB)

The following response is from Distributed Consensus: Blockchain & Beyond (DC:BB), a community-based organization of national security experts, entrepreneurs, and leaders in the web3/blockchain space. The group started as a club at Naval Postgraduate School and is now transitioning to become a 501c3. Our purpose is to provide the best possible advice and education on all things related to distributed ledger technologies, as it relates to national security, for the United States and our allies. To contact DC:BB please reach out to Kelly McCoy at [redacted] or [redacted]

Response below is outlined with the six topics listed in the RFI. Given the nature of the request we focused, where applicable, on how our responses could impact the ability to project national power by framing our comments around the model of DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement. Resulting input was a collective effort from our active members.

1. *Goals, sectors, or applications that could be improved with digital assets and related technologies:*

- Information: The introduction of the information age has generated a post-truth crisis impacting the ability of common citizens to trust institutions and discern fact from fiction. Distributed ledger technologies offer a means to establish an immutable ledger that can help discern fact from fiction and reinforce the ability to trust institutions.
    - Examples of ongoing efforts on this principle:
        - Golden Protocol — A blockchain protocol to generate a decentralized graph of canonical knowledge that is open, free, permissionless and incentivizes individuals to enter data into the graph.
        - Edge & Node's Geo — A web3 browser and knowledge graph application using digital assets to organize public knowledge and information on to a global decentralized knowledge graph.
        - The Starling Lab — A research center dedicated to using decentralized tools, like cryptography and blockchain to advance the cause of human rights.
    - Potential Applications:
        - Diplomatic — Documenting of war crimes and other information of value to assist in maintaining international agreements and prosecuting war crimes.
        - Military — Documenting articles of war and their associated jus ad bellum onto a public chain can help in the political discourse and debate to ensure all facts are representative of verified truth.
        - Economic — Utilizing a digital assets and ledgers for tax collection can greatly assist in generating transparency of tax payer funds for both the tax payer and the government.
- Diplomacy:

- Blockchain's diverse technology solutions reveal higher adoption rates with communities in developing regions, typically intended to help improve accountability in fragmented bureaucratic ecosystems (i.e.medical records, financial inclusion, federated licensing and credentials)– especially when applied through zero knowledge proofs. There is potential fora divergence in blockchain development and adoption between authoritarian regimes and democratic nations, underscoring the need to understand the implications of blockchain technology in U.S.national security strategies.
- Civilians impacted by conflict and/or political upheaval benefit from blockchain technologies by offering immutable records (i.e. digital identities for refugees) and an alternative means to transact with digital assets when markets and economies are disrupted. Specific to the U.S. national security audience, global and borderless blockchains offer a new communication mechanism to reach populations and resist censorship or manipulation.
- The United States is positioned to assist allies who are looking for regulatory clarity and policy guidance to establish global norms in line with U.S. values for blockchain and digital assets. There is a significant need for public/private partnerships to quickly improve awareness, capacity, and competency in the complex blockchain ecosystem (DoD is too often overlooked in key stakeholder positions).

2. *Goals, sectors, or applications where digital assets introduces risks or harms:*

- Given the above positive observations, of the impact on information, the reverse can also be true. Actors, specifically from totalitarian states, will create alternative chains as means to generate their version of the truth. It is vital for liberal order that a chain is built with the means to provide finite detail on the claims and positions it takes. Data centric approaches to fact verification, such as that of Belling Cat, would likely be a good base to start from.
- Given a public immutable distributed ledge, without zero knowledge proofs, privacy is impossible—as all transactions are public. Given the identification of an individual and their wallet address, their entire financial history (on that wallet) and who they associate with can be quickly discovered.
- Exchanges and/or clearing house supporting the Central Bank Digital Currencies (CBDCs) of two or more countries (e.g., mBridge).
- Charitable payment rails without accompanying identity protection mechanisms in areas with high levels of conflict, corruption, and/or sophisticated criminals

3. *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets:*

- Expand the window of critical infrastructure dependency analysis to include blockchain and blockchain-dependent services (such as some implementations of decentralized identity)

4. *R&D that should be prioritized for digital assets:*

- Customizable programs/applications on blockchain to automate enforcement of spending controls, dictate payment rules, check for sanctioned wallets, and simplify reporting.
    - Smart contracts offer unavailable solutions to some of biggest challenges facing government financial management—specifically for supply chain traceability and internal controls.
- Covert communications over the Ethereum blockchain is possible and relatively simple if a modest amount of training is dedicated to the process.
    - The transparency of the Ethereum blockchain allows for the immediate publication and distribution of financial transactions, which helps prevent manipulation by third parties. However, prior planning is essential and required between the two communicating entities to ensure covert communications are effectively exchanged.
    - Transparent blockchains are pseudonymous, which means public wallet addresses are observable while personal identity behind the transaction is not apparent.
    - By utilizing open-source encryption tools, it's possible to send a transaction from a pre-planned wallet address to a random (unaffiliated) address which holds the encryption hash intended to be decrypted into the covert message.
    - For more information, please see "Framework for Anonymized Covert Communications: A Blockchain-based Proof-of-Concept" https://calhoun.nps.edu/handle/10945/71071

5. *Opportunities to advance responsible innovation in the broader digital assets ecosystem:*

- Entrepreneurial grants to bring digital asset solutions to economic problems in developing countries. Per example, Iraq is taking on the digital Yuan due to a USD shortage. Entrepreneurs aligned with Department of State/USAID mission, aims, and requirements could provide an invaluable soft power tool to compete against encroachment on U.S. economic power and influence in developing economies.
- Opt-in services that allow innovators to explore automated approaches to governance and compliance. Examples could include:
    - per-transaction tax payments to the IRS
    - per-transaction reports based on existing Federal compliance requirements (e.g., SEC, FINCEN, etc.)

6. *Other information that should inform the R&D Agenda:*

- Preceding any R&D must be an informed strategy and vision on digital assets for the U.S. government. Such strategy must include a clear regulatory format designed to encourage and embrace thoughtful and positive innovation. Without such strategy and vision to lead the way, productive innovation that can help save significant tax dollars or *help the United States compete in this renewed era of great power competition — all remains unlikely to develop and evolve.*

- *United States Special Operations Forces are well situated to rapidly test, evaluate, and protype blockchain based solutions that could be of use in semi and non-permissive environments outside the United States. For more information on this, please see "Special Operations and Cryptocurrency: Concepts To Harness Innovation For National Security" at: https://calhoun.nps.edu/handle/10945/71537U.*

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

The Digital Dollar Project (DDP)

THE DIGITAL DOLLAR PROJECT

The Digital Dollar Project
Response to the Office of Science and Technology Policy
Digital Assets Research and Development Request for Information
March 2023

The Digital Dollar Project (DDP)[1] welcomes the opportunity to respond to the Office of Science and Technology Policy (OSTP) on its request for information (RFI) on digital assets research and development. The DDP commends OSTP for its thoughtful exploration of digital assets, including a potential U.S. central bank digital currency (CBDC).

The DDP is a non-profit, non-governmental organization dedicated to catalyzing private sector exploration of the potential advantages and challenges of a U.S. CBDC – or "digital dollar." The DDP believes that the dynamism and innovation of the private sector has a crucial role to play in the exploration of a well-designed digital dollar. The decision of whether to digitize the dollar is no different from past U.S.-led technological innovations – including the space race and the creation of the internet – in which both the public and private sectors contributed significantly. The DDP conducts research on the implications of a potential CBDC on important topics such as privacy and risk. The DDP also created a pilot program that tests hypotheses about a U.S. CBDC under real-world conditions. The DDP and the Depository Trust & Clearing Corporation (DTCC) completed the world's first entirely private sector initiated CBDC pilot in November 2022, which examined how a wholesale U.S. CBDC could impact security settlement to support U.S. post-trade infrastructure.[2]

The DDP seeks to serve as a neutral resource for policymakers, including OSTP, as they consider the benefits and challenges of a digital dollar. While the DDP does not advocate for the ready deployment of a digital dollar, we encourage the U.S. government accelerate research initiatives in coordination with private sector, non-profit, and academic leaders. We also encourage the United States to play a leading role in international digital currency standards setting.

In addition to answering the specific questions posed by OSTP, the DDP has outlined three high-level recommendations for the U.S. government's exploration of a digital dollar:

1. **The U.S. government should increase investment and activity in research initiatives to explore the benefits and challenges of a tokenized digital dollar.** The U.S. government should prioritize research to reimagine the potential "rails" of such a system and evaluate technical and policy solutions to preserve all forms of privacy. Further research and bold leadership are needed to explore how a digital dollar could benefit underserved populations and increase broad access to safe and efficient financial services.

[1] The Digital Dollar Project. "Revisiting the Digital Dollar Project's Exploration of a U.S. Central Bank Digital Currency." January 2023.
[2] The Digital Dollar Project and DTCC. "Security Settlement Pilot: Exploring Post-Trade Security Settlement with a U.S. Central Bank Digital Currency." November 2022.

2. **The U.S. government should leverage public-private partnerships in its exploration of a digital dollar.** Transparent public-private partnerships promote innovation and ensure that new technologies are not developed in siloes. Dynamic public-private partnerships to explore a digital dollar could help the U.S. government better understand technical design choices and challenges, as well as possible impacts on the private sector and the general public.

3. **The U.S. government should lead international digital currency standards setting regardless of whether it decides to deploy a digital dollar.** The United States has been conspicuously absent from global digital currency discussions – an unsustainable position given the impact of foreign CBDC issuance on the American economy. The DDP believes the United States should participate in and lead discussions on global standards regardless of whether it decides to deploy a digital dollar.

Responses to Specific RFI Questions

Below are the DDP's responses to OSTP's specific questions. While the RFI seeks information on a range of digital assets, DDP focused its response on a potential U.S. CBDC as that is most relevant to our perspective as a non-profit exploring advantages and challenges of a digital dollar.

1. Goals, sectors, or applications that could be improved with digital assets and related technologies:

Digital assets could improve a broad range of sectors, goals, and applications. A tokenized digital dollar that is issued by the Federal Reserve and enjoys the full faith and credit of the U.S. government could offer particularly significant benefits to the American economy. Because there is no better, riskless settlement medium than U.S. central bank money, a tokenized digital dollar could offer safety and stability along with payments efficiency and enhanced financial inclusion.

The DDP believes that a tokenized digital dollar could serve as a base layer for economic activity and private sector innovation in the increasingly digitized 21st century economy. A tokenized digital dollar could facilitate interoperability and transferability globally and advance the dollar's key role in global transactions such as trade and remittances.

A digital dollar would be distinct form other forms of existing digital payments instruments, such as credit cards and payments apps, as it would be a direct claim on the central bank rather than a liability of a private institution. A digital dollar would be a safer payment medium than other digital assets that may be subject to liquidity and counterparty risks. The DDP hypothesizes that a tokenized digital dollar could serve as a bearer instrument and therefore a major technological upgrade over existing, private digital money. A tokenized digital dollar could also represent a significant improvement over the outdated, time-consuming, and reconciliation-intensive account-based financial system of today.

When discussing CBDC, it is crucial to understand its two main forms: retail and wholesale. Retail CBDC refers to a CBDC that is accessible to individual consumers and can be used for everyday purchases and peer-to-peer, peer-to-business, or business-to-business payments. Wholesale CBDC is a type of CBDC utilized by large financial institutions – rather than individuals – to facilitate interbank settlements and other large transactions. Both retail and wholesale CBDCs could offer significant improvements to a range of goals, sectors, and applications.

Retail CBDC

In the retail context, a tokenized digital dollar could be used to facilitate fast and safe settlement in an array of transactions. While the DDP believes that a retail digital dollar should serve as a complement to and not a replacement for physical cash, we note that a retail CBDC could fill a cash-like role for the emerging digital economy. Cash is a safe, privacy-protected, censorship-resistant bearer instrument that issued with the full faith and credit of the U.S. government. Only a tokenized digital dollar could fulfill a cash-like role for digital commerce and ensure that the public has continued access to safe central bank money in the increasingly digitized 21st century economy.

The DDP hypothesizes that a retail digital dollar, if designed to be private by default and interoperable with other domestic and foreign payments systems, could increase payments efficiency, lower transaction costs, broaden access to financial services, and increase financial security for underserved populations.

Depending on design choices, a retail digital dollar could provide financial institutions and financial technology companies – in partnership with community outreach efforts – with the underlying CBDC technology upon which to build inclusive payment and banking services. Regulated institutions could develop digital wallets that provide unique services that cater to distinct user bases. The DDP believes that lower operational costs combined with innovative offerings from private sector digital wallet providers would expand access to un-and-underbanked populations. To fully maximize the cash-like potential of a retail U.S. CBDC, offline functionality is a necessary requirement to reach broad swaths of the American population which still lack consistent internet access.

The DDP notes that the current landscape for retail payments in the United States is sophisticated and does offer significant benefits. However, these benefits often come with tradeoffs could be resolved with the issuance of a well-designed digital dollar. For example, some merchants and consumers prefer the immediate liquidity provided by cash payments, but physical cash has transport and storage limitations. Electronic credit and debit card payments provide broader access and optionality for consumers but create trapped liquidity for merchants bound to multi-day settlement cycles. A U.S. CBDC could enable consumers to pay the retailer directly and instantaneously for lower cost. A digital dollar could provide treasury benefits for small businesses that cash currently offers and electronic access that does not require a banking intermediator to verify and settle the transaction. A digital dollar could thus offer retailers, consumers, and financial institutions a potentially more affordable and efficient payment method over existing cash, card, and app-based payments. Additionally, the increased speed by which merchants receive and access funds would provide them with working capital benefits.

DDP encourages continued U.S. government experimentation, data-gathering, and innovation involving both the public and private sectors to advance consideration of the advantages and challenges of a well-designed retail digital dollar.

Wholesale CBDC

A natively tokenized wholesale digital dollar could serve as a technological upgrade over existing and upcoming wholesale payments systems. Wholesale CBDC could reduce counterparty risk and trapped liquify, increase capital efficiencies, provide a more efficient, automated workflow, guarantee that cash and securities are delivered, and provide appropriate transparency to regulators.

The DDP and DTCC completed a pilot that explored how a wholesale digital dollar might operate in the U.S. clearing and settlement infrastructure by leveraging distributed ledger technology in a simulated environment created to reflect real-world conditions. The pilot tested real-time delivery-versus-payment (DVP) settlement using cash tokens to explore the potential benefits of a wholesale U.S. CBDC in increasing payments efficiency while reducing counterparty risk and trapped liquidity.[3]

2. Goals, sectors, or applications where digital assets introduces new risks or harms

Foreign CBDCs could introduce new risks and harms to U.S. economic and national security. The United States has long benefited from the dollar's role as global reserve currency, but it is possible that the dollar's crucial status could be face mid-to-long term challenges stemming from the rapid proliferation of foreign CBDCs and leadership of other central banks in the digital currency standards setting process.

Importantly, foreign countries could utilize CBDCs to circumvent economic sanctions, which serve as a key pillar of U.S. foreign policy. The U.S. government should devote resources to fully understanding and evaluating the impact of foreign CBDCs on national security, with a focus on U.S. sanctions policy.

There is also a risk that the United States will fall further behind as other countries participate in the development of global digital currency standards. Global leaders of CBDC exploration will play an outsized role in setting the standards for money's future as these technologies advance. The DDP believes that the United States should play a key role in the formation of global digital

[3] The Digital Dollar Project and DTCC. "Security Settlement Pilot: Exploring Post-Trade Security Settlement with a U.S. Central Bank Digital Currency." November 2020.

currency standards. The decision of whether to engage in global standards setting is key and independent of the decision to deploy a digital dollar.

In a major development that largely flew under the radar, several central banks completed the initial phase of project mBridge, a Bank for International Settlements (BIS)-led collaboration that experiments with cross-border payments using a custom-built platform based on DLT upon which multiple central banks can issue and exchange their respective CBDCs. Project mBridge participants include the central banks of China, Hong Kong, Thailand, and the United Arab Emirates. Each central bank contributed to the testing or "real-time, peer-to-peer, cross-border payments and foreign exchange transactions using CBDCs."[4] The transactions in Project mBridge are wholesale, which, as discussed above, are large-value transactions predominately executed by banks and other financial institutions.

Project mBridge is an early example of how global trade could be conducted outside of the existing global financial system that is led by the United States and its affiliated institutions. In some of the scenarios tested in Project mBridge, transactions were settled instantly across borders – a substantial increase in efficiency over the existing system in which transactions often take multiple days to pass through the correspondent banking system.

Project mBridge developed a system in which one bank could pay another bank in a different country, and the receiving bank is enabled to receive the payment in its own currency. If a Thai bank sent funds to a Chinese bank in its own CBDC, the Chinese bank would receive funds in its own currency. The influential role of the People's Bank of China and the clear potential for a new global financial order that sidesteps U.S.-aligned conventional banking channels makes Project mBridge among the key global CBDC initiatives to follow.

In addition to evaluating the risks posed by foreign CBDCs, the U.S. government should continue exploration of a digital dollar with the private sector to understand potential risks posed by the issuance of a digital dollar in the domestic context. Real-world testing is necessary to uncover any CBDC implications on markets and users. Importantly, the DDP encourages the U.S. government to focus exploratory work on appropriate CBDC rails as ultimate selection will have a profound impact on system governance, interoperability, security, resiliency, and privacy.

In addition to the new risks posed by the deployment of foreign CBDCs, the deployment of a digital dollar and establishment of a U.S. CBDC system could create new risks related to cybersecurity and privacy. The DDP expands more on these potential risks and opportunities to mitigate these risks below.

3. *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets:*

[4] Bank for International Settlements. "Project mBridge: Connecting economies through CBDC." October 2022.

To mitigate the potential cybersecurity risks facing a potential U.S. CBDC system, the U.S. government should explore different CBDC rail options, which range from a centralized government database to open public blockchains to middle-ground permissioned blockchains with curated nodes and validators. While testing is necessary to better understand the technical, operational, and governance implications of underlying CBDC rails, DDP suggests that the U.S. government avoid pursuing a highly centralized database system. Such an approach could raise critical security and resiliency concerns. A highly centralized database would also raise privacy concerns given the “honey pot” of information contained in a centralized place.

A likely preferable design approach would focus on a DLT-based or inspired CBDC network that prevents a single point of attack. If designed as a distributed network, such a network would definitionally be a more resilient and redundant data construct. Additionally, a blockchain-based CBDC could utilize a multi-signature wallet to stop single-channel attacks. Funds could be verified and transacted locally within a wallet. If a CBDC enabled offline payments during low or no network connection, the system would be resilient to operational failures or disruptions such as natural disasters, electrical outages, and other issues.

To this end, systems designed with distributed architectural components and validations can continue to operate when other parts of the network are offline or unavailable. In an extreme case, if the entire system goes offline, then the ability to conduct transactions offline allows digital currency to exhibit a degree of resiliency regardless of its online/offline status. Offline transactions will no doubt have limits as security of these transactions are directly proportional to the storage capacity in secure end-devices such as chip cards or secure storage options.
Unavoidable cyber risks include cryptographic algorithm insecurity over the lifetime of any digital currency used. Digital currencies are typically comprised of cryptographic keys that are intended to be resistant to attacks. There is a direct correlation between the strength of algorithm used, the size of the cryptographic key material, the compute time to generate the encrypted or signed data, the time value of the data, and the compute time to cryptographically 'break' or compute the above with access to the key. Evaluation of cryptography durability is an area of focus and exploration for central banks. Much like how security features on old physical bills are easier to replicate, the design must consider a modular infrastructure that prepares for advancements in attack capabilities. Certain security features may have tradeoffs that reduce functionality or may not be enforceable, e.g., recall old digital currencies and re-issue new ones. Further exploration and experimentation into the design requirements of diverse use cases will help shed light on the potential risks and design trade-offs.

Concerns have also been raised that the introduction of a U.S. CBDC could lead to disintermediation of the banking sector. However, the magnitude of such an impact is unclear and will depend on the design of a CBDC and how attractive it is to hold and use when compared to commercial bank money. The desire for consumers to hold and use CBDC tokens will depend on design considerations such as privacy, programmability, interoperability, and public confidence. To get these considerations right, the U.S. government should engage with the public to understand preferences and design tradeoffs.

Higher levels of disintermediation could have implications for the efficiency of credit provision in the economy – specifically, leading to more expensive credit and tighter lending criteria (already a challenge for the underserved communities). It is arguable that without safeguards or system assurances on convertibility, CBDCs could exacerbate financial instability during periods of economic stress as people would likely seek to substitute bank deposits with CBDCs. The same set of trade-offs that exist today between cash and account-based funds, such as immediate access, security, interest on account, and access to other financial services, will also apply to greater or lesser degrees in the future of CBDC and online banking. If consumers are confident in their ability to exchange CBDCs for FDIC insured commercial bank money, the banking relationship should mirror the current cash model.

Additionally, the U.S. government should take steps to understand other novel risks that could face the private sector, including banks and other regulated financial technology companies that would likely play key roles in distributing digital dollars. The DDP has convened a private sector Risk Working Group to develop a preliminary Risk Management Framework for banks in a CBDC future. The DDP looks forward to sharing the Risk Work Group's findings with OSTP and other policymakers and regulators to inform thoughtful consideration of a digital dollar and its potential impacts on the private sector.

In addition to the risks outlined above, the U.S. government should take steps to mitigate potential risks to privacy, which we explore in our response to question #4 below, and against risks stemming from foreign CBDCs, which we evaluate deeper in our response to question #5.

4. R&D that should be prioritized for digital assets:

The DDP unequivocally believes that privacy – a fundamental democratic value – is a core principle that must underly the potential success and adoption of a digital dollar. The United States should continue its CBDC exploration in a way that promotes democratic values of individual liberty, freedom of speech, personal privacy, limited government, and the rule of law.

To do so, the United States should prioritize R&D initiatives that could enable a privacy-preserving digital dollar. There is a broad range of technological innovations, including privacy-enhancing technologies (PETs), that enable the confirmation of critical identity information while continuing to mask other pieces of sensitive and personally identifiable information.

The U.S. government should prioritize R&D related to encryption techniques and PETs including but not limited to:

- **Zero-knowledge proofs (ZKPs) –** A type of cryptographic protocol that allows one party (the prover) to prove to another party (the verifier) that they know a certain piece of information without revealing any information about the actual content of that information. ZKPs are useful for many applications in which it is important to preserve privacy.

- **Homomorphic encryption –** An encryption technique that allows mathematical operations to be performed on encrypted data without the need to decrypt it first.

- **Multi-party computation –** A distributed computing technique where multiple parties with their own private data can jointly compute a function over their inputs without revealing their inputs to each other.

- **Differential privacy –** A system for publicly sharing dataset information by describing patterns of groups within the dataset while withholding information about individuals in the dataset.

Additional U.S. government R&D is needed to fully understand the potential tradeoffs between privacy, security, and financial inclusion, and to develop technologies and policies to address these tradeoffs. The U.S. government can play a significant role in conducting basic R&D that complements and leverages the best of private sector innovation. We encourage the OSTP and the rest of the U.S. government to prioritize public-private partnerships and seek input from a range of private sector stakeholders, including leading non-profits, privacy and civil liberties advocacy groups, and academics.

5. R&D Opportunities to advance responsible innovation in the broader digital assets ecosystem:

The DDP appreciates and supports OSTP's emphasis on "standards setting efforts that could help advance democratic values in the use and governance of digital assets." Global standards are critical to ensuring interoperability, transferability, consistency, and safety across various industries. Global standards often promote societal values, including democratic values such as privacy, free enterprise, and economic liberty.

The United States has been a leader in developing global standards for the fields of technology, trade, and finance, among others. The United States' crucial role in the global financial system dates to the enactment of the Bretton Woods agreement in 1944, where representatives from 44 countries signed an agreement that established rules and principles that guided international financial relations for several decades following World War II.

Importantly, the U.S. dollar is the global reserve currency – a status that is maintained by a range of factors. In recent years, we have seen some countries begin to develop alternative payment rails that could be sued to circumvent sanctions imposed by the United State and its allies, as well as other rules and norms that govern the current financial system. It is possible that CBDCs could be used to avoid financial sanctions, depending on how they are designed and implemented, making it imperative that the U.S. government consider ways to maintain the use of the dollar in digital global payment systems and develop a strategy related to the use of alternative payment systems.

However, the United States should not engage globally on digital assets from a purely defensive posture. The United States should offer forward-thinking leadership on issues such as CBDC interoperability and transferability. Interoperability is particularly important when designing CBDCs. Interoperability can prevent market fragmentation, increase payment provider competition, and enable broad adoption. While many countries are developing CBDCs in silos (likewise for private sector companies developing stablecoins), the United States should consider the dollar's global utility when designing a CBDC to achieve global economic efficiencies, as the dollar is a payment mechanism that underpins and provides liquidity across international markets. As of March 2023, it is increasingly clear that global CBDC developments are heading in the direction of siloes – a concerning trend.

A CBDC could enable a translation layer between multiple CBDC networks and technology platforms, creating a shared language domestically and globally. This transferability across traditional and DLT-based networks would streamline transaction data sharing across many use cases. To achieve this level of interoperability, CBDC development should consider emerging token standards to connect future CBDC networks. The United States can collaborate with corporations, regulators, government agencies, and academics globally to advance technology standards and other layered facets such as identity frameworks and consumer protections. By taking a leading role in interoperability, the U.S. will be able to set global standards in the internationalization of CBDCs and protect against countries that do not serve U.S. interests.

If other countries develop widely adopted CBDCs that become the de facto standard for international wholesale and retail payments, they may have a head start in setting global standards for the future of money.

China may be well-positioned to begin setting the global CBDC standards agenda following its influential role in driving Project mBridge. If Project mBridge marks the start of a renewed effort to redirect the global financial order away from the current U.S.-led system, it may constitute a critical inflection point that necessitates a dynamic response. The United States today largely relies on its ability to leverage the dollar's outsized global role and the position of its banking system. If the U.S.-led global financial infrastructure is perceived as too slow and expensive in comparison to foreign alternatives, it is reasonable to anticipate that countries around the world will begin, and in some cases continue, the process of "de-dollarization."

In 2022, a working group of distinguished experts in national security, finance, economics, central banking, technology policy, and computer science from the Hoover Institution studied the global implications of China's CBDC, the e-CNY. The working group's report analyzed and detailed the degree to which China has established a first-mover advantage in not only the deployment but also the technical underpinnings of CBDCs.[5]

[5] The Hoover Institution. "Digital Currencies: The US, China, and the World at a Crossroads." March 2022.

The study also notes that the e-CNY enhances China's ability to cement its international leadership of payment technology, innovation, and adoption, set economic norms and technical standards that align with its authoritarian governance system, and increase its ability to undercut the traditional dominance of the U.S. dollar a source of geo-economic and strategic influence.

As foreign countries develop CBDC systems that replace traditional payment rails and provide CBDC as a service to international financial participants, U.S. policymakers should develop a strategy to preserve the dollar's vital role in the global digital economy and consider how best to future-proof the dollar in a way that is consistent with American ideals and values and grounded in empirical data and research.

Global leaders of CBDC exploration will play an outsized role in setting the standards for money as these technological developments advance. The Digital Dollar Project is focused on supporting the United States in taking a leadership role in exploring and designing a CBDC that upholds American democratic values of freedom, economic stability, and personal privacy.

In the coming CBDC future, the United States should actively lead global discussions on governance, interoperability, security, privacy, and scalability standards, rather than reacting to foreign CBDC decisions. Independent of a decision to deploy a U.S. CBDC or not, the United States should lead the development of an international regulatory framework around digital currencies, including CBDCs, that prioritizes privacy, consumer protection, financial anti-crime compliance, financial stability, and the protection of monetary sovereignty.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

DigiByte Alliance (DGBA)

Response of the DigiByte Alliance to the Office of Science and Technology Policy (OSTP) Request for Information; Digital Assets Research and Development

March 3, 2023

For additional information about this response please contact:

Michelle Dougherty
DigiByte Alliance
[redacted]

Introduction

The DigiByte Alliance (DGBA) respectfully submits these comments in response to the White House Office of Science and Technology Policy's Notice of Request for Information (RFI) to help identify priorities for research and development related to digital assets.[1] DGBA[2] is a 501(c)(3) public non-profit research and advocacy organization focused on the development and adoption of DigiByte, an open-source, permissionless blockchain network.[3]

DGBA appreciates and supports the development of a National Digital Assets Research and Development Agenda (NDARDA), and recognizes the vital roles of the Office of Science and Technology Policy (OSTP), the Fast Track Action Committee (FTAC) on Digital Assets Research and Development of the Subcommittee on Networking and Information Technology Research and Development (NITRD) of the National Science and Technology Council (NSTC) and the National Science Foundation, and the NITRD National Coordination Office as they endeavor to craft a comprehensive NDARDA.

DGBA's response to the RFI focuses primarily on the benefits and applications of public decentralized permissionless blockchains (DPB) to an overall NDARDA. As stewards of the DigiByte blockchain, we are intimately familiar with the potential of DPBs. We believe that blockchains like DigiByte should be an essential part of any NDARDA and are vital to demonstrate America's global leadership in digital asset innovation and security. Our response focuses collectively on Topics 1, 4, and 6 of the RFI.

Built upon Open-Source Software (OSS), DPBs reinforce the ideals of privacy, individual sovereignty and free market competitiveness and offer the type of access and public accountability that can reinforce rather than hinder American values. History teaches us that innovation and inclusion flourish when participation barriers are lowered or eliminated. DPBs by their very nature fulfill that promise. We believe that it is inevitable that blockchain technology will replace much of todays' information, communication, financial, and storage infrastructure, each of which will demand robust and resilient cybersecurity and public trust. Since DPBs like DigiByte have immutable encryption technology in their DNA, they are an ideal substrate upon which to research and build future democracy enhancing innovations in the emerging digital economy.

A. U.S. Government Strategy for Establishing Federal R & D Priorities

1. Identify the Problems

DGBA believes it is essential to develop a public framework and common lexicon among public and private stakeholders regarding the key challenges and impediments to the wider adoption and public trust of digital asset technology. Specifically, those areas where a lack of transparency, efficiency, and security cause the greatest misallocation of resources, fraudulent activities, and system exploitation. Expert insights from private and public stakeholders, including the various agencies (e.g., Offices of Inspector General and cyber security related agencies) about current

---

[1] Office of Science and Technology Policy (OSTP) "Request for Information; Digital Assets Research and Development," *Federal Register*, Vol. 88, No. 17 (January 26, 2023) https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development

[2] https://www.dgballiance.org

[3] https://digibyte.org/en-us/

system or operational vulnerabilities within the Federal Government and beyond should be gathered in parallel. Such a survey would better inform federal resource allocation and priorities for future development of digital asset technology solutions and applications within the Federal Government, and beyond.

Since blockchain technology is by its very nature an evolving "general purpose technology,"[4] a research and development strategy that starts with known problems avoids research and development looking for lesser problems to solve.

2. Identify the Technologies with Potential to Solve the Identified Problems

The full potential of DPBs' role is understood among disinterested developers and advocates of a more democratized, secure, fair, and transparent blockchain ecosystem. The future of DPBs like DigiByte and other digital asset technology has been obscured by the lack of regulatory clarity, and the adjacent issuance and trading of private digital assets. DGBA believes that these distractors have hindered private resource allocations and investment in legitimate, long-term platforms and technologies.[5] The value of DPBs enabling technology has been distorted by speculative valuations and misallocated investments that might otherwise have been directed to proving the universal value of permissionless open-source projects.

As NDARDA considers which technologies to prioritize for research and development, DGBA believes that open-source technologies must be the bedrock upon which future blockchain adoption and applications are built. Only then can we harness the creativity of the disinterested developer community and the public trust needed to realize the potential of this nascent technology. If that future is dictated by technologies that are proprietary or opaque, the speed of adoption and trust will be measured in decades.

B. The Benefits of DPBs

1. DPBs Will Unlock American Innovation and Reinforce Democracy in the Emerging Digital Economy

The United States has been the dominant economic leader in the world for the past century because our system facilitates innovation and growth through free market participation. While our most important civilian technologies have been developed and commercialized by the private sector, the government plays a crucial role in funding the basic research and development which makes that success possible. Economic decentralization is a central prong in the story of America's success. Indeed, we export these principles to other economies, particularly those with limited or no access to capital. The US Agency for International Development, for example, rightfully emphasizes economic decentralization as a critical element in its guide to developing democracy in foreign

[4] "[T]he ability to track transaction attributes, settle trades and enforce contracts across a wide variety of digital assets is what makes blockchain technology a general purpose technology." Catalini & Gans (2016), *NBER WORKING PAPER SERIES SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN* Retrieved from https://www.nber.org/system/files/working_papers/w22952/w22952.pdf, p.3

[5] In addition, open-source projects that are likely to have a high degree of application and use by the general public are least likely to garner support by private investors as they cannot guarantee a return on investment. Where "market forces will lead to an underinvestment in R & D from society's perspective, …a rationale for government intervention [is provided]." Speech by Chairman Ben S. Bernanke on Promoting Research and Development: The Government's Role. (n.d.). Board of Governors of the Federal Reserve System. https://www.federalreserve.gov/newsevents/speech/bernanke20110516a.htm

countries.[6] The "cornerstones of economic freedom are personal choice, voluntary exchange, open markets, and clearly defined and enforced property rights."[7] It is axiomatic that the NDARDA create policy supporting technology that reinforces these values.

DPBs are the networks upon which "entrepreneurial experimentation can take place and be rewarded from anywhere in the economy."[8] Research shows that open permissionless networks have a greater likelihood of boosting economic innovation and thereby inclusion in wider segments of the population.[9] Permissionless blockchain networks will become the public utilities upon which economic value can be created without the necessity of a third-party intermediary, unlocking the unprecedented potential for increased economic activity and growth.[10] That DPB's have the potential to create more economic innovation stems from their underlying technological properties which enable distinct commercial aptitudes.

From an economic perspective, "two key costs are impacted by blockchain technology-the cost of verification of state and the cost of networking."[11] While permissioned blockchains can impact the former, it is only permissionless blockchains that can impact both.[12] Permissioned blockchain protocols operate under the same limitations of a traditional database-where trust is placed in intermediaries. DPBs by contrast sustain that trust using the mathematical code of a distributed ledger and have the potential to serve as vehicles for economic growth "by reducing barriers to entry within sectors that are heavily concentrated because of network effects and control over data, [thereby enabling] a new wave of innovation in digital services, and greater consumer choice."[13] As regulatory frameworks become clearer these increased benefits can begin to come to fruition.

2. The Open-Source Software Environment of Decentralized Blockchains Can Accelerate Digital Asset Development

OSS contributions lead to a greater escalation of entrepreneurial activity and growth.[14] That "software for the public benefit should be open source by default" has been noted by many[15] and is consistent with the United States' policy about the benefits of using OSS. *See* OMB Memorandum M-16-21 *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through*

[6] *Democratic Decentralization Programming Handbook | Document*. (2022, December 16). U.S. Agency for International Development. https://www.usaid.gov/democracy/document/democratic-decentralization-programming-handbook
[7] Gwartney, J., Lawson, R., Hall, J., Murphy, R., Djankov, S., & Mcmahon, F. (n.d.). *ANNUAL REPORT*. Retrieved February 28, 2023, from https://www.cato.org/sites/cato.org/files/2022-09/efw-2022-full-issue.pdf
[8] Catalini & Gans (2016), *NBER WORKING PAPER SERIES SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN* Retrieved from https://www.nber.org/system/files/working_papers/w22952/w22952.pdf
[9] Ibid.; KR, Dr. V., & K, M. (2022). The Emergence of Decentralized Business Models: Blockchain Interruption and Decentralized Finance. *International Journal for Research in Applied Science and Engineering Technology*, *10*(6), 2165–2171. https://doi.org/10.22214/ijraset.2022.44168
[10] "A private blockchain is an intranet, and a public blockchain is the internet. The world was changed by the internet, not a bunch of intranets. Where companies will be disrupted the most is not by private blockchains, but public ones." https://bitcoinmagazine.com/business/mit-s-brian-forde-companies-will-be-disrupted-the-most-by-public-blockchains-1466028606
[11] Catalini & Gans, https://www.nber.org/system/files/working_papers/w22952/w22952.pdf, p. 2
[12] Ibid., p. 2 and 19.
[13] Ibid.
[14] Langburd, N., Nagle, W., & Greenstein, S. (n.d.). *Open Source Software and Global Entrepreneurship*. Retrieved from https://www.hbs.edu/ris/Publication%20Files/20-139_bd835fdf-a293-4912-aa21-769e77f2754a.pdf
[15] *Building and Reusing Open Source Tools for Government*. (n.d.). New America. Retrieved March 27, 2022, from https://www.newamerica.org/digital-impact-governance-initiative/reports/building-and-reusing-open-source-tools-government/

Reusable and Open Source Software.[16] While the full benefits of an OSS policy in the digital asset arena are articulated in that Memorandum, including cost savings and efficiencies, one benefit stands out:

> Making source code available as OSS can enable continual improvement of Federal custom-developed code projects as a result of a broader user community implementing the code for its own purposes and publishing improvements. This collaborative atmosphere can make it easier to conduct software peer review and security testing, to reuse existing solutions, and to share technical knowledge.[17]

OSS lowers the barriers to entry for disadvantaged income populations, is an opportunity for their participation in the frontier of digital asset development, democratizes access for contribution, and enables a "financial inclusion" strategy that encompasses a "financial participation" strategy with groups who are otherwise excluded from access in closed, private, siloed environments. The White House recently acknowledged the importance of equalizing access to maximize and harness American ingenuity in the context of its National Artificial Intelligence Research Resource Task Force final report: "[w]hile AI research and development (R&D) in the United States is advancing rapidly, opportunities to pursue cutting-edge AI research and new AI applications are often inaccessible to researchers beyond those at well-resourced companies, organizations, and academic institutions."[18] As stated by NSF Director Sethuraman Panchanathan:

> By creating an equitable cyberinfrastructure for cutting-edge AI that builds on-ramps for participation for a wide range of researchers and communities, the NAIRR could build AI capacity across the nation and support responsible AI research and development, thereby driving innovation and ensuring long-term U.S. competitiveness in this critical technology area.[19]

The same holds true for any NDARDA.

DGBA acknowledges the reflexive resistance to use of OSS for non-civilian (national security) applications, [20] but believes that adequate security perimeters can be deployed and weighed carefully in digital asset research and development efforts to take advantage of OSS-led innovations without sacrificing our most sensitive digital data and applications.

---

[16] MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES FROM: Tony Scott United States Chief Information Officer Anne E. Rung United States Chief Acquisition Officer SUBJECT: Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-Source Software. (2016). https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

[17] Ibid., p. 2 citing Department of Defense Chief Information Officer. *Clarifying Guidance Regarding Open-Source Software (OSS).* October 16, 2009: "The continuous and broad peer-review enabled by publicly available source code supports software reliability and security efforts through the identification and elimination of defects that might otherwise go unrecognized by a more limited core development team." http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf.

[18] *National Artificial Intelligence Research Resource Task Force Releases Final Report - OSTP*. (n.d.). The White House. Retrieved February 28, 2023, from https://www.whitehouse.gov/ostp/news-updates/2023/01/24/national-artificial-intelligence-research-resource-task-force-releases-final-report/

[19] Ibid.

[20] Ibid. Subsection 6.2 "The sharing of the source code would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy."

3. Permissionless Blockchains Are Weapons of Resiliency for Cybersecurity

Single points of failure are the Achilles heel of today's online security architecture. The network encryption properties of blockchain can mitigate these vulnerabilities, and additional research and development of these advantages is of paramount importance.[21] DPBs are built upon decentralized peer to peer networks that enable non-trusting parties to interact with each other without the need for a trusted authority, eliminating the need for a single, centralized third party vulnerable to single points of failure. Stated more simply, "[t]rust in the intermediary is replaced with trust in the underlying code and consensus rules."[22] It is the removal of this single point of failure that is the essence of DPBs whose outcome-agnostic encryption methodologies have the potential to create new avenues of secure online relational realities among and between businesses, governments, and individuals.[23]

DGBA assumes that the use of blockchain technology to mitigate the ongoing epidemic of cyber insecurity is a NDARDA priority. New cybersecurity solutions are of interest to every consumer of the internet, most particularly the U.S. Government. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*[24] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero-trust architecture. The White House's January 2022, *Memorandum Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*[25] further specified the mandate of a new security architecture paradigm. In 2021, cybercrime costs approached 7 billion dollars.[26] Cyber insecurity is a chronic disease in desperate need of a cure.[27] Decentralizing assets, applications, and security infrastructure through blockchain could make it possible to stop hackers in their tracks and beat them at their own game.[28]

The distributed nature of DPBs provides the underlying foundation of resilience upon which to build applications to achieve cybersecurity goals. Decentralized applications can include anything from IOT security, securing private messaging, authentication of software provenance, verification of cyber-physical infrastructures and securing DNS and DDoS.[29] Advances in cryptography, discreet

---

[21] A significant benefit of public blockchains is the general public's global participation in the security of the network. This eliminates devops requirements for the network, which are replaced with a simplified POW or POS operation. Devops required for POW security operations is simpler than standard server farms, thus producing a significant cost reduction.

[22] Christian Catalini & Joshua S. Gans, https://www.nber.org/system/files/working_papers/w22952/w22952.pdf, p.9.

[23] For an extensive review of current blockchain applications *See* Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*(36), 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[24] *Improving the Nation's Cybersecurity*. (2021, May 17). Federal Register. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[25] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[26] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[27] NPR. (2021, May 30). USAID Hack: Former NSA Official Calls U.S. Cyber Insecurity A "Chronic Disease." Retrieved February 28, 2023, from NPR website: https://www.npr.org/2021/05/30/1001748861/usaid-hack-former-nsa-official-calls-u-s-cyber-insecurity-a-chronic-disease

[28] Napoli, R. (n.d.). *Council Post: How Blockchain Could Revolutionize Cybersecurity*. Forbes. Retrieved February 28, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/03/04/how-blockchain-could-revolutionize-cybersecurity/?sh=6a65937c3a41

[29] Legrand, J. (2020, September 4). The Future Use Cases of Blockchain for Cybersecurity. Retrieved from www.cm-alliance.com website: https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity

permissions, and key distribution made possible by blockchains can become a cornerstone of how nation states protect classified information, intellectual property, and critical infrastructure.

4. The Potential of the DigiByte Blockchain as a Public Utility for Cybersecurity

DPBs can be considered public utilities like a highway, something for everyone to consume for the benefit of all. To the extent that the NDARDA intends to further explore cybersecurity applications on DPBs, DigiByte's nine year tested distributed ledger technology is perfectly suited to many functionalities due to the speed, security and scalability of its architecture.

The DigiByte blockchain is a DPB whose technology has potential to establish higher levels of protection to the prevalent and often insecure intermediary laden paradigms of today's economic realities.[30] The May 2021 paper *Achieving Cybersecurity in Blockchain Based Systems: A Survey*,[31] evaluated several extant blockchains for their adherence to NIST cybersecurity criteria[32] and found that "all cybersecurity properties are reached in DigiByte."[33] Having a resilient baseline level of technological properties places DigiByte in a unique category of public DPBs to serve a substrate for the development of decentralized solutions that can provide fast, secure, and scalable methods for the transfer, verification, authentication, and storage of data and communications.

a. Architecture of the DigiByte Blockchain

Since the utility and integrity of any blockchain network is coextensive with the degree of the security and performance capacity of that network, DGBA provides some background on the uncommon architecture of DigiByte.

DigiByte is an American born derivative of the Bitcoin blockchain[34] and is similarly a decentralized peer-to-peer worldwide network enabling transfer of value without third party intermediation. While DigiByte is a UTXO[35] blockchain that uses consensus mining algorithms, enhancements made to its core protocol allow for significantly improved functionality via its 15 second block times, real-time difficulty adjustment, extremely low fees, and distributed mining algorithms. DigiByte's five separate mining algorithms are geographically distributed across countries around the globe. This mining model increases DigiByte's decentralization by distributing it across distinct types of hardware thereby offering protection against malicious attacks.[36] Since implementation, the DigiByte blockchain has had over 16,000,000 blocks mined without interruption to the network. With over nine years of development, DigiByte is the longest and fastest UTXO blockchain in the world.

---

[30] As one of the only DPBs supported by a 501(c)(3) public foundation, the DigiByte blockchain is uniquely situated to participate in any R & D funding allocation to advance the capabilities of digital asset technology.

[31] Achieving cybersecurity in blockchain-based systems: A survey. (2021). *Future Generation Computer Systems*, *124*, 91–118. https://doi.org/10.1016/j.future.2021.05.007

[32] Based on a review of 272 papers between 2013 and 2020 and 128 business initiatives and specifically evaluating authenticity, non-repudiation and confidentiality elements of the NIST criteria.

[33] Ibid., p. 102; *see also* Ibid., Table 11.

[34] The maximum supply of DigiByte is 21 billion compared to Bitcoin's supply of 21 million.

[35] https://en.wikipedia.org/wiki/Unspent_transaction_output

[36] Spackman, J. (2020, August 2). *Some updated DigiByte mining stats graphs / comparisons*. Medium. https://josiah-digibyte.medium.com/some-updated-digibyte-mining-stats-graphs-comparisons-7f0c902b7554

DigiByte is a rare "layer one" public blockchain whose speed, security and decentralization coexist.[37] DigiByte's block timings are forty times faster than Bitcoin. The net result of this is a wallet-to-wallet transaction is received within a couple of seconds. Speed is important when implementing blockchain into real-life applications. The same can be said regarding DigiByte's negligible transaction fees which also bolster its capacity to serve as an instrument of real-world utility.[38]

In April 2017 DigiByte became the world's first major blockchain to successfully activate Seg Wit (Segregated Witness) which helps to achieve faster transactions. DigiByte also pioneered both Multi Shield and Digi Shield.[39] Demonstrating the power of OSS, many blockchain developments innovated by DigiByte developers have been incorporated into other major blockchain networks. For example, DigiByte's Digi Shield technology that facilitates predictable block timing performance in the face of fluctuating hash power has been added into over 2-dozen other blockchains.[40]

In 2019, DigiByte implemented a privacy feature Dandelion++ that can protect the privacy and security of DigiByte users. Dandelion++ protects your location by making it difficult to ascertain from a transaction the originating IP address. In addition, DigiByte has added technological features such as an assets layer which enables the issuance of NFTs and a DigiID cryptographic key log in technology that sets it apart as an emerging UTXO blockchain with an unusual capacity for Web3 and cybersecurity applications.

In sum, the unique characteristics of DigiByte include: (1) the difficulty adjustment algorithm is evolutionary compared to that of Bitcoin; (2) a fixed 15 second block timing that is adjusted dynamically block by block providing predictable function execution timing; (3) blockchain nodes are metaphorically comparable to RAID implementations. Each node is a redundant RAID 1 copy of the entire chain; (4) DigiByte's 5 separate algorithms give developers more options to design and securely optimize their use of the network based upon hardware availability, electrical costs, and infrastructure requirements; (5) Dandelion privacy features; and (6) an Assets layer.

a. DigiByte Applications

DigiByte's randomized multi-algo UTXO architecture makes it one of the most secure, fast, and scalable and cost-effective networks upon which to build applications and solutions. The breadth of real world DigiByte applications is constantly evolving without proprietary investments, an ICO or

[37] The current Transactions Per Second (TPS) for DigiByte range from 560 to 1066, and the underlying code enables DigiByte's TPS to be increased to 280,000 with further development.

[38] The precise carbon footprint of DigiByte as compared to other cryptocurrencies is not precisely known due to a lack of funding to conduct a comprehensive environmental audit. However, at the current time it is fair to say that it is significantly less than Bitcoin due to its lower market share. Some theorize that due to its faster block timing, DigiByte inherently consumes less electricity even if it were to increase Bitcoin's market share. However, this theory would require an in-depth environmental audit for confirmation. The countervailing benefits provided by blockchain mining to capture otherwise dormant natural resources, not to mention increase infrastructure resiliency, would have to be factored into any such cost benefit analysis.

[39] Activated in February 2014, this network upgrade allowed for the DigiByte blockchain to protect against multi-pools that mine large numbers of DigiByte at a low difficulty. It achieves this protection by recalculating mining difficulty between each block, allowing for a faster correction when a large amount of hashing power begins or ceases contributing to DigiByte, rather than recalculating once every two weeks as is the case with Bitcoin.

[40] Including Ethereum, Bitcoin Cash, Zcash, Dogecoin, and Bitcoin Gold, among others.

significant premine[41] to fund development efforts.[42] Below, we describe potential, current and past use cases and applications which illustrate the scope of technological advancements provided by the DigiByte blockchain network.

Document Verification and Authentication

DigiByte can be used to facilitate the issuance and storage of digital documentation in a way that prevents or minimizes fraud, counterfeiting and forgery. In an academic publication from the University of Lausanne, DigiByte is described as a viable blockchain technology to create a tamper proof timestamped provenance ledger for police in Switzerland, illustrating the viability of the DigiByte blockchain to support data integrity and authentication.[43] The Dutch company V-ID has used the DigiByte blockchain to achieve this result using their blockchain validation and verification platform[44] that protects against any form of digital fraud.[45] In 2019 Doewes Fine Art Gallery[46] in partnership with V-ID used the DigiByte blockchain to secure the authentication of a Rembrandt painting,[47] demonstrating the ability to use DigiByte to authenticate not only documents, but physical goods.

DigiByte can similarly be used to secure government documents, including its archives, using public and private keypairs associated with DigiByte addresses. Public addresses can retain encrypted hashes of stored documents; encrypted using the public key itself. The private key serves as identification for the public address, as well as facilitating the decryption of the encrypted hash. Once decrypted the hash is used to identify the specific stored document to retrieve from firewalled storage.

Digi-ID – Passwordless Login

Considering the current U.S. government wide effort to move to zero trust cybersecurity principles, Digi-ID may be of particular interest to those working on establishing zero trust protocols. This application was developed specifically for cyber protection.[48] This free, fast, and secure authentication method can be used as an alternative to passwords to sign into online applications. Using a blockchain-based signature, a private key is generated to log into a website or other platform. A multi-factor authentication tool, the keys are securely generated in a decentralized

---

[41] The .5% premine was for development of the first wallets and given away to early adopters to get the network up and running. See Bitcoin talk forum https://bitcointalk.org/index.php?topic=408268.0…

[42] DigiByte is not a company, and there is no central authority who can control its growth, distribution, development, or usage. This is the foundation upon which DigiByte is based. It is an open-source project, developed and supported by a truly decentralized global community of volunteers.

[43] Jaquet-Chiffelle, D.-O., Casey, E., & Bourquenoud, J. (2020). Tamperproof timestamped provenance ledger using blockchain technology. *Forensic Science International: Digital Investigation*, *33*, 300977. https://doi.org/10.1016/j.fsidi.2020.300977

[44] https://www.v-id.org

[45] *AmSpec And V-ID Verify and Protect Certification in The Petroleum and Petrochemical Industry*. (n.d.). Cryptodaily.co.uk. Retrieved February 28, 2023, from https://cryptodaily.co.uk/2019/06/amspec-and-vid-verify-and-protect-certification-in-the-petroleum-and-petrochemical-industry It is our understanding that V-ID no longer uses DigiByte as an anchor blockchain since it launched a DAO on Ethereum.

[46] https://douwesfineart.com

[47] Team, V. D. A. (2022, August 3). *First Blockchain Validated Rembrandt*. Medium. https://vidtdao.medium.com/first-blockchain-validated-rembrandt-4cca632f6a82

[48] https://www.digi-id.io/integration.html; Digi-ID is based on https://github.com/bitid/bitid and developed further into a user-friendly application. It is currently being used as a sign in method on the website https://changeangel.io

manner and are secured by the DigiByte blockchain protocol. Unlike many solutions on the market, Digi-ID keys are not generated by any private company or stored in a centralized database. Digi-ID can also be used as a complimentary 2FA.[49]

Besides the use to login to different websites, Digi-ID can be used for building security, to replace access cards, and to validate access to databases. Governments might save thousands of hours by using a system like Digi-ID to validate accesses since it allows for the creation of an ecosystem that upholds the concepts of safety and need-to-know. With Digi-ID no information is ever logged or stored on-chain.

The power of Digi-ID lies in its flexibility to also be used in connection with the assets layer of the DigiByte blockchain. The architecture of DigiByte enables the leveraging of its blockchain as a credential (or any asset) authenticator through the combined use of Digi-ID and its Assets layer. This potential combination of technologies is currently unique to the DigiByte blockchain.

Digi Assets

Digi Assets are metadata tagged fungible or non-fungible tokens issued on top of DigiByte's blockchain.[50] While the concept of assets and tokenization are possible across a wide variety of blockchains, Digi Assets benefits from its unique protocol properties, large global geographical node distribution, and variety of consensus algorithms. Since DigiByte does not have Turing complete smart contract capabilities, Digi Assets are not subject to smart contract attacks.

Digi Assets can be used to securely and cryptographically represent anything we find in the real world from physical assets such as real estate, airplanes and boats to any type of document such as wills and health care records. Governments could distribute any type of benefit via Digi Assets including anything from health care, social security and WIC benefits, and serve as the rails to ensure the distribution of benefits that can thereby effectuate the goal of financial inclusion.

Identity Verification

The promise of the DigiByte blockchain as a platform to provide security and combat fraud in identity credentialing was most recently recognized with an Honorable Mention for a presentation by DGBA at the Security Innovation Challenge sponsored by the Homeland Security Technology Consortium in September of 2022.[51] The Assets layer of the DigiByte blockchain is a metadata storage layer upon which credentials like passports and visas can be encrypted and then authenticated using Digi-ID. More specifically, a trusted authority could issue an asset reflecting ownership of a credential. The non-transferable asset, sent to the owner's wallet after encryption on an asset, can be verified by its owner using Digi-ID at a credential check point.

CONCLUSION

Due to its security features, blockchain may be used as a trusted infrastructure to develop a large variety of use cases and applications. We have presented some security-related use cases in this response. Just as no one understood how the internet would transform the world economy in 1990,

[49] See also https://www.thecrimson.com/sponsored/article/digibyte-digi-id/
[50] This application is in a beta stage of development.
[51] https://hstech.ati.org/#1666036158120-146598a3-aee4

it is difficult to predict how security provided by the asymmetric cryptography of blockchain may be applied in advance.

The NDARDA should integrate DPBs as an integral part of the research and development agenda so that they can reach their full potential as an open-source tool of innovation, particularly to achieve a higher degree of resilience, protection and cybersecurity in our increasingly online interactions. As the current intermediary laden paradigms of today's internet are restructured, the world will need secure and reliable decentralized blockchains upon which to build solutions.

We are reimagining how value and information can be exchanged and protected on the new "internet of value" freeway. Open source DPBs can provide the rails of a public infrastructure to manifest this new reality while preserving American values of democracy and economic freedom and creating opportunities for financial inclusion and participation.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Digital Asset Holdings, LLC

Central Bank Digital Currency

Principles for Technical Implementation

Response to Federal Office of Science and Technology Policy (OSTP)
Request for Information; Digital Assets Research and Development, Topic 6

From

Digital Asset Holdings, LLC

[redacted]

March 2023

Executive Summary

In response to the Federal Office of Science and Technology Policy (OSTP) Request for Information (RFI) on Digital Assets Research and Development, Topic 6 "Other information that should inform the R&D Agenda," Digital Asset, a smart contract and distributed ledger software technology provider, is pleased to submit this response, which leverages content from its *Central Bank Digital Currency Principles for Technical Implementation*[1], April 2021.

Digital Asset believes that certain principles of Central Bank Digital Currency (CBDC) and key factors should be considered when choosing and implementing a technology to support CBDC, including the following:

- Critical distinctions between CBDC and crypto assets, traditional and digital currency, and tokenization and digitization
- Benefits for the Central Bank, policymakers, consumers, markets, and institutions
- Technology factors to consider prior to CBDC inception
- Why interoperability is critical and must be considered from the start
- Key advances in central bank ledger functionality, such as name-on-register protections, improved B2B settlement mechanisms, and B2C payment options
- Protection of privacy while safeguarding compliance
- Creation of an effective foundation for CBDC with a smart contract application framework and digital ledger

The challenge of creating and implementing CBDC is large and complex, requiring a thoughtful approach and technology solutions that not only address current challenges but also facilitate future innovation and support yet-to-be-known requirements and opportunities. The ability to start small, facilitate wide adoption, evidence controls, and maintain flexibility to maximize growth are essential.

1.0 Introduction

As businesses and the lives of consumers become increasingly digitized, the drive for efficient digital solutions intensifies. New technologies such as smart contracts and distributed ledger solutions could solve long-standing banking and financing challenges, where complex transactions are handled on aging infrastructure using outdated business processes, and with information silos that hinder the ability to swiftly capture and analyze data.

From simple retail payments to sophisticated cross-border institutional transactions, attention is turning to smarter ways to move money quickly, track it carefully and prevent fraud. Central banks are exploring options for upgrading banking and payment technologies while preserving privacy and controls. Government entitlement programs can also be better expedited.

Digital currency offers the potential to address these challenges. This will take more than just establishing the digital currency. It will also be necessary to modernize processes and policies, to ensure that the Central Bank's ledger is equipped to handle, issue, and manage a digital form of currency, and that access to the ledger is defined with rights, permissions, and controls that are necessary to govern currency issuance, distribution, and circulation.

[1] Published with Darrell Duffie, Graduate School of Business, Stanford University, in April 2021. Darrell Duffie received no compensation or other consideration for his collaboration on the white paper.

1.1 Defining Central Bank Digital Currency (CBDC)

A CBDC is a digital form of currency backed by a central bank with legal tender status, meaning it can be used to settle debts or meet financial obligations. Importantly, we largely agree with the Central Bank of Sweden (Section 3.2) February 2021 that CBDC should not be a bearer instrument, in order to ensure that digital payments are between known entities and include Office of Foreign Assets Control (OFAC) checks.

Central banks will generally choose to issue CBDC **in addition** to conventional cash. The Central Bank retains control over the money supply because it would manage CBDC creation and destruction. CBDC should not be forgeable, and its authenticity should be easily verified. It should be efficient to store and easily transferable. Owners should have an expectation of privacy. The Central Bank (issuer or supervisory authority) should be in a position to monitor compliance with anti-money laundering and other legal limits on payments, but privacy should otherwise be protected. Notably, the provider of the technology infrastructure and any entity not party to the transaction should not have access to transaction details, except as expressly authorized by the authorities for compliance purposes and disclosed to users.

Digital currency, unlike cash, is not a bearer instrument and should not be conflated with cryptocurrency (often referred to as tokenization). Cryptocurrencies, because they are freely transferable bearer assets, are ill-suited as CBDCs. A widely available cryptocurrency would run on a public ledger, thus making a substantial amount of data publicly available.

A digital currency supports some key desirable properties for a CBDC:

- Transferable, but with rights that are programmable — allowable actions that can be set by smart contracts.
- Ownership is known and can be restricted to conform with Know Your Customer (KYC), Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and other compliance requirements.
- Data access is controlled; only the participants to a transaction can see the information relevant to them.
- Portable across any ledger, allowing the Central Bank to retain flexibility in terms of capabilities and choice of service providers, in both the short and long term.

Our view is that CBDC should support both retail and wholesale activities, over time. Therefore, for the purposes of this paper, we are not considering private ledgers or fully anonymous solutions because the former would place restrictions on participation, while the latter provides no traceability or opportunity for controls and regulatory oversight.

1.1.1 Required Properties of a CBDC Solution

CBDC must be easy to use but also exchangeable as an element of complex financial transactions. To realize its full potential, a CBDC should have the following properties:

High levels of privacy: A CBDC solution must guarantee fine-grained privacy controls. Transaction details should be accessible on a strict need-to-know basis.

Boundless horizontal scalability: A CBDC solution must be able to cope with an ever-increasing throughput of transactions. This calls for unrestricted horizontal scaling capabilities. The processing of transactions must be highly parallelizable.

Use case extension and integration: Beyond replacing the existing payment infrastructure, it must be possible to seamlessly integrate CBDC into other processes and workflows.

Infrastructure interoperability: Since it is unlikely that different countries will decide on the same infrastructure, a CBDC should interoperate across different technical infrastructures in order to reap the benefits of frictionless FX transactions. But even for domestic payments, the applications integrating into the CBDC ecosystem need not run on the Central Bank's own infrastructure, and should interoperate across commercial banks and payment providers. Therefore, infrastructure interoperability is needed to ensure that the CBDC solution is more than a like-for-like replacement of the existing payment system.

A CBDC with these properties could be utilized in complex transactions such as:

- The purchase and sale of securities, commodities, real estate, and other regulated activities for which ownership rights are restricted and rights, obligations, and exposures must be clear to all participants.
- Transactions for which not all steps or participants are necessarily visible to other participants on the blockchain or ledger (e.g., preventing competitors from viewing an institution's investment activity, or unauthorized persons from viewing an individual's personal financial transactions).
- Transactions for which transparency of ownership is sufficient for the purposes of meeting requirements for KYC, AML, and CFT.
- Activities requiring that records are kept and controlled by regulated entities that are recognized by law and have legal enforcement rights (e.g., property transfers). Similarly, activities for which access to change records or effect transfers must be restricted to appropriate parties only.

In the design and approach to CBDC that we envision, the ability to manage these activities with more controls, nuance, sophistication, and transparency will be critical to public trust and Central Bank oversight.

1.2 Market Drivers for CBDC Exploration

Support for the concept of digital currencies is gaining momentum. Payment-system innovations such as Sweden's prospective e-Krona, China's immensely successful mobile payment services Alipay and WeChat Pay, and China's Digital Currency Electronic Payment System (DC/EP) have captured the attention of experts and non-experts alike. These innovations and the significant frictions associated with conventional bank-railed payments, especially in the United States, have caused many expert commenters to heighten expectations for more efficient payment systems, especially over the prospect of an effective CBDC. Many central banks have responded with CBDC research and development programs, according to BIS surveys, January 2021. Increasingly, the limits of aging, weakly connected information systems are stressed to keep up with compliance demands that involve knowing your customer, being able to prevent unauthorized or fraudulent transactions, and restricting access to funds for bad actors. Investors seek better ways to reduce counterparty risk with trading partners and depositories.

With global supply chains and voluminous wholesale and retail cross-border payments, there are increasing demands for rapid and safe payments. Currently, international transactions and poor payment processes create undue friction in commerce and involve annoyingly high fees for consumers. Settlement risk remains a costly concern. Existing technology constraints necessitate reliance on trusted third parties (e.g., escrow service providers), adding another layer of time, complexity, and expense to cross-border activities.

The global pandemic accelerated digitization. Economic stimulus programs highlighted the need to distribute funds rapidly and, in some cases, to set parameters for the use of funds (e.g., supplemental nutrition assistance, housing, or retraining). Heightened cybersecurity concerns call for improvements in transparency and the ability to embed safeguards.

A CBDC simplifies — and in some cases, removes — these challenges. A well-designed digital currency can be authenticated and tracked, relies on smart contracts to verify transactions, and utilizes complex business logic to address different financial activities. These features reduce and may even remove reliance on third parties, creating additional efficiencies throughout the transaction chain.

1.3 Costs and Benefits of Introducing Digital Currencies

A CBDC is a significant undertaking. The assurance of safety, operational reliability, privacy, and efficient payments are substantial responsibilities. Failures could be costly and could fall at the feet of the Central Bank, impinging on its reputation. The technology implementation of a CBDC should provide the Central Bank with flexibility in how to handle, delegate, or assign such responsibilities. One possible approach would be a two-tier system. In the first tier, the Central Bank provides the system of record for all consumer accounts and positions. In the second tier, the Central Bank delegates authorities to banks and other payment service providers allowing them to offer access and services to their customers, and to perform KYC, AML, and other regulatory requirements.

The object of paramount importance is the single system of record — the Central Bank ledger, with a single golden source of data and the ability for permissioned participants in the CBDC ecosystem to view, access, and act on those data. Critical to this architecture are interoperability capabilities, allowing the different systems of the Central Bank, banks, and other payment service providers to have a common, fully synchronized view of the current state of the Central Bank ledger. Payment service providers, however, are permissioned to view only the essential data regarding their own customers. With these properties — a single system of record and interoperability — the current challenges of duplicated data and constant reconciliations across the separate records of participants can be removed.

Such an approach requires a technology with expressive and fine-grained permission delegations and privacy rules. Models such as the two-tier approach above, as well as hybrids that align broader roles and responsibilities to central banks, become possible. These technology properties allow banks and other payment service providers to act on behalf of their customers on the Central Bank ledger for specific actions, as agreed with their customers. The Central Bank remains the sole issuer and governs the system of record of CBDC positions. The Central Bank sets standards for the use of CBDC (such as interoperability requirements) and could potentially be the regulator of the payment service providers, which could be commercial banks and authorized fintech firms, as is the case with China's DC/EP.

A further concern is the potential impact of a widely used CBDC on commercial banks, which currently have substantial payment and deposit franchises that might suffer adverse impacts. Disruption of existing payment arrangements can be viewed negatively or positively, given weaknesses in the service quality and costs of many bank-railed payment systems.

The main benefits of a CBDC are the prospect of much-improved payment efficiency and increases in financial inclusion. The transfer of money — whether peer to peer, customer to business, business to business, across banks, and potentially internationally — would become more straightforward, faster, and cheaper. This is so mainly because payments would involve fewer intermediate systems and fewer profit-taking service providers along the payment path. CBDC payments would be available instantly, around the clock. The introduction of a CBDC would permit the Central Bank to extend its ledger to a broader group of participants, including under- or un-banked consumers. This can especially improve the welfare of lower income households, who might otherwise have weak access to the economy or suffer from extremely high payment fees.

Users of a CBDC could realize additional benefits:

- More transparency, including real-time payment and account information.
- Reduced depository risk, as Central Bank-issued CBDC would remove consumer concerns about individual bank solvency or limits on bank deposit protections.
- When implemented correctly, improved privacy protections. For example, transactions would not be visible to those involved in preceding or following transfers, except as desired and arranged.

The introduction of CBDC would give businesses the option to settle transactions directly at the Central Bank, allowing access to funds more quickly and easily. Other advantages would include:

Frictionless wholesale payments between counterparties, wherein money is automatically transferred if and only if all steps of the transaction are successful and the conditions of the contract have been met. The result is increased settlement efficiency and certainty.

Enhanced settlement, covering both settlement and lifecycle events, by employing a common data model within or across markets, automated lifecycle events, and mutualized workflows across parties. The result is increased settlement transparency and lower operating cost and risk.

Significant risk reduction for counterparties and depositories, with synchronized protocols guaranteeing that data are reliably shared with entitled parties in real time, accurately. Compliance monitoring and regulatory requirements can be built into the workflows, providing real-time, continuous oversight.

Various Liquidity Saving Mechanisms developed for any anticipated Real-Time Gross Settlement solution can be more easily implemented (such as those proposed by Rodney J. Garratt in *An Application of Shapley Value Cost Allocation to Liquidity Savings Mechanisms*, July 2019).

Some of the advantages of a CBDC can also be achieved with new fast bank-railed payment systems, such as the FedNow system under development in the United States. While this is a clear step forward toward faster and continually available payments, fast payment systems continue to rely mainly on banks for the provision of payment services and to use bank deposits as the medium of payments. Although a fast payment system could potentially increase competition among banks for payment and deposit services, this is not assured. For example, commercial banks would retain the incentive to maintain a "walled garden" around their customers. Moreover, there is not yet much prospect that bank deposits will be redesigned with the "smart" features of digital currencies that we have described and will detail in the next section.

2.0 Designing a Technology Approach for CBDC

Conversations about digital currency often begin at the end, with discussions about potential technology stacks or distributed ledger options. Centralized databases or existing payment rails also come under review, raising important downstream questions of adoption, extension, and interoperability.

Locking into a specific ledger provider restricts new solutions to a particular infrastructure or set of features even before they begin to take shape. This matters because many ledger providers:

- Lack the granular privacy and authorization controls necessary to build critical market infrastructure.
- Cannot seamlessly connect to other ledgers and infrastructures.
- Lack horizontal scalability and set an upper limit on the number of possible transactions.
- Have poor trust properties and cannot effectively deal with malicious participants. To provide security, they are strongly permissioned and "locked down," limiting participation to privileged, vetted users.

These restrictions run against the flexibility required of an effective Central Bank ledger and digital currency.

2.1 Foundational Considerations

Central banks will want to embed flexibility and interoperability from the start. Given the proliferation of infrastructures, interoperability will be critical. If different central banks decide on non-interoperable ledger providers, new technology silos will replace old ones, and large opportunities for efficiencies will be lost.

Any approach should be considered with an eye toward future-proofing: allowing for the broadest possible set of uses and greatest flexibility to expand as opportunities arise. This includes looking downstream to equitable adoption, allowing users to choose how they interact with the CBDC and to avoid commitment to a particular technology.

Key considerations of a ledger implementation include:

- Data integrity. No user or entity is able to change data without the authorization of its owners.
- Sub-transaction level privacy. Data minimization is the maxim. Even within a complex transaction, every entity will have access only to data that they own or are allowed to observe, even if this means that they see only a part of a transaction.
- Ability to model and enforce multi-party agreements. The modeling language should allow custom tailoring, so as to allow the capture of rights and obligations in multi-party agreements.
- Focus on Day 2 operations. Management, deployment, and monitoring, including comprehensive metrics and logs, are necessary for any systemically important market function. Entities operating such infrastructures or utilities must have access to established, 24x7 global support.
- Suitability to scale across multiple data centers. Integration with current SDDC (software-defined data center) infrastructure is necessary to allow for use across public, private, and/or hybrid environments.

Given the potential complexity associated with the deployment of a CBDC, it is likely that most CBDC programs will start small and grow as new adopters come on board or new solutions are identified. Over time, a central bank's needs may change, necessitating a switch of ledger partners or the ability to work across multiple ledger partners.

2.2 The Value a Smart Contract Application Platform Brings to a Central Bank Digital Ledger

The creation of CBDC allows the Central Bank to extend its ledger to a broader group of participants, including consumers who may be under- or un-banked, while still retaining control over the money supply and over who is permissioned to transact on the digital ledger. To be successful, the digital ledger should be implemented using a smart contract application platform that allows rules and permissions to be embedded within the CBDC and facilitates connections with a broad range of technology providers, existing institutions, and infrastructures.

A digital CBDC ledger, running on a smart contract application platform, reduces depository counterparty risk for the consumer, improves business-to-business settlement mechanisms, and modernizes and accelerates domestic and international payment options.

The Daml™, Digital Asset's smart contract application platform, provides the necessary foundation to meet these objectives. With Daml, a provider can develop the underlying business logic once, then run it on multiple infrastructures or even across ledgers. Key features include:

Capacity to create multi-party solutions that transform silos into synchronized networks with guaranteed, consistent data. This allows the provider to focus on its use case, develop functional and non-functional requirements, and test them up front.

The ability to simplify complex workflows across infrastructure(s), eliminating boundaries through integration with either traditional databases or enterprise-scale distributed ledger technology (DLT).

A unique way to model and execute essential interactions, such that business logic is separated from systems code and the language is easy for business experts to understand and technologists to use.

One layer that sits across multiple applications to simplify individual processes. Data are extracted to create a single source of truth that can be used simultaneously across multiple applications, while combining common tasks to create efficiencies.

Built-in capabilities to include agreements, signatories, privacy, rights, and more, with components that are flexible and can be built up-front, added later, or incorporated as discrete modules to be used in certain scenarios. Daml provides the framework to model and establish discrete rights and permissions.

Daml supports a breadth of potential applications of CBDC, giving the Central Bank the flexibility to start with specific use cases and then expand without being constricted by the limitations of a particular ledger provider or infrastructure partner.

2.2.1 Support for Core CBDC Features

Daml's component approach delivers strong, secure data governance, workflow, data modeling protocols, and business interactions.

- Traceability by authority. Daml naturally supports auditing and tracking transactions, storing data and contracts (to the lowest level of identification) along with the history of each transaction. The set of observers of a Daml contract can be customized to allow for more transparency and visibility.
- Closer control of ownership by authority. The authority can control who can hold money at a programmatic level, for example, to comply with restricted lists (e.g., OFAC).
- Transaction safety. For simple or complicated transactions, Daml can establish specific rules for money transfers. The transactions are then executed atomically, so that for a successful transaction, all steps must be successful.
- Interoperability. Using a common language and protocol, Daml would permit a CBDC system to bridge different ledgers and technologies. (See Section 3.2 below.)

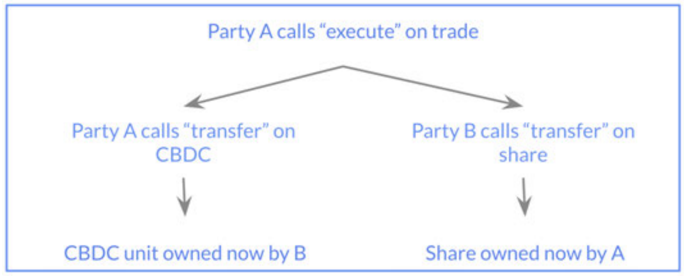
2.2.2 Efficiencies and Safeguards

For the Central Bank, Daml's key features simplify the development of a CBDC and increase efficiency while providing important safeguards and transparency:

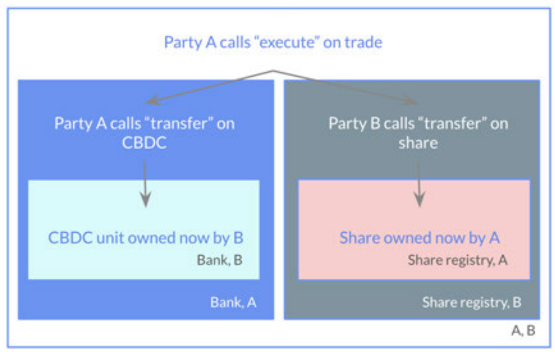
- Common data and processes can be extracted to simplify highly complex, multi-step, multi-party workflows, making it convenient and safe for day-to-day business.
- Rights and obligations are defined and enforced using built-in business roles and fine-grained permissions. This ensures that information is shared with those who need to know it, when they need to act on it.
- Existing legal concepts can be digitized for efficiency, providing additional safeguards.
- Assets are extremely safe with Daml. Developed by cryptography experts, Daml's declarative security model minimizes accidental data leakage, hacks, and break-ins.

Figure 1. Two examples of how Daml smart contracts work within a trade workflow.

Example: Integrating CBDC money in a share-trade workflow between parties. Party A transfers its CBDC money to party B in exchange for shares. The CBDC operator should not be aware of the share transfer, and the share operator should not be aware that the transfer was paid with CBDC.



Example: Different parts of a trade workflow are visible on a need-to-know basis. Each box is labeled with those parties who must be able to see the particular sub-transaction. E.g., the CBDC transfer is not visible to the share registry, share transfer is not visible to the Central Bank, while A and B see the entire transaction.



3.0 Future-Proofing

Given the extensive interactions of central banks with other institutions, individuals, and jurisdictions, a digital currency should freely support financing, trade, and commerce, whether at home or across borders. The necessary level of interoperability requires protocols that can span different technologies, which in turn requires the systems to be able to "speak" to compatible ledgers.

3.1 Daml-driven Interoperability

We believe that seamless and built-in interoperability is the only way for CBDCs to reach their full potential, and that true interoperability includes four key elements:

Multi-ledger technology: The ability to deploy and connect digital currency systems across disparate networks regardless of the underlying IT infrastructure. Top among the challenges is deciding which technology to use — distributed ledger technology (DLT), centralized database, or existing payment rails. Riding on the back of this issue is the requirement for compatibility with other CBDCs, since there will be no single master ledger, and because some CBDCs may not use DLT. Ensuring that a CBDC is compatible with other CBDCs is a critical first step to preventing the CBDC from hitting a dead end in cross-border applications.

Cross-ledger atomicity: If one leg of a transaction fails, all legs fail. By ensuring atomicity, systems can achieve payment versus payment and delivery versus payment without the risk of handing over goods when the payment leg fails and without the need for a central bank to act as an escrow.

Data privacy: Almost all non-Daml blockchains lack the basic properties of privacy, leaking transaction information to the world. Some chains have addressed some of the privacy concerns but lack the ability to guarantee their privacy mechanisms when transacting across chains. A CBDC solution should feature privacy within as well as across ledgers.

Composable extensibility: This property is the ability to dynamically add new applications and to connect to other networks easily. Without composable extensibility, companies will likely reinvent the wheel when future technologies arise or when there is a need to deploy future use cases to the same infrastructure. Since it would be impossible to predetermine all potential uses for CBDC, the design of the currency should allow new uses to be created without requiring changes to the initial implementation. Thus, extensibility is critical to ensuring the ongoing effectiveness of the digital currency.

3.2 Interoperability Using the Canton Protocol

Canton is a scalable, privacy-enabled blockchain for running Daml applications. Canton allows for interaction among different ledger technologies including databases, permissioned or open blockchains, and hardware enclaves.

Canton extends Daml's ability to write a distributed application independent of the platform on which it will eventually run. With Canton, Daml workflows can be run across multiple platforms, making them interoperate even when the original platform owners had not included this capability.

In combination, Daml and Canton solve many of the immediate challenges inherent in creating and mobilizing CBDC, while also leaving the door open to future needs and expansion.

3.3 Canton Features

Daml works with a growing number of major enterprise blockchains as well as centralized databases and other systems. Digital Asset has used its deep knowledge of each of those technologies and their different privacy mechanisms to create Canton. Canton's embedded synchronization guarantees that data are reliably shared only with entitled parties, and in a correct manner, even in the presence of malicious actors.

Canton can be extended without friction to new parties, ledgers, and applications, building on other applications without requiring a central managing entity or global consensus within the network.

Canton offers:

Global composability. Different Daml-based ledger instances can operate using the Canton synchronization protocol.

Data privacy. Canton is built around the principle of data minimization and the right to forget, enabling compliance with laws, regulations, and global standards such as General Data Protection Regulation (GDPR).

Integrity. Canton's synchronization protocol ensures that a participant's ledger remains in a valid state, and that a corrupted state never occurs.

Horizontal scalability. Canton has no upper bound on transaction throughput. The throughput scales linearly with the employed hardware.

4.0 How CBDC Can Foster Efficiency and Innovation

By leveraging a CBDC's structure and functionality, programmable government ledgers can protect data, streamline processes, and reduce fraud, waste, and abuse while simultaneously increasing trust and accountability. Consumers, businesses, and governments can share resources over a secure distributed ledger, mitigating single points of failure and protecting sensitive citizen and government data.

Figure 2. Real-world examples showing potential use cases for CBDC

Government Benefits Balance controls and compliance to help the government set benefit parameters and manage use, and to provide citizens with greater convenience and certainty of receipt *Real-world example: controlled stimulus payments*	**Government Processes** Streamline processes across agencies, with auditable workflows and multi-agency application *Real-world example: budget allocations and contract approvals*
Supply Chain Management Reduce complexity by managing data across multiple (often untrusted) parties, and reducing risk-prone manual paperwork, one up-one down visibility, and long execution times *Real-world example: streamlined procurement and payments*	**Financial Market Resiliency** Enhance the efficiency of and ability to provide oversight on financial market processes *Real-world example: interbank payments*

5.0 Conclusion

The size and scope of financial markets and the high recent rate of flux in payment system design make any discussion of CBDC necessarily complex. Given the myriad challenges and impacts of introducing CBDC, designing such a system calls for prioritizing flexibility and interoperability, allowing use cases to expand over time, and reducing potential limitations on reach or effectiveness. Central banks are properly worried about getting “painted into a corner.” At the same time, security and privacy remain paramount, while allowing authorities to monitor the legality of transactions.

Daml and Canton offer central banks the chance to model and test digital currencies and explore potential use cases, while allowing for the creation of contracts that can be extended and used across one or more ledgers, blockchains, or existing hardware when the time is right. Daml gives central banks the ability to start small and to maintain control while exploring and updating the eventual designs of CBDCs.

Appendices

Technical Details

1. **Ensuring the Central Bank controls the volume of CBDC** with rights and transparent trust relationships that support the creation and destruction of digital currency. Each Daml contract representing CBDC records the party that issues it.

2. **Proving authenticity and making it impossible to counterfeit CBDC**, since each Daml contract has verifiable signatories. Using digital signatures, if each issuer is mentioned in the contract and declared a signatory, no other party can create a contract representing CBDC without the issuer's consent.

3. **Providing transferability, similar to physical cash.** Each owner can be set up for "simplified transfer"," allowing them to exercise that choice only if they say who the receiver should be. Transfers happen atomically, meaning that all steps complete successfully, or none of them do. In a simple transfer:

   a. The old contract is archived, effectively marking it as inactive.

   b. The simplified transfer is executed, creating a new contract where the receiver is the rightful owner of the CBDC.

4. **Supporting (a) consensual ownership and (b) transferability in financial transactions**, to ensure that the money belongs to the owner and the recipient must consent to the transfer. Consent is critical as owning money usually comes with responsibilities, such as taxes. To fix this, the issuer is added as the owner and added to the list of signatories (so it can initiate a transfer). Once the receiving party accepts, all authorizations are collected, and the transfer can be settled. Importantly, each contract can only be used for one transfer, preventing double spending.

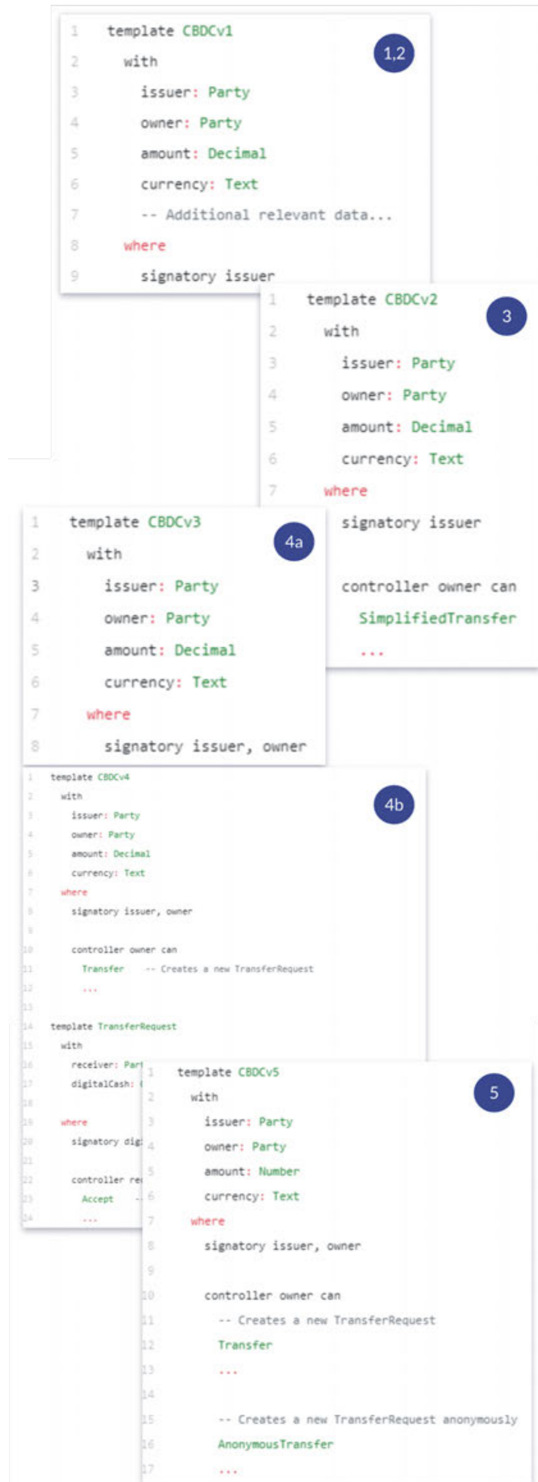
5. **Allowing configurable privacy,** so that the parties to the transaction know only that step of the transaction - not what came before or what will happen next. For example, when you pay for something at a store, the merchant does not know where the money comes from, and you do not know where it will go next. And if you pay in cash, the merchant may not even know the identity of the purchaser. Daml supports privacy with sophisticated modeling:

   a. Visibility rules guarantee that the chain of owners is not disclosed to subsequent owners.

   b. Sub-transaction privacy ensures that parties only see the parts of the transaction in which they participate - even in a complex transaction.

   c. Parties can be promoted to be observers of a contract.

   Where a payer requests a transfer and a receiver accepts it, an "Anonymous Transfer" can be created to protect the privacy of both parties without sacrificing the integrity of the transactions or their permissions. Atomicity ensures that all steps must complete successfully, or the transaction does not take place.



Additional Resources

Digitization and tokenization

Beyond Tokenization **-** Overview of the challenges a tokenized solution would face in supporting complex transactions and how those challenges can be overcome with digital currency and smart contracts. (January 2020)

Interoperability and the Canton protocol

"Central Bank Digital Currencies" Technology Properties: We need Interoperability and More - Discussion of how application composability provides the technology underpinning for atomic settlement, sub-transaction privacy, and security, and how a CBDC system can be extended across participants using the Canton protocol. (July 2020)

Elements of Canton - A short explanation of how Canton works. (February 2020)

Canton Reference Demo - Overview showing what Canton offers in terms of application composability, network interoperability, privacy, and regulatory compliance, and how Canton differs from existing solutions. (2021)

A Structured Semantic Domain for Smart Contracts - Extended abstract that reviews how additional structure yields a more secure programming model for smart contracts and allows for distributed implementations with better confidentiality, privacy, and scalability properties. (April 2019)

Canton: A Private, Scalable and Composable Smart Contract Platform - White paper providing a detailed overview of how Canton implements Daml's built-in models of authorization and privacy while also resolving issues of scalability and interoperability common to other platforms. (February 2020)

Canton Documentation - User information including documentation, tutorials, user manual, and an in-depth review of architecture. (2021)

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

DLT Labs USA Inc.

RFI Response: Digital Assets R&D Agenda

Authors:

Adam Goldstein – Executive Chairman at DLT Labs USA Inc.

Loudon Owen – CEO at DLT Labs USA Inc.

Jovan Maric – Solution Architect at DLT Labs USA Inc.

Respondent Type:

Members of the Public on behalf of DLT Labs USA Inc. - a Blockchain and DLT Product Company

DLT Labs USA Inc. has vast experience in developing and deploying full-spectrum Distributed Ledger Technology products and solutions in more than 50 blockchain-centric projects and across various industries including supply chain and logistics, as well as financial services, and cites its Walmart deployment as evidence of its expertise in the realm of Blockchain and Distributed Ledger Technologies. We are currently working on directly analogous/applicable products and solutions with Walmart (under NDA).

DLT Labs' experience includes delivering **the world's largest industrial blockchain deployment** to the world's largest revenue company and its business partners as a hybrid (cloud and on-premises) solution. Importantly, this unique capability, experience and expertise is directly applicable to provide information and support the Federal Government's objectives. Our team comprises one of the world's largest pools of highly experienced enterprise blockchain experts. We believe our depth of understanding and range of expertise is unparalleled.

Our commitment to professionalism across the industry is reflected by training over 2,000 students at AKG Engineering College annually in blockchain and related software technologies. Among its wide range of industry affiliations: DLT Labs has a Strategic Agreement with Mastercard, is a contributor on the Forbes Technology Council, technology advisor to numerous organizations (e.g. BiTA - Blockchain in Transport Alliance, and MOBI – Mobility Open Blockchain Initiative) and an active partner and contributor to the Hyperledger Foundation.

QUALIFICATIONS

Evidence of best-in-class provider of relevant technology or service — qualitative and quantitative.

To our knowledge, DLT Labs is the only company with a proven blockchain-enabled data platform deployed at scale in both enterprise and governmental sectors, including the largest enterprise blockchain deployment globally.

DL Asset Track™ is an award-winning enterprise solution for data standardization and contract management which helps improve data quality, traceability, and security. DL Asset Track™ is designed and developed using DLT Labs' unique DNC1 architecture framework which guarantees high throughput and low latency in a distributed environment.

Our Customers

DLT solutions are growing rapidly and have already been deployed at more than 100 enterprise accounts worldwide in retail supply chain (Fortune #1 Walmart and its network of carriers and suppliers – for example Pepsi, Coke, Nestle, Unilever, Bison Transport, P&G, CH Robinson, JD Hunt, Uber and many others); resource sector logistics (Teck Resources); and in aviation fuel management (Bangkok Aviation Fuel Services).

In addition, we have had the honor of being cited in various articles and publications, including Harvard Business Review: How Walmart Canada Uses Blockchain to Solve Supply Chain Challenges. We are also a proud recipient of numerous awards including the 2021 Accenture Freight & Logistics Innovator Award for North America, the 2020 ICMG Architecture Excellence Awards, and CSCMP Supply Chain Innovation Award, but all this culminates with the testimonials received from our clientele.

What DLT Customers Are Saying…

DLT is a uniquely positioned and proven solution in the market, but don't just take our word for it. Here are some comments provided by DLT customers.

"Blockchain is enabling a material advance in our smart transportation network, with expedited payments, extensive cost savings and other benefits among our supply chain." **VP of Transportation, Walmart Canada**

"I think this solution has the potential for being a big game changer for supply chains across the industry. We have hundreds of customers. When I see the improvement that we have seen in terms of the cleanliness of the account and the timeliness of the payments, if I had all of my accounts in such good shape, I would be in a very happy mood." **VP Finance and Administration, Bison Transport Inc.**

"I would really, really love to see the industry and other companies adopt DL Freight as their standard and the reason is simple: it creates a lot of efficiencies, and it simplifies the billing and payment process… But what it really does is help with out cashflow and cash is king! With better cashflow we can expand our capacity to carry more loads." **CFO, Titanium Transportation**

"The platform has opened up a tremendous amount of opportunity to track and aggregate information that had been disparate around our transportation business: for example, we can now integrate TMS information, and important temperature and other readings from our IoT partners (Fourkites), which confirm on time at stores, vehicle turn time, use time. It is all now in one place as part of the record of that transaction, so we have the opportunity to identify patterns and save millions of dollars in waste. This brings this all together into one ledger that originally was a payment platform, but we are using it much more as an information platform to give us insight on how we run our business." **EVP, Transformation Officer, Walmart Canada**

Successful Projects

Walmart and its network of suppliers and transportation partners

Fortune #1, Walmart is the largest retailer in the world operating approximately 10,500 stores and clubs in 24 countries and eCommerce websites. Walmart Canada was established in 1994 through the acquisition of the Woolco chain and has grown to more than 400 stores nationwide serving more than 1.2 million customers every day. Walmart Canada's flagship online store, Walmart.ca is visited by 750,000 customers daily. With more than 85,000 associates, Walmart Canada is one of Canada's largest employers and is ranked as one of the country's top 10 influential brands.

Walmart's Initial Challenge

Walmart places enormous value on its partnerships with third-party transportation carriers. However, these relationships were at a crisis point. There were disputes in over 70% of invoices from its carriers, and its largest carrier was actively discussing withdrawing services. Walmart and its carriers were unable to effectively reconcile conflicting information and calculations. They each work with multiple systems to account for expenses and track shipment data funneling in from each trailer, railcar, or ship and these different systems are largely incompatible. They faced the classic challenge of working in silos, and despite a host of initiatives they had tried, were unable to resolve it. Each load delivered has extensive associated data regarding load costs, carrier details, and tracking information that amount to approximately 220+ data points per load. All this data needs to be reconciled before an invoice can be approved.

With more than 550,000 loads moving across the country each year, the volume of information that needs to be managed and accounted for is staggering.

DLT worked with Walmart and its largest carrier (Bison Transport) to solve the root cause of invoice disputes. Interestingly, Walmart approached this project on a virtually identical project management basis as outlined in this RFP and continued to be closely involved in a leadership role throughout.

DLT implemented its data management platform based on distributed ledger technology. Information from each source, including Walmart, each carrier and all IoT data, was ingested into DLT's platform, synchronized throughout each transaction from start to finish, and the calculation of the invoice was automated by smart contracts and by drawing data from Master Tables. Instead of waiting for the proof of delivery and invoice generation, then working backwards, there was a continuous synchronization of data from the outset resulting in a single source of truth for each party. Any disputes that arose from manual intervention or any form of error are immediately communicated to both sides, and typically resolved in hours, in contrast to weeks or months (and sometimes never) previously.

In effect, each invoice generated on the platform is an NFT (Non-Fungible Token), representing both any dollar amount as well as time (when the invoice total is fully recognized). With $1.5 billion represented on the platform, this is the largest commercial b2b NFT platform. If CBDCs are Central Bank Digital Currencies, DLT has in effect created a CADC, a Central Authority Digital Currency, where the calculation of the invoice is done fully on blockchain, which has allowed Walmart to diminish (and effectively replace) the traditional invoice audit function.

Below are examples of the DLT solution outcome:

- 89% improvement in data quality
- 97% reduction in invoice disputes (from $350M annual to <$5M, now resolved in hours/days)
- $30M annual savings (6% annual freight spend)
- 250+ CRs/ERs with no downtime
- $1.5 billion processed on the platform

Teck Resources Limited (Teck)

A globally diversified mining and mineral development company, with production focused on steelmaking coal, copper, zinc, and energy. Teck revenues exceed $10 billion. And it is a leader in sustainability and technical advances within the mining industry. Teck has a sustainability goal to develop and implement a "product passport" - a responsible producer program that is traceable through the value chain - by 2025.

Teck engaged DLT to configure its DL Asset Track™ platform to provide provenance and visibility for their end-to-end sourcing, refining, and manufacturing process. The solution leverages the use of distributed ledger technology to:

- Capture Germanium attributes at each of the designated touchpoints along the chain of custody, through manual and/or electronic inputs.
- Provide a single shared version of truth between multiple business process participants (internal and external to Teck Resources).
- Provide immutable data to stakeholders (internal & external) based on a user's role within the supply chain.
- Demonstrate adaptability and scalability of the solution for other Teck products o Incorporate into the pilot data of various formats, and methods of input not covered with Germanium.

Germanium Provenance Challenges include:

- Lack of end-to-end identification as to who is operating the mines where raw materials originate, and who is involved across the supply chain.
- Lack of visibility into the supply chain from the various Zinc origin mines, to concentrate suppliers and Teck's Trail Operations.
- Unable to share with customers in an auditable, verifiable way that the Trail Operations are meeting the required responsible standards.
- Unable to share with customers in an auditable, verifiable way that they are sourcing their Zinc from responsible mines.
- Unable to lot track concentrates entirely due to the co-mingling of lots while concentrates are being stored.

The Outcome

As the project evolved, Teck requested extensive expansion of the platform's capability, and the result is a comprehensive resource management platform that can be used among Teck and its business partners both to optimize operations and satisfy Teck's Product Passport ESG objectives.

- Roughly 20,000 lots per year – this is over the span of 2 mines.
- 20 – 30 mt (megatonne) of germanium concentrate.
- 400 kmt (kilometer-tonne) of germanium concentrate from the first onboarded mine.
- Work towards disposing zero industrial waste by 2040.
- Reduce the carbon intensity of operations by 33% by 2030.
- Procure 50% of electricity demands from clean energy by 2025, and 100% by 2030.

Strategic Partnerships

Mastercard, Transcard

Mastercard and Transcard have partnered with DLT Labs in launching **FreightX**, a Global Freight Payment Network.[1]

FreightX is an industry-first solution that allows all the parties involved in freight processing to share information via a secure digital ledger. The solution was designed for any shipper, broker, or carrier in over-the-road haulage in the United States. Over time, FreightX will be available worldwide.[2]

The seamless connection of data orchestration from payments to financing shows the potential power of a digital currency by improving efficiency and visibility throughout supply chains. This gives lenders a real time view of the transactions they are financing, and operators multiple new opportunities to finance their working capital.

FreightX uses advanced technology to overcome the challenges of freight processing:

- Digitally connects shippers, brokers, carriers, and other parties via a distributed ledger.
- Uses smart contracts to manage business rules in real-time.
- Automatically updates invoices based on events in the field, as they happen.
- Embeds payments and financing in freight processing for faster, frictionless cash flows.
- Reconciles payments in real-time with a carrier's ERP, TMS or system of record.

FreightX was designed for shippers who struggle with back-and-forth emails and phone calls with carriers trying to resolve disputes and are tired of paying third-party services to audit invoices.

FreightX helps shippers:

- Improve control of freight spend.
- Reduce the need for costly third-party audit services.
- Eliminate carrier conflicts over invoice disputes.
- Protect customer relationships through stronger carrier relationships.
- Better utilize their existing infrastructure.

With FreightX, carriers:

- Virtually eliminate invoice disputes.
- Streamline their back-office processes.
- Accelerate cash flow without paying punitive fees.
- Strengthen relationships with shippers.

[1] https://www.dltlabs.com/news/transcard-dlt-labs-and-mastercard-team-up-to-launch-freightx-a-gamechanging-digital-freight-processing-solution-147068
[2] https://blog.transcard.com/collaboration-between-transcard-mastercard-and-dlt-labs-is-driving-new-efficiencies-in-freight-processing

Japan International Cooperation Agency (JICA), Deloitte Tohmatsu

Data Collection Survey on the Prevention of Child Labor in Côte d'Ivoire Using Blockchain Technology

Since the 1970s, child labor has been banned by various international treaties and SDG Target 8.7 calls for the eradication of child labor in all its forms by 2025. Although the number of child laborers is on the decline thanks to efforts by the international community, 152 million children—9.6% of all children worldwide—are working as child laborers.[3]

In the course of demonstrating the PoC, we created three app systems: a farmers' group app, a school app and a CLMRS [Child Labor Monitoring & Remediation System] verification app.

The farmers' group app is equipped with a function that enables farmers to check points acquired, a function that enables cooperatives to check certificates acquired and a function that enables users to report and check information about the work attendance of children working on farms (hours worked, nature of labor).

The school app is equipped with functions that enable teachers to check points acquired and report and check information about children's school attendance.

The CLMRS app is equipped with a function that enables users to check the results of comparisons of information about children and, if there are inconsistencies, to update the information after conducting audits; and a function for checking children who have engaged in hazardous labor and farmers' groups and schools that are not reporting information.

The system is configured based on DL Asset Track, a blockchain platform provided by DLT Labs. Data input into the app (e.g. information about work/school attendance, records of points, certificates) is stored on a blockchain platform (Hyperledger Fabric), but personal information (e.g. children's names) are managed offchain (RDB) to fulfill the standards set out in the guidelines of the General Data Protection Regulation (GDPR).[4]

[The survey] aim[s] to verify the viability of bringing appropriate stakeholders on board and obtaining accurate insights into child labor through a traceability system, by way of a demonstration experiment.[5]

Before the PoC, children worked an average of 17 hours per week during the harvesting season and other busy times and an average of five hours per week during other times. In contrast, during the PoC, children worked an average of five hours per week. Given that the PoC took place during the cocoa harvesting season, the PoC had the effect of reducing child labor by 12 hours per week. Although the PoC did not eradicate child labor, it did have a noticeable effect on it.[6]

---

[3] https://openjicareport.jica.go.jp/pdf/12368809.pdf Page 8
[4] https://openjicareport.jica.go.jp/pdf/12368809.pdf Page 66
[5] https://openjicareport.jica.go.jp/pdf/12368809.pdf Page 16
[6] https://openjicareport.jica.go.jp/pdf/12368809.pdf Page 81

Goals, sectors, or applications that could be improved with digital assets and related technologies.

1. Reduce the cost of transactions: CBDCs reduce the cost of transactions by eliminating intermediaries which reduces the time, cost, and unpredictability (it is not always possible to determine how many intermediaries involved in a transaction) associated with processing payments. CBDCs can also reduce the cost of cross-border transactions by eliminating the need for currency exchange and reducing the fees associated with international wire transfers.

2. Increase monetary policy effectiveness: CBDCs can allow central banks to implement monetary policy more effectively by providing them with real-time data on the money supply, allowing them to control and monitor the flow of money more precisely. This can help central banks to make informed economic decisions to, for example, respond to economic crises more rapidly, or manage inflation.

3. Improve transparency and reduce fraud: CBDCs are traceable and transparent, which can help prevent fraud and money laundering. The use of blockchain technology can also ensure that transactions are recorded in a secure and tamper-proof manner, providing greater transparency and payment system integrity.

4. Increase financial inclusion: CBDCs can provide access to banking services for unbanked and underbanked individuals, including those in remote or low-income areas. CBDCs can provide a low-cost and easy-to-use alternative to traditional bank accounts, allowing people to participate in the economy and access financial services that were previously unavailable to them.
    a. For instance, physical cards or mobile apps can be issued that enable quick and cost-effective p2p digital transactions in place of traditional cash transactions.
    b. Social security programs can also be distributed relatively easily and affordably using CBDCs.

5. Maintain competitiveness: CBDCs can help countries maintain their competitiveness in the global economy by providing a modern and efficient payment system that can compete with other digital payment systems. Many countries are at the very least exploring adopting CBDCs. China, for instance, has launched e-CNY as of 2022, with many other countries exploring the technology.
    a. Improving payment systems: CBDCs can help to modernize the US payment system. By providing a fast, secure, and efficient payment system, CBDCs can help the US to compete with other countries that are investing in digital payment technologies.
    b. Promoting innovation: CBDCs can stimulate innovation in the financial sector by providing a platform for new financial products and services, like what we've achieved with Walmart, launched alongside CBDCs. This will help to attract investment and talent to the US, which can enhance its competitiveness in the global economy.

6. An example:
   a. In a CADC/CBDC-powered economy, the issuing authority has greater power over the asset (what can it be spent towards?)
   b. In the case of social services, for instance, money can be dispensed to a user, with limitations on what it can be spent on. For instance, government aid funds can only be spent on food, shelter, and other essential goods/services, subject to political, legal, and social controls.
   c. This enables an increased degree of trust and good conduct in society and ensures that funds that are being dispensed are used for their intended purpose.

Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

1. The environmental impact of Blockchain-based digital assets has been a common concern, but is largely specific to Bitcoin due to the “Consensus Mechanism” employed to guarantee transactions are legitimate (called Proof of Work)
    a. One study went so far as to say that Bitcoin “Mining” (the “Work” in “Proof of Work”) could rival Crude Oil in environmental impact[7].

2. This estimate, however, only applies to Bitcoin and other Blockchain platforms using Proof of Work as their Consensus Mechanism.
    a. Ethereum, the second most popular Blockchain platform has switched to using “Proof of Stake” as their Consensus Mechanism, which is estimated to use ~99.95% less energy than Proof of Work[8].

3. Proof of Work and Proof of Stake are Consensus Mechanisms used in what are known as “Public Blockchain Platforms”, where anyone can join the Blockchain network, and participate in the reading, writing, and validating of transactions. All users are equal in such an arrangement.
    a. PoW and PoS are designed to financially discourage bad actors from writing and approving fraudulent transactions to the ledger, given that anyone can join and participate.

4. A CBDC launched by the Federal Government will not run on a “Public Network”, but rather, a “Private, Permissioned Network”, where reading, writing, and validating transactions will be the responsibility of a few pre-defined users or computer systems.
    a. This allows the use of “Consensus Mechanisms” that are significantly less power hungry, such as “Proof of Authority”, where users or organizations are explicitly given the authority to validate a transaction.
    b. The IMF suggests that CBDC transactions may even be more cost-effective and environmentally friendly than even typical Credit Card transactions[9].

5. That said, a fully digital US Currency will need to stand up to the highest levels of cyber security scrutiny to avoid counterfeiting, fraud, double-spending, DOS attacks, etc.
    a. For instance, today, if credit card systems are down, physical cash is always an acceptable form of payment. In a digital economy, CBDC systems need to be fully distributed and secure to avoid any downtime or other issues.

---

[7] Jones, B.A., Goodkind, A.L. & Berrens, R.P. Economic estimation of Bitcoin mining’s climate damages demonstrates closer resemblance to digital crude than digital gold. Sci Rep 12, 14512 (2022). https://doi.org/10.1038/s41598-022-18686-8

[8] https://blog.ethereum.org/2021/05/18/country-power-no-more

[9] https://www.imf.org/en/Blogs/Articles/2022/06/16/how-crypto-and-cbdcs-can-use-less-energy-than-existing-payment-systems

Other information that should inform the R&D Agenda.

Ultimately, the largest major benefit to adopting a National Digital Asset would be the development and adoption of supporting applications using this proposed Digital Asset as a basis.

At DLT Labs, we have built an ecosystem that provides a practical platform for any form of payment (transitional, multimodal, etc.) that enables trust and reliability. With Walmart, we have built (at scale) all the requisite building blocks in the form of a CADC (Central Authority Digital Currency) to enable the introduction and evolution of a CBDC implementation that eliminates risk.

This, we believe, will be crucial in the development of governance and operations in American trade and commerce. In our discussions with top 3 US banks, we have outlined that the core technology is identical to what would be powering CBDCs and stands up to bank-level security standards.

In the best case scenario, a successful adoption of CBDCs alongside supporting applications can turbocharge industry savings, saving 50%-80% on operating costs (as we've seen in the Freight industry).

In the worst case, a CBDC launched in isolation will have little to no impact, and struggle with adoption, as seen for instance with China's e-CNY CBDC.

DLT Labs has proven how to represent value in the form of NFTs issued by a central authority, with embedded finance inside the asset. DLT has married financial services under the umbrella of a CADC/CBDC by integrating digital assets with data transparency. The lack of integrability in attempts to fully digitize currency have failed and will fail.

It is our belief that the highest and best use of our technology can be delivered in a simple and viable manner expected to be adopted and deployed in a parallel with CBDCs, and we will continue to strive to be at the forefront of a fully digital economy.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Dorae Inc.

3 March 2023

RFI Response: Digital Assets R&D Agenda

Name of Submitter: Aba Schubert
Submitting Organization: Dorae Inc.
Respondent Type: Industry (technology company)

Dear Ladies and Gentlemen,

Below kindly find our response to your request for information. We are grateful for the opportunity to share our views and remain at your disposal if we can be of further service.

1. *Goals, sectors, or applications that could be improved with digital assets and related technologies:*

Digital assets in the form of CBDCs could dramatically improve transaction processing in the global trade space. In particular, in circumstances where international trade transactions are denominated USD, payment processing and settlement time can be significant, often requiring the use of letters of credit. These processes in turn often lead to complex documentary requirements. Prolonged payment settlement cycles directly increase the working capital requirements of trade participants, eroding their margins and competitiveness.

This already disadvantages USD transactions compared to Euro denominated transactions where the entire transaction can be completed within the SEPA system, and efforts such as E-CNY and the Pan African Payment and Settlement System aim to achieve meaningfully improved settlement speeds.

In the event that adoption of a U.S. CBDC could shorten international payment settlement cycles dramatically as compared to SWIFT, this would support continued preference for USD in many major and strategically important categories of goods, such as energy, industrial commodities and consumer goods, thus supporting global demand for USD and the Treasury market, and enabling continued U.S. policy influence.

It is also noteworthy that dollar shortages of national central banks in certain emerging and frontier markets continue to arise not from payment imbalances, but rather from the need to restrict USD transactions for compliance purposes. This "blunt instrument" enforcement can have geopolitically disadvantageous consequences, in the form of a shift away from USD denominated trade. For example, we noted with interest the recent announcement of Iraq's central bank that it will allow trade with China to be settled directly in CNY.

To the extent that adoption of U.S. CBDC is implemented in a manner that increases audit trail robustness in USD denominated international transactions, it can lead to refined processes in areas such as sanctions enforcement and anti-money laundering compliance in a manner that moderates dollar shortages and thus decreases the shift away from USD observed in associated markets.

4. *R&D that should be prioritized for digital assets:*

Advance implementation planning to ensure that a U.S. CBDC does not disenfranchise the incumbent banking system is important to support Policy Objectives 1 (Provide benefits and mitigate risks for consumers, investors, and businesses), 2 (Promote economic growth and financial stability and mitigate systemic risk) and 4 (Promote economic growth and financial stability and mitigate systemic risk).

Such implementation planning should comprise both technical and regulatory workstreams, spanning from studies of how implementation of digital asset enabling infrastructure, such as decentralised identities and verifiable credentials, can be integrated with existing core banking systems, to providing a clear regulatory framework for CBDC payment processing providers that yields operational consistency with existing rules.

6. *Other information that should inform the R&D Agenda:*

Adoption of a U.S. CBDC would facilitate trade finance in the manner described in item 1, above. This can be amplified by the integration of CBDC payment systems into a broader trade digitalization agenda.

The harmonization and digitalization of links along supply chains and trade routes can yield rich data sets that are akin to 'digital assets' in the sense they comprise a repository of useful information about goods, which information is effectively a digital twin that must be shared in part with some stakeholders, in entirety with others and subject to creation by multiple orchestrated stakeholders.

This harmonization can be achieved through a coordinated effort to advance standardization of information requirements (e.g., hazardous materials disclosure requirements), data format standards and user-facing utilities that enable industry "self-service" to the greatest extent possible.

The information arising from this next generation of trade data can yield (a) better structured data sets (enabling more powerful analysis), (b) increased ability to detect customs fraud, (c) better understanding of domestic and international trade flows and (d) opportunity for increased automation (for example, to enable automated scrutiny of areas such as shipments below the $800 threshold, which have grown to significant levels in recent years).

Sincerely,

____

DORÆ INC.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Earthjustice, Environmental Working Group, Sierra Club, and Greenpeace.

March 3, 2023

Office of Science & Technology Policy
Eisenhower Executive Office Building
[redacted]
Submitted electronically via DARD-FTAC-RFI@nitrd.gov

Re: Request for Information: Digital Assets Research and Development

Thank you for the opportunity to provide comments on your Request for Information ("RFI") on the Digital Assets Research and Development Agenda, 88 Fed. Reg. 5043 (Jan. 26, 2023). Please accept these comments on behalf of Earthjustice, Environmental Working Group, Sierra Club, and Greenpeace.

Building upon on the OSTP's groundbreaking report about the climate and energy implications of proof-of-work crypto-assets,[1] Ethereum's decrease in energy consumption by 99.95% due to its merge from a proof-of-work consensus mechanism to proof-of stake,[2] and Earthjustice and Sierra Club's report on the environmental impacts of proof-of-work crypto-asset mining,[3] it is crucial that the Biden administration incorporate meaningful and comprehensive research and development activities to fully document the past, present, and future impacts that the energy-intensive, energy-wasteful proof-of-work crypto-asset mining industry have on the Biden administration's climate and clean energy goals, ratepayers, communities, and environmental justice.

While the undersigned organizations generally support the creation of a National Digital Assets Research and Development Agenda, we are concerned that this agenda will leave open the possibility of support for digital assets, including proof-of-work crypto-assets, without the scrutiny they should be receiving due to their real-time climate and energy implications – especially considering the current track record – and the industry's rampant greenwashing and misleading statements.[4] We appreciate that the RFI does offer that "some digital assets can consume a lot of energy," and that digital assets introduce risks or harms, direct or indirect, on communities and the environment. In our response, we outline key questions that the Biden administration should incorporate into its National Digital Assets Research and Development Agenda. If the Biden administration is to stay the course on its goals to combat the climate crisis and advance environmental justice by cutting U.S. greenhouse gas pollution by 50–52% below 2005 levels by 2030 and a net-zero emissions economy by 2050, then the administration needs to take full account of the climate, energy, and environmental challenges associated with digital assets, in particular proof-of-work crypto-assets like Bitcoin and Dogecoin, among others.

---

[1] White House, *FACT SHEET: Climate and Energy Implications of Crypto-Assets in the United States*, Office of Science and Technology Policy (Sept. 8, 2022), https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/.

[2] Ethereum Foundation, *The Merge*, https://ethereum.org/en/upgrades/merge/ ("The Merge reduced Ethereum's energy consumption by ~99.95%.").

[3] Earthjustice & Sierra Club, *The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now* (Sept. 2022), https://earthjustice.org/feature/cryptocurrency-mining-environmental-impacts.

[4] *See, e.g.*, Earthjustice & Sierra Club, *The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now*, at Section VIII: Breaking Through the Bitcoin Myths (Sept. 2022), https://earthjustice.org/feature/cryptocurrency-mining-environmental-impacts; Kaylee Tornay, *Can crypto mining go green? Critics are skeptical*, Grist (Feb. 18, 2023), https://grist.org/climate-energy/can-crypto-mining-go-green-critics-are-skeptical/; Andrew R. Chow, *Fact-Checking 8 Claims About Crypto's Climate Impact*, Time (July 1, 2022), https://time.com/6193004/crypto-climate-impact-facts/.

2. Goals, sectors, or applications where digital assets introduces risks or harms.

The explosive growth of crypto-asset mining in the United States is impacting utilities, energy systems, emissions, communities, and ratepayers in real-time. Crypto-asset mining is an extremely energy-intensive process that threatens the ability of governments across the globe to reduce our dependence on climate-warming fossil fuels. If we do not take action to limit this growing industry now, we will not meet the goals set forth by the Paris Agreement and the Intergovernmental Panel on Climate Change to limit warning to 2°C. Because these operations operate 24/7/365, and are designed to consume enormous quantities of energy, they increase demand for fossil fuel operations – increasing local air, water, and noise pollution, increasing costs on others, and increasing climate pollution at a time when we should be doing everything in our power to move in the opposition direction to mitigate the worst impacts of the climate crisis.

In the year prior to July 2022, Bitcoin consumed an estimated 36 billion kilowatt-hours (kWh) of electricity, as much as all of the electricity consumed in Maine, New Hampshire, Vermont, and Rhode Island put together in that same time period. Top-down estimates of the electricity consumption of cryptocurrency mining in the United States imply that the industry was responsible for an excess 27.4 million tons of carbon dioxide (CO_2) between mid-2021 and 2022 — or three times as much as emitted by the largest coal plant in the U.S. in 2021.[5]

The past two years have demonstrated that the industry preferentially seeks readily-available energy and minimal regulation, re-starting defunct coal and gas plants, flooding the restructured electricity market in Texas, and tapping into rural power grids where regulators have little oversight. This explosive growth strains energy grids, raises retail electricity rates, and increases total carbon emissions and local air pollution.

For a full documentation of proof-of-work crypto-asset mining's on-the-ground impacts for communities, ratepayers, and the environment, please reference Earthjustice and Sierra Club's report on "The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now," attached as Attachment A. Additionally, please reference Attachment B, which compiles our responses to last year's RFI by OSTP on the Energy and Climate Implications of Digital Assets, which informed the agency's groundbreaking report on the "Climate and Energy Implications of Crypto-Assets in the United States."

4. R&D that should be prioritized for digital assets. The federal government must include climate, energy, environmental, community, ratepayer, and noise pollution impacts of digital assets in its R&D agenda – not just as an aside, but integral to the administration's efforts to research digital assets while advancing the administration's climate, clean energy, and environmental justice goals. Below, we offer a list of questions related to the climate, energy, environmental, community, and ratepayer impacts of proof-of-work crypto-asset mining that OSTP should prioritize in its R&D agenda.

- How would a complete moratorium on proof-of-work crypto-asset mining lead to better outcomes of the Biden administration's climate, clean energy, and environmental justice goals?
- What are the marginal increases of CO_2 emissions due to current, expected, and project load on grids across the United States, in particular crypto-asset mining heavy states like Kentucky and Texas, due to increased demand in fossil fuel electricity generation?

---

[5] Earthjustice & Sierra Club, *The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now*, at 13 (Sept. 2022), https://earthjustice.org/feature/cryptocurrency-mining-environmental-impacts.

- What are the ratepayer implications of crypto-asset mining, at the national, regional, state, and local level?
- How do power purchase agreements between crypto-asset miners and power plants or utilities exacerbate dependence on fossil fuel generation?
- What are the downsides to what the RFI is referring to as "environmentally-friendly consensus mechanisms," and any related use-case such as those touted for carbon credit and carbon offset schemes, which are well-documented to not lead to any meaningful climate impact? Further, any proof-of-work consensus mechanism is inherently energy-intensive and energy-wasteful, and therefore, not environmental-friendly or compatible. Thus, the federal government should not invest R&D funding to any proof-of-work consensus mechanisms – while also evaluating in full the environmental, energy, and climate costs and benefits of any consensus mechanism.
- What are the implications for plugging and cleaning up orphaned and abandoned oil and gas wells, and for the Biden administration's methane reduction goals, if energy-intensive, energy-wasteful crypto-miners are allowed to combust fossil gas at orphaned and abandoned oil and gas wells?
- How much economic development dollars and tax incentives have proof-of-work crypto-asset miners received at the federal, state, and local level? What are the economic implications, costs, and benefits of these incentives on residents and state and local government, considering the lack of jobs at facilities?
- Could Inflation Reduction Act funds be utilized by crypto-miners in a climate-negative manner?[6]
- How can utilities and utility regulators ensure that speculative mining operations do not leave a trail of stranded assets and ensure that mining facilities do not increase electricity or capacity costs for existing customers?
- How are grid operators studying the impact of crypto-asset mining on congestion, resource adequacy, and wholesale market prices? What gaps exist from grid operators being able to plan for massive load posed by proof-of-work crypto-asset mining, while also transitioning to clean energy resources?

Thank you for the opportunity to submit these comments and for your attention to this issue. Please do not hesitate to contact us for any follow-up questions. Sincerely,

Earthjustice

Environmental Working Group

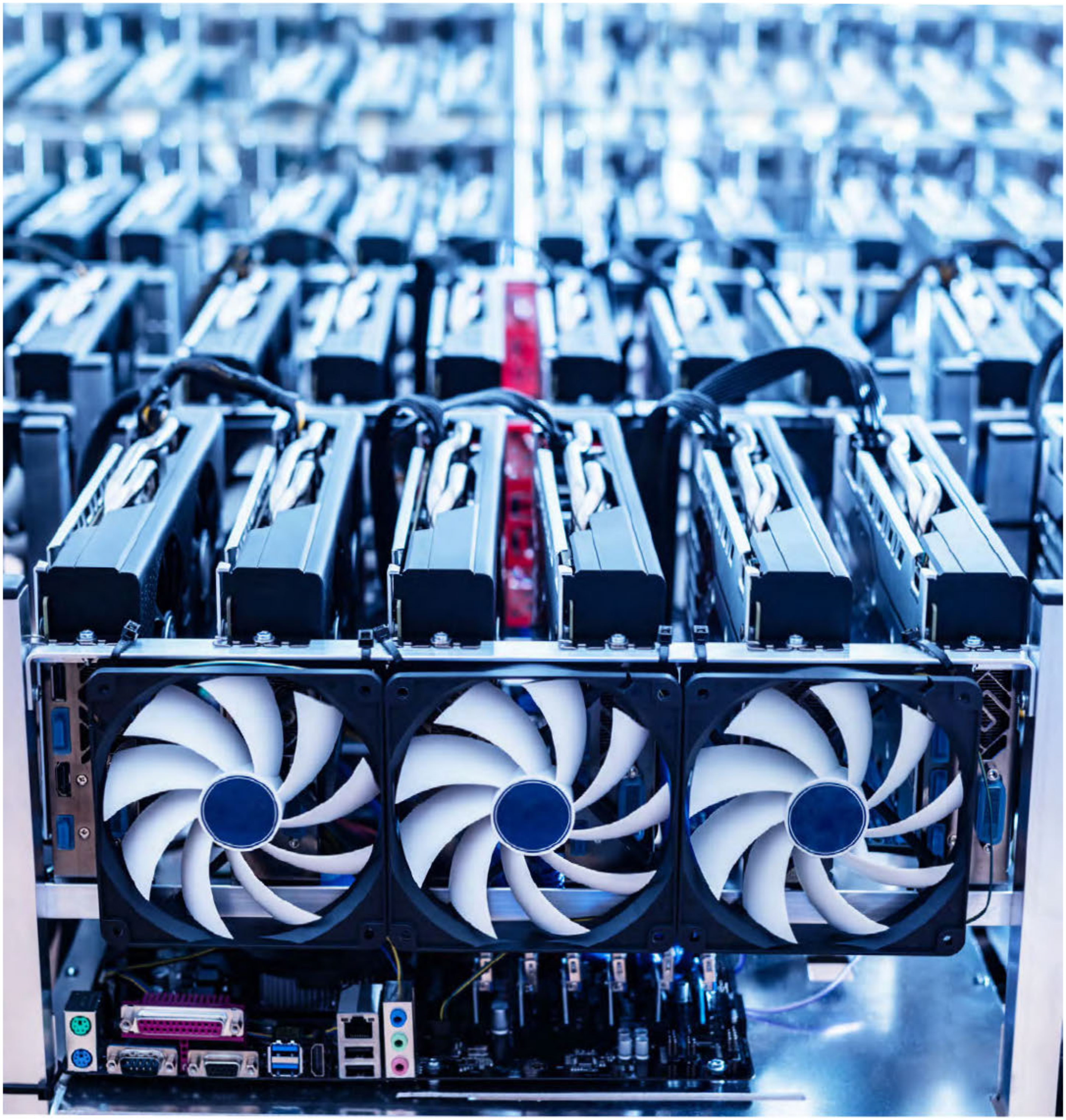
Sierra Club

Greenpeace

[6] *See, e.g.*, Brady Dale, *Crypto mining advocate sees green business in abandoned gas wells*, Axios (Jan. 27, 2023), https://www.axios.com/2023/01/27/crypto-mining-advocate-green-abandoned-gas-wells.

Attachment A

Earthjustice & Sierra Club, *The Energy Bomb: How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now* (Sept. 2022)



THE ENERGY BOMB

How Proof-of-Work Cryptocurrency Mining Worsens the Climate Crisis and Harms Communities Now

SIERRA CLUB

EARTHJUSTICE
BECAUSE THE EARTH NEEDS A GOOD LAWYER

September 2022

Mandy DeRoche, Deputy Managing Attorney,
Clean Energy Program, Earthjustice

Jeremy Fisher, Senior Advisor for Strategic Research and
Development, Environmental Law Program, Sierra Club

Nick Thorpe, Climate & Energy Senior
Program Associate, Earthjustice

Megan Wachspress, Staff Attorney,
Environmental Law Program, Sierra Club

Suggested citation: DeRoche, M., Fisher, J., Thorpe, N., and
Wachspress, M., *The Energy Bomb: How Proof-of-Work
Cryptocurrency Mining Worsens the Climate Crisis and Harms
Communities Now* (Sept. 2022).

Cover photo: iStock/NiseriN

Table of Contents

Executive Summary

Cryptocurrency mining is an extremely energy-intensive process that threatens the ability of governments across the globe to reduce our dependence on climate-warming fossil fuels. If we do not take action to limit this growing industry now, we will not meet the goals set forth by the Paris Agreement and the Intergovernmental Panel on Climate Change to limit warning to 2 degrees Celsius. And cryptocurrency mining operations harm local communities now, including by increasing local pollution and impacting electricity rates and delivery. In our paper, we discuss several such examples where fossil-fueled cryptocurrency mining has increased local air, water, and noise pollution, increased costs on others, and increased climate pollution at a time when we should be doing everything in our power to move in the opposite direction to mitigate the worst impacts of the climate crisis.

The cryptocurrency mining industry is opaque: there are few, if any, reporting standards, and there is little or no formal tracking of mining operations. This paper is the first attempt to comprehensively document the explosive growth of cryptocurrency mining in the United States and examine how this industry is impacting utilities, energy systems, emissions, communities, and ratepayers — based on public filings before utility and financial regulators, investor presentations and reports, and local media reports.

Cryptocurrency Mining's Explosive Growth in the United States

After cryptocurrency mining was banned in China in 2021, the amount of mining operations exploded in the United States. As of this writing, it is estimated that 38% of Bitcoin — the predominant proof-of-work cryptocurrency — is mined in the United States. We estimate that in the year prior to July 2022, Bitcoin consumed around 36 billion kilowatt-hours (kWh) of electricity, as much as all of the electricity consumed in Maine, New Hampshire, Vermont, and Rhode Island put together in that same time period. And while proof-of-work mining proponents claim that cryptocurrency always looks for the cheapest energy, the last two years have demonstrated that the industry preferentially seeks readily-available energy and minimal regulation, re-starting defunct coal and gas plants, flooding the restructured electricity market in Texas, and tapping into power grids where regulators have little oversight. This explosive growth strains energy grids, raises retail electricity rates, and increases total carbon emissions and local air pollution.

What is Cryptocurrency Mining, and How Does It Work?

Proof-of-work cryptocurrency mining is designed to consume enormous quantities of energy. The process effectively entails millions of computing machines racing to solve a complex, but meaningless, problem. In Bitcoin's algorithm, for example, the computer or mining machine that successfully solves the problem is rewarded with Bitcoin (and functionally verifies the blockchain). As long as the reward is high enough (i.e., the price of Bitcoin is high enough), miners will attempt to use more — and faster — mining machines to increase their chances of winning that reward. As more mining machines enter the race, the difficulty of the computational problem gets harder, and the electricity required to win increases. Over time, the electricity used by miners in these races increases exponentially.

The design of proof-of-work cryptocurrency mining incentivizes miners to ramp up operations as quickly as possible, often irrespective of the source of energy. Indeed, big mining operations have shown a willingness to invest in otherwise uneconomic power sources, like defunct coal plants or low-capacity gas plants, as long as that electricity can be made available quickly. Unlike other large electricity users, cryptocurrency mining operations have a short time horizon, and most have shown little interest in investing in new clean energy.

In addition, the mining industry is becoming highly concentrated. The energy and technology requirements of cryptocurrency mining means that mining operations require the backing of large capital. For example, the National Bureau of Economic Research estimates that 0.5% of mining companies control 70% of mining. This increasing concentration in turn lends itself to the arms race where large corporations are able to leverage enormous capital to build massive mining facilities, like the 750 megawatt Whinstone mining facility an hour east of Austin, Texas.

Proof-of-Work Cryptocurrency Mining Increases Emissions in the United States

Top-down estimates of the electricity consumption of cryptocurrency mining in the United States imply that the industry was responsible for an excess 27.4 million tons of carbon dioxide (CO_2) between mid-2021 and 2022 — or three times as much as emitted by the largest coal plant in the U.S. in 2021. But these estimates are simply based on the likely energy consumption to solve cryptocurrency's puzzles. A ground-up approach, looking at how the industry has actually been deployed, suggests that proof-of-work cryptocurrency might be yet more impactful.

Tracking down the energy sources—or even just the consumption—of proof-of-work cryptocurrency mining in the United States is difficult. The industry is notoriously opaque, and little-to-no reporting requirements exist at either the state or federal level. The most reliable sources of information are a patchwork of filings before the Securities and Exchange Commission (SEC) by publicly-traded cryptocurrency companies, environmental permit applications, utility and other energy filings, and local reporting.

Cryptocurrency miners procure their electricity in four different ways: (1) outright purchase of power plants that supply mining rigs "behind-the-meter;" (2) power purchase agreements with power generators or utilities; (3) electricity purchases from a local utility; and (4) by burning fossil gas at oil and gas wells. Each type of mining produces excess emissions, and impacts electricity and energy consumers.

- **Behind-the-Meter at Power Plants.** Most egregiously, we identified four fossil-fueled power plants (the Scrubgrass and Panther Creek waste coal plants in Pennsylvania and the Greenidge and North Tonawanda gas plants in New York) that have been purchased and converted to mine proof-of-work cryptocurrency mining.
- **Power Purchase Agreements (PPAs).** Power plants or utilities may agree to sell a specific amount of electricity to a cryptocurrency miner. In some cases, a PPA is just a financial transaction, and in some cases, it can even change the amount that a power plant operates. In either case, when a cryptocurrency mining facility holds a contract with a fossil plant or a fossil-heavy utility, it provides a direct incentive to keep running polluting power plants. For example, an arrangement between Marathon Digital and the Hardin coal plant in Montana, which had been on the verge of retirement, led to ramped up operation and an 800% increase in CO_2 emissions (and 500% increase in sulfur dioxide emissions) from the plant in one year. Another example is the recent AboutBit agreement to purchase electricity from the Merom coal plant in Indiana. There, the plant's owner had previously announced a May 2023 retirement date, which has now been postponed, and a nearby coal mine has reopened to serve the plant.
- **Electricity Purchases.** Cryptocurrency miners that rely on retail electricity seek low cost—and rapidly available—electricity, wherever they can find it. An influx of new, large customers (sometimes doubling the utility's existing load) has forced utilities to seek additional generation resources or reduce off-system sales, strained their ability to manage the system, and raised prices for other customers. We found numerous examples of utilities making significant investments to serve cryptocurrency miners that were — or are likely to be — paid for by existing ratepayers. In some of these cases, the mining operation left abruptly months later, leaving behind stranded costs that are picked up by the utility and its customers:
    - The Nebraska Public Power District spent \$17.6 million, or 18% of its 2020 budget, on transmission and a substation for a cryptocurrency mining operation.
    - Big Rivers Electric utility plans to spend \$12.7 million in upgrades to service a new cryptocurrency mining operation in Paducah, Kentucky.
    - Entergy Arkansas reported that a cryptocurrency mining operation left "virtually overnight" in search of lower rates in 2019 after the utility expended significant funds on facility upgrades on the customer's behalf.
    - In 2018, a mining operation in Washington State left more than \$700,000 in utility bills unpaid after it declared bankruptcy.
- **Combusting Fossil Gas at Oil and Gas Wells.** Some companies mine cryptocurrency at the site of previously closed or low-operating fossil gas wells and use on-site generators to power their mining equipment. There is also an increasing amount of companies that sell cryptocurrency mining rigs specifically designed to tap into gas at oil-producing wellheads. The cryptocurrency mining operations provide additional revenue to oil drilling companies, by finding entities that would have otherwise been unwilling to gather oil-drilling's "associated gas" as required.

The Industry Keeps Greenwashing Its Poor Practices

The proof-of-work cryptocurrency mining community is well aware that its extraordinary energy consumption—and fossil fuel habit—is unattractive when much of the rest of the economy strives to rapidly decarbonize. In the last year, the industry and its trade organizations have rolled out a series of sustainability claims that are anywhere from outright fiction and greenwashing to no more than hopeful theories, undermined by actual practices.

One of the most widespread mischaracterizations is that mining is "sustainable" when the facility is physically located near existing wind power or solar power. But most mining facilities draw power from the grid — meaning their electricity is generated by whatever existing energy is in place in the region, or is contracted by their utility. Worse, adding a new large-scale load, like a cryptocurrency mining facility, to the grid generally requires existing fossil generators to increase their output. Mining facilities located near wind or solar sites do not have a special claim to energy produced by that energy, but instead drive increased emissions from gas and coal plants.

Another myth put forward by proponents is that proof-of-work cryptocurrency mining only uses "wasted" (or curtailed) energy from solar or wind overproduction. The fact is that mining operations operate and draw on the grid at all hours, not just when there is excess solar or wind. Mining operations would likely fail to be profitable using only the sparse hours in which solar or wind curtails. Few cryptocurrency mining operations are even located where wind or solar might provide curtailed energy, and operate far in excess of the amount of curtailed energy even available.

Proponents of proof-of-work cryptocurrency like to claim that the intensive demand of mining will spur new renewable development, and stabilize the grid. The reality is that clean energy allocated to cryptocurrency mining is then unavailable for grid decarbonization. As such, there are few mining facilities that are actually building new renewable energy to power their operations. The only claim to grid stability is that cryptocurrency mining operations may be willing to curtail operations if they paid enough to do so. A miner's participation in demand response programs during emergency periods (which many other electricity users do as well) can amount to tens of millions of dollars a year and is often paid by other ratepayers. Unlike batteries, mining operations cannot store electricity produced at peak solar or wind hours for later use, and provide no other grid services.

Today, the cryptocurrency mining industry already uses half the electricity of the entire global banking sector (while holding a miniscule fraction of the value), and continues to increase. In the United States, the industry has shown little indication of slowing its growth when prices are high. Miners have demonstrated, consistently, from their initial rush to China where coal is a predominant source of electricity to the recent deal between AboutBit and a soon-to-be-retired coal plant in Indiana, that proof-of-work cryptocurrency mining prioritizes the short-term need for large amounts of electricity over longer-term investments in renewable energy. And unlike other industries where self-imposed, or regulation-based, community standards could result in more sustainable practices, proof-of-work mining is an inherent arms race towards increased energy consumption, until prices no longer support growth.

Regulators and Policymakers Can Take Steps to Reduce the Harm of Cryptocurrency Mining

State, local, and federal policymakers and regulators can help ensure cryptocurrency mining does not undermine climate or health goals, or adversely impact ratepayers.

The massive energy consumption of cryptocurrency mining threatens to undermine decades of progress towards achieving climate goals, and threatens grids, utilities, communities, and ratepayers. Some jurisdictions have, or are considering, simply banning the practice of mining proof-of-work cryptocurrencies. Shy of a complete moratorium, there are actions that can be taken by state, local, and federal officials to protect energy systems, communities, and ratepayers.

POLICY AND REGULATORY OPTIONS

- Local and state officials can enforce pollution and noise ordinances, ensure that they are not extending economic development dollars on false promises of long-term jobs or revenue, develop careful zoning codes, and — in the cases where municipalities run the electric utility — develop tariffs that protect existing ratepayers.
- Utility regulators can influence or bar problematic power purchase agreements, create protective electricity rates or system benefits charges that ensure speculative mining operations do not leave a trail of stranded assets, critically assess utility plans for energy procurement for cryptocurrency mining facilities, and ensure that mining facilities do not increase electricity or capacity costs for existing customers.
- Utilities can develop electricity rates that protect against stranded assets, ensure that they do not need to expand power capacity to meet cryptocurrency mining load, and charge rates sufficient to fully protect existing ratepayers from the increased marginal cost of production.
- Grid operators can develop comprehensive guidance and rules around the interconnection of high-density loads, study the impact of cryptocurrency mining on congestion, resource adequacy, and wholesale market prices, and create rules that minimize the impact of cryptocurrency mining on other customers.
- Environmental regulators at all levels should consider affirmative regulation to minimize the local health and environment impacts cryptocurrency mining places on local communities.

I. Cryptocurrency Mining's Explosive Growth in the United States

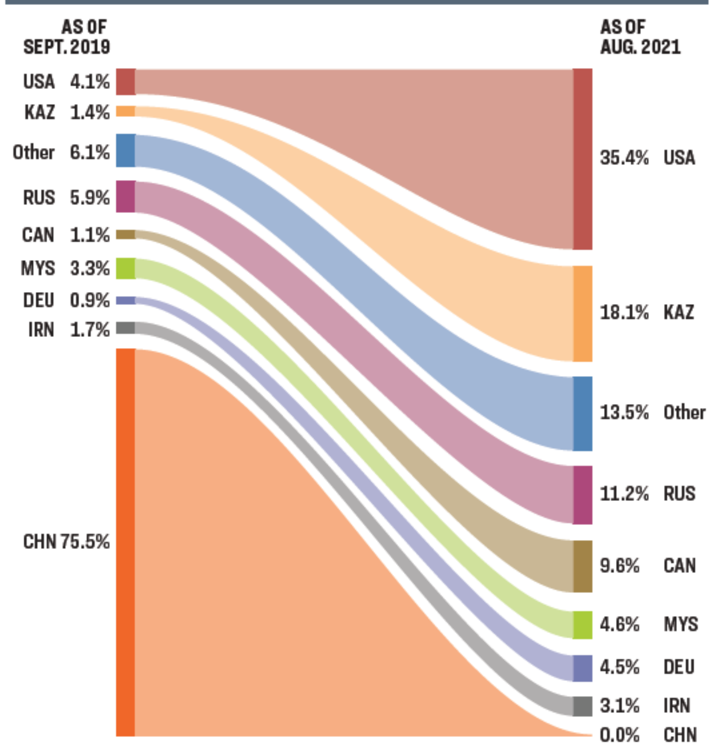
So-called "proof-of-work" cryptocurrencies are secured by the use of intensive computing — and electricity — resources. Cryptocurrencies, starting with Bitcoin, innovated an approach to tracking, and verifying, transactions that requires no central entity, like a bank. But the currently predominant cryptocurrency, Bitcoin, bases its security on an approach that requires machines to compete to solve complex puzzles. The growth in the value of Bitcoin led to an arms race — and explosive energy consumption globally, and over the last year, in the United States. The Cambridge Centre for Alternative Finance estimates that Bitcoin alone increased its electricity consumption from less than a gigawatt (GW) per day in early 2017 to more than 11 GW in July 2022.[1] By early 2022, prior to the collapse of Bitcoin prices,[2] Bitcoin was consuming over 10.5 billion kilowatt hours (kWh) every *three months* — or the equivalent output of ten large coal-fired power plants.[3]

In its April 2022 report, the Intergovernmental Panel on Climate Change (IPCC) warned that soaring electricity use by proof-of-work digital currencies is likely to "be a major global source of CO_2 if the electricity production is not decarbonized."[4] The White House's Office of Science and Technology Policy (OSTP) recently estimated that proof-of-work cryptocurrency mining likely comprises somewhere between 0.9% to 1.7% of total annual U.S. electricity usage, or 36 to 66 billion kWh per year in mid-2022.[5]

Bitcoin has been at the center of cryptocurrency energy debates, and rightfully so: Bitcoin mining uses far more electricity than any other cryptocurrency, for two reasons. First, Bitcoin makes up more than 40% of the cryptocurrency market share, by far the largest of any currency.[6] Second, Bitcoin is the most energy-intensive cryptocurrency in wide circulation, because it uses a "proof-of-work" mining method that is designed to require increased energy inputs for the same economic output over time. Because of its outsized energy footprint, this paper focuses on Bitcoin as a proxy for other proof-of-work cryptocurrencies. As of this writing, the second largest energy consuming cryptocurrency, Ethereum, was in the process of transitioning from a proof-of-work construct to a "proof-of-stake" verification, an alternative mechanism of securing cryptocurrency transactions that does not require machines to solve the same volume of puzzles — and hence uses only a small fraction of proof-of-work algorithms.[7]

Until last year, the majority of Bitcoin mining was physically located in China. In May 2021, Chinese officials initiated a crackdown on cryptocurrency mining operations; within a month, more than 90% of operations were shut down or planned to.[8] Bitcoin mining, however, continued its upward trajectory, with much of the computing shifting to the United States.[9] Although there had been some indications of growth in U.S.-based mining in 2020,[10] in a matter of months, the amount of U.S.-based mining exploded, with little regulatory oversight.[11] In 2019, the U.S. accounted for just 4% of global mining; as of August 2022, nearly 38% of Bitcoin mining activity is estimated to be based out of the U.S.[12] By January 2022, U.S. Bitcoin operations were consuming an estimated 3.7 billion kWh per month — more than the January electricity sales of the entire state of Kansas or Nevada.[13] Assuming that the efficiency of mining machines in the United States is roughly consistent with those used in other countries, we estimate that Bitcoin mining consumed 35.8 billion kWh from June 2021 to July 2022, or as much electricity as all of Maine, New Hampshire, Vermont, and Rhode Island put together — or every industrial electricity customer in Georgia.[14]

Migration of Cryptocurrency Miners, Sept. 2019 — Aug. 2021[15]



When primarily located in China before it was banned, cryptocurrency mining was often powered by hydroelectric facilities and coal plants. When miners fled China, they began to power operations with gas and fossil-heavy grids (especially in the United States) and hard coal (in Kazakhstan). The share of renewable energy used to power Bitcoin mining is estimated to have dropped from 41.6% in 2020 to about 25.1% in August 2021.[16] At least one estimate suggests that U.S.-based Bitcoin miners are already responsible for at least one-quarter of the global greenhouse gas emissions caused by Bitcoin mining.[17] OSTP estimates that Bitcoin mining in the United States alone is responsible for between 21 to 35 million tons (Mt) CO_2 per year; and global Ethereum operating on a proof-of-work algorithm accounts for 25 to 50 $MtCO_2$ per year.[18]

This paper identifies the impacts from proof-of-work cryptocurrency mining have on our electric system, utility bills, air and water quality, communities, and decarbonization goals. The rapid rise of massive, centralized, proof-of-work cryptocurrency mining operations affects utilities, ratepayers, and the environment. It also threatens to reverse ongoing trends toward the decarbonization of the U.S. power sector, further entrenching fossil fuel production and consumption. This paper seeks to educate advocates, policymakers, regulators, and the public about the immediate threat that proof-of-work cryptocurrency mining poses to communities, ratepayers, and climate action and to provide a much-needed corrective to myths that cryptocurrency mining companies have promoted about the relationship between their business model and clean energy.

II. Proof-of-Work Cryptocurrency: A Brief Introduction

What are "proof-of-work" cryptocurrencies, and why do they use so much energy? In short, proof-of-work cryptocurrencies' mechanism for protecting the integrity of ownership is to require computers or mining machines to compete to solve complex mathematical puzzles, and reward the winner (the miner) with currency. The mechanism is designed to promote an arms race: more machines competing to solve the puzzle theoretically means that no single entity can control, or monopolize, the system. The person or company with the most computational power will be rewarded with the most currency. Consequently, cryptocurrency mining operations are running immense computational operations, often *tens of thousands* of mining machines, around the clock to secure the best chances of winning.

Cryptocurrencies generally use a "distributed ledger," meaning that ownership and transaction records are not centrally located but can only be established through computations conducted across participants' mining machines. To minimize the chances of participants trying to cheat each other by writing false transactions into the ledger, cryptocurrencies need a mechanism to decide how a transaction can be considered valid. For proof-of-work cryptocurrencies, the first mining machine to solve a cryptological problem (i.e., a puzzle) gets to validate the next set of transactions, and in doing so, earns a reward. The form of the puzzle requires mining machines to perform millions of computations, in effect guessing at the answer. To induce individuals to commit computing power towards these validation puzzles, the Bitcoin network rewards participants with new Bitcoins if they successfully validate a set of transactions—that is, be the first to solve the puzzle, thereby adding another "block" (or solution) in the chain (that in turn becomes an input to the *next* puzzle). Operations that try to earn this new Bitcoin are called "miners" (because they are "mining" new Bitcoin), as are the mining machines that are specially designed to *only* solve these puzzles.[19]

The puzzle that Bitcoin miners try to solve is calibrated approximately every two weeks such that across the global network, rewards are earned, on average, about every ten minutes.[20] As more miners enter the system, the reward becomes harder to earn. To have a better chance of earning the reward, miners add new machines to the system, consequently consuming more energy, and in doing so, make the reward harder to earn. The entire system can be compared to an unbounded lottery, played every ten minutes. To have the best chance of winning the lottery, you need to buy more tickets, but as more people buy tickets, your chances of winning the lottery decrease. The winning strategy, to date, has been to buy as many chances at the lottery as possible, as quickly as possible—*i.e.*, build mining centers as quickly as possible.[21] Importantly, the vast majority of computational energy in the Bitcoin system at any one time is wasted: the system works if there are twenty thousand mining machines competing—or two million.[22]

Will the explosive growth in energy consumption ever come to an end for proof-of-work cryptocurrencies? There are two countervailing forces that drive the trajectory of energy use for Bitcoin: difficulty drives the value of mining down, and the price of Bitcoin drives the value of mining (and energy consumption) up. Difficulty is driven by miners entering the system, increasing the complexity of the problems and thereby raising the energy cost of winning a block of Bitcoin. By design, the Bitcoin reward offered to miners is cut in half approximately every four years. These two factors together make it increasingly costly to obtain new Bitcoin.[23] But higher Bitcoin prices can overwhelm these barriers. Even at the relatively depressed price of Bitcoin as of this writing (~$20,000), Bitcoin miners can afford to pay well above what ordinary users of electricity pay—and can afford to keep adding new processing power.

III. No Longer a Hobbyist's Experiment: How Cryptocurrency Mining Transformed Into Massive, Centralized Operations to Maximize Profits

In October 2010, just one year after Bitcoin was publicly introduced, its network processed around ten billion calculations (gigahashes) per second (Gh/s),[24] meaning the entire network could be run by between 6,000 and 7,000 mining machines.[25] With Bitcoin trading at a modest 20 cents, Bitcoin miners were mostly restricted by the cost of acquiring hardware and allocating it to Bitcoin mining.[26] Cryptocurrency mining was largely a hobbyist's exercise, with miners found in garages, basements, or home offices.[27] But today, these small operations are in the minority; in 2020, 4.5% of Bitcoin holders held 85% of the currency.[28]

Beginning in early 2012, miners began switching to specialized equipment, first using modified graphics processing units and quickly advancing to application-specific integrated circuit (ASIC) machines. As mining got more popular (and thus more competitive), the estimated power dedicated to Bitcoin mining rose from less than 1 GW at the start of 2017 to nearly 4.4 GW by the end of 2018.[29]

Today, the scale of cryptocurrency mining is expanding rapidly in the United States. Cryptocurrency mining is now the largest source of electricity demand for some utilities. In Texas alone, we tracked 2,234 MW of cryptocurrency mining facilities, almost entirely built since mid-2021. Eight of the facilities are between 150 to 300 MW each.[30] A single 300 MW facility might host nearly 100,000 machines,[31] consuming enough electricity to power, on average, nearly 49,000 nearby homes.[32] Unlike many industrial operations or even data centers that reduce energy usage at off-peak times, these facilities typically run 24 hours a day, seven days a week, 365 days a year, at full capacity. Any downtime is a lost opportunity to "win" blocks of Bitcoin, and mining machines can run for hours with minimal human supervision.

Cryptocurrency is touted as a democratizing form of finance[33]—but it is increasingly a highly concentrated industry that relies on large financial institutions to fuel its growth. Because of the immense amount of capital needed to purchase enough ASIC miners, with high-performance machines many thousands of dollars each, cryptocurrency mining is beyond the reach of only a few mining companies.[34] Even small-scale miners' operations are part of high-density loads, as many pool their computing power to increase their chances of validating a coin. Almost 80% of all computing power on the Bitcoin network is owned by seven mining pools.[35] A 2021 paper from the National Bureau of Economic Research tracing rewards within a subset of those pools found that 90% of rewards (Bitcoin blocks) were received by just 10% of miners—nearly 70% were received by just *half a percent* of miners.[36]

A. Proof-of-Work Cryptocurrency Mining Incentivizes Mining As Quickly As Possible to Maximize Profits

The structure of proof-of-work cryptocurrency mining—where the first mining machine to solve the puzzle gains a reward, where the reward falls over time, where there is no limit on the number of entrants in the competition to earn the reward, and where there is a perception that the value of cryptocurrency is effectively limitless—creates an incentive to mine cryptocurrency as quickly as possible. Mining equipment, too, quickly becomes obsolete.[37]

The ability to get existing mining equipment running as soon (and often) as possible is incentivized over nearly all other considerations. Bitcoin is designed so that the reward that miners receive for validating a transaction shrinks over time. These are known as "halving" events. At the inception of Bitcoin, miners that successfully validated transactions were provided 50 Bitcoin. That reward has fallen approximately every four years. Today, in 2022, it is just 6.25 Bitcoin. At the height of Bitcoin's value in March 2022, that 6.25 Bitcoin was worth $294,146. The next halving event is projected for 2024, at which point the value per computational effort of mining Bitcoin will immediately fall by 50%. Miners looking towards that halving event will seek to mine as much Bitcoin today as feasible, knowing that the value of mining will sharply decline at that event.[38]

B. Cryptocurrency Miners Often Value *Speed* of Access to Energy Over Price, Even to the Point of Reviving Dying Fossil-Fueled Power Plants

Proponents of proof-of-work claim that it seeks low-cost energy, or even excess energy. This is true—but only to an extent. Utilities with particularly inexpensive energy due to subsidized hydropower, for example, have seen a higher number of interconnection requests from miners. But because proof-of-work cryptocurrency mining rewards speed above all other considerations, miners are turning to any and all readily available energy options, such as defunct or otherwise uneconomic power plants, so they can set up mining operations as quickly as possible.

Accordingly, some of the fastest growth of cryptocurrency mining in the United States recently has occurred where miners have made direct deals with defunct generating stations, and in Texas's unique electricity market.

Miners have invested at power plants that have otherwise struggled to demonstrate economic value, a trend that would seem to be counter to prudent planning. But unlike other customers, miners have been willing to pay above-market prices for electricity from otherwise retiring coal plants (such as at the Hardin coal plant in Montana), or inefficient plants (such as the Panther Creek and Scrubgrass waste coal plants in Pennsylvania) because energy from these plants could be procured quickly, and with few regulatory hurdles.

Similarly, Texas's deregulated electricity market means end-users are not limited to a particular retail electricity provider based on location, and the absence of a wholesale capacity market (basically, a requirement that utilities pay for a guarantee of available electricity) can lead to price extremes (both low and high). Both of these characteristics have made Texas attractive to geographically flexible miners who can shop around for favorable terms, and can shut down operations when prices spike. Texas's restructured market makes it easy for miners to build facilities with few obligations to the grid.

Given the uncertainty as to future Bitcoin prices, the fact that Bitcoin cannot be widely used as a currency for ordinary transactions, and the exceptional volatility in prices, mining operations cannot—and generally do not—bet on the long-term stability of their enterprise. There is little reason for cryptocurrency miners to make investments lasting even a year or two to build solar or wind generation, as long as existing fossil fuel plants can provide the same electricity, faster.

IV. The Scale and Source of Bitcoin Energy Usage is Largely Invisible to Regulators

Although cryptocurrency mining operations have become increasingly specialized, concentrated, and capital-intensive—and thus identifiable as a distinct class of business and energy user—it is difficult or impossible to find information about the scale, location, or fuel source of cryptocurrency mining operations in the United States.

Proof-of-work cryptocurrency mining operations are not tethered to any particular geography: miners seek speed to market, cheap energy, flexibility, and distance from regulators. For example, multiple companies offer mining equipment in shipping containers to chase the best prices,[39] and when prices fluctuate, mining facilities can migrate quickly. For example, in April 2022, Marathon Digital announced that it would abandon its new position adjacent to the Hardin coal plant in Montana, noting that it could complete the transition by the third quarter of 2022, or in less than half a year.[40] Similarly, Compass Mining recently announced that it would close its Georgia facilities and move its mining machines to Texas, reportedly just two months after proposing to ship Texas mining machines to Georgia to chase a faster interconnection.[41]

Currently, the primary sources for publicly available information about cryptocurrency's energy usage and environmental impacts are local journalists, company press releases, and Securities and Exchange Commission (SEC) filings for publicly-traded cryptocurrency mining companies. Occasionally, information about mining operations may be found incidentally through regulatory oversight of utilities or generation facilities (such as through utility tariff filings that identify new interconnection requests or Federal Power Act Section 203 filings before the Federal Energy Regulatory Commission (FERC) relating to the sale of generation facilities).

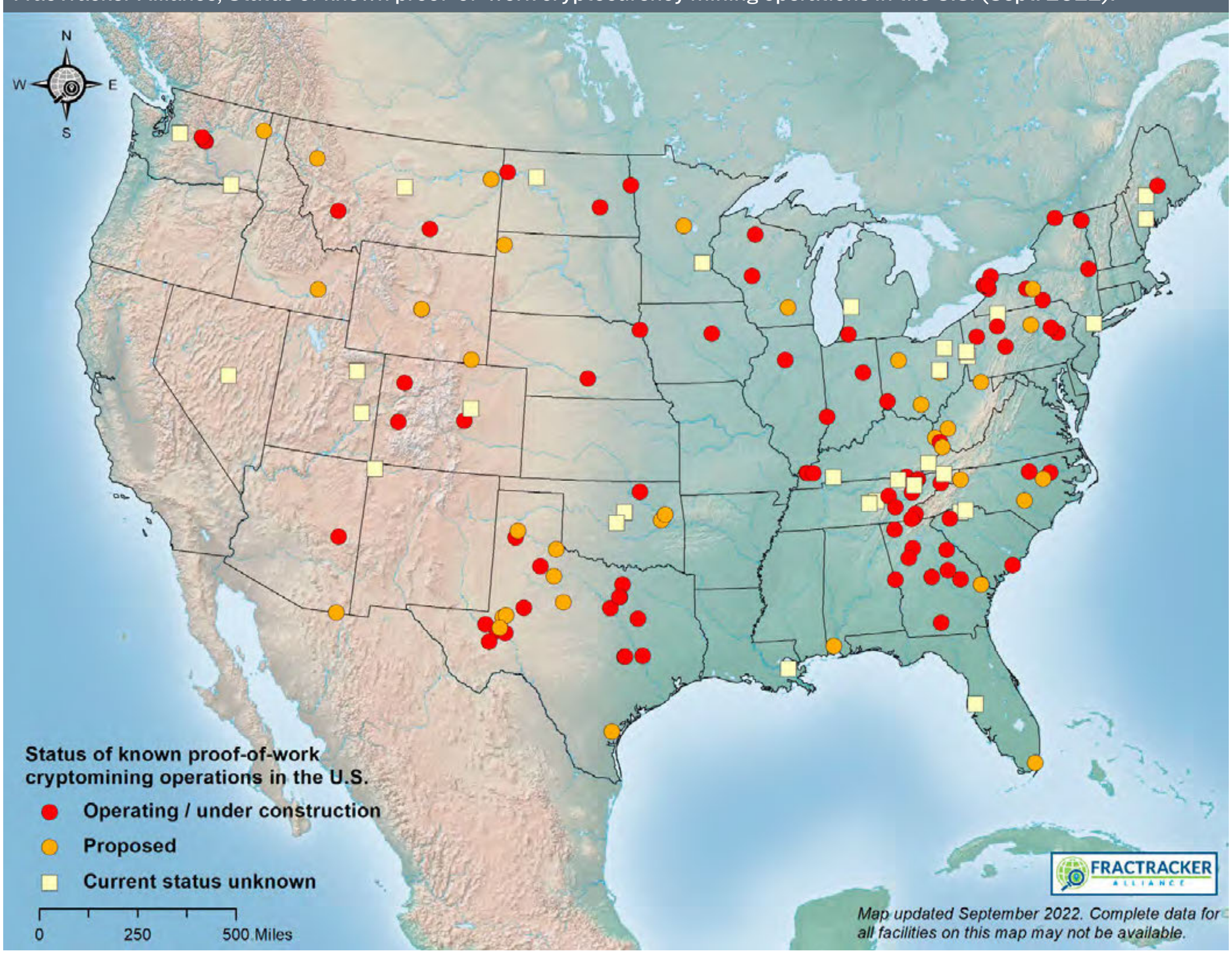
Many mining operations, however, are not owned by publicly-traded companies. Among those that *do* file reports with the SEC, many do not disclose the fuel sources associated with the miners listed in their 10-K or 8-K reports, or provide only partial or selective information, such as describing the energy supply as "reliable, renewable" or as having "high emissions free content."[42] If the mining company reports a Power Purchase Agreement (PPA) with a utility, and that utility is required to file an integrated resource plan or other public information about its generation under state law (or does so voluntarily),[43] that information can be used to help determine fuel mix when operations use energy from the grid.

In the cases where the mining company directly purchases generation resources, there may be additional information through the U.S. Environmental Protection Agency (EPA) or state air or water permitting processes,[44] or within filings under Section 203 of the Federal Power Act if FERC approval is required for the purchase.[45]

V. Where *Do* The Electrons Come From?

Despite the lack of centralized information about the location or energy source for large-scale cryptocurrency computing centers, we were able to identify more than 140 cryptocurrency mining operations through a patchwork of SEC filings, investor presentations, public utility commission dockets, grid operators' public processes, local newspaper coverage, and local activist efforts. Using this information, we then attempted to determine how these operations were obtaining electricity and the greenhouse gas emissions associated with that electricity usage.

FracTracker Alliance, Status of known proof-of-work cryptocurency mining operations in the U.S. (Sept. 2022).[46]



A. Types of Electricity Procurement by Cryptocurrency Miners

There are four primary means by which proof-of-work cryptocurrency mining companies power their operations: (1) operating behind-the-meter at a power plant;[47] (2) purchasing power directly from a power plant or utility; (3) purchasing electricity from the grid either through a power purchase agreement with a utility or by paying a retail rate (which may be a general industrial rate or an even lower "economic development" rate); or (4) hooking up a generator to oil and gas wells to burn gas that would not be combusted, or otherwise not be injected into the pipeline system, either through flaring or venting. In nearly all of these scenarios, these unregulated, energy-intensive proof-of-work cryptocurrency mining operations are financing the continuation of fossil fuel extraction and generation—in direct opposition to what is needed to prevent the worst of the impacts from the climate crisis.[48] And in some places, investments in fossil generation will be made in response to this boom in demand that will have ongoing effects for decades.

1. Behind-the-Meter Generation at Fossil-Fueled Power Plants

Cryptocurrency mining operations most directly drive increased greenhouse gas emissions when they outright purchase fossil fuel plants. We have identified several fossil fuel power plants where greenhouse gas emissions and local pollution increased dramatically after those plants were acquired by cryptocurrency mining companies and began operating around-the-clock.

i. Burning Waste Coal to Generate Electricity for Cryptocurrency Mining in Pennsylvania

In July 2021, Stronghold Digital Mining Inc. filed an S-1 report with the SEC disclosing plans to purchase three waste-coal-fired power plants in Pennsylvania with a combined capacity of 300 MW and install 57,000 ASICs dedicated to mining cryptocurrency.[49] To date, Stronghold has purchased the 94 MW Scrubgrass power plant in Venango County and the 94 MW Panther Creek facility in Carbon County.[50]

Burning waste coal to generate electricity for cryptocurrency mining is one of the worst possible choices for the climate and for local air pollution.[51] According to U.S. Energy Information Administration data, Pennsylvania's waste-coal-fired power plants had average CO_2 emissions of over 2,760 pounds per megawatt-hour (MWh), making them the second most carbon intensive fuel behind residual fuel oil.[52]

The Scrubgrass plant relies on a mixture of rejected waste coal and dirt that emits hundreds of tons of dangerous air pollution, including sulfur dioxide, nitrogen oxide, and hazardous air pollutants.[53] The waste coal is also carried on hour-long trips by large trucks over two-lane country roads, endangering communities along the route with additional air pollution. Adding insult to injury, the plant receives subsidies from Pennsylvania taxpayers and ratepayers because it burns "waste," including $4/MWh for the Pennsylvania Coal Refuse Reclamation tax credit and $16/MWh from the Pennsylvania Tier II Alternative Energy Portfolio Standard Program.[54] Stronghold, which owns and operates the two waste coal plants, has claimed that 60% of their generation costs will be covered by subsidies from taxpayers and ratepayers.[55]

ii. Burning Fossil Gas to Generate Electricity for Cryptocurrency Mining in New York State

In upstate New York, the Fortistar North Tonawanda gas-fired power plant plans to power proof-of-work cryptocurrency mining full-time behind-the-meter. Prior to the change in operations, the facility operated rarely, at only a 2 to 13% capacity factor, meaning its emissions of greenhouse gases and other harmful air pollutants were relatively small compared to what the plant was capable of.[56] Running the plant full-time to mine cryptocurrency could cause a nearly 3,000% increase in its annual CO_2 emissions along with dramatic increases in other harmful local air pollutants such as haze-producing nitrogen oxides, particulate matter, and carbon monoxide.[57] This significant increase in air pollution will spew into several nearby environmental justice areas.[58]

About a hundred miles away, on the western shores of Seneca Lake, among the productive vineyards and farms of the Finger Lakes, the former coal-fired and now fossil gas-fired Greenidge Generation Station began operating as a cryptocurrency mining facility full-time in 2020. In its first year of mining operations, CO_2 emissions at the plant increased 479%.[59] Other local air pollutants rose sharply as well when it began operating 24 hours a day.[60]

Fortunately, it is not clear how much longer Greenidge will continue to pollute; the New York State Department of Environmental Conservation denied an air permit renewal application for the Greenidge gas plant in June 2022, concluding the plant's expanded operations and significant increase in air emissions over the past two years were inconsistent with the state's climate law, because its behind-the-meter cryptocurrency mining "was creating a significant demand for energy for a wholly new purpose unrelated to its original permit."[61] There are also serious question as to whether the plant's owners can safely and effectively address and remediate the existing coal ash contamination or water pollution issues on site.[62]

2. Power Purchase Agreements with Fossil-Fueled Power Plants or Utilities

As the Greenidge plant's air permit denial demonstrates, outright ownership of fossil fuel resources entails legal responsibilities and both invites scrutiny and requires transparency that many cryptocurrency mining operations have sought to avoid. Therefore, a large number of mining operators instead set up mining facilities in close proximity to, and directly connected with, fossil fuel power plants, and enter into power purchase agreements for electricity from those plants. Some of these arrangements are negotiated with the local utility to purchase electricity at rock bottom prices, often with no scrutiny from regulators. For example, Cipher Mining has negotiated PPAs with an average fixed price of 2.73 cents per kWh.[63] For many others, the electricity rate paid by miners in PPAs is unknown.

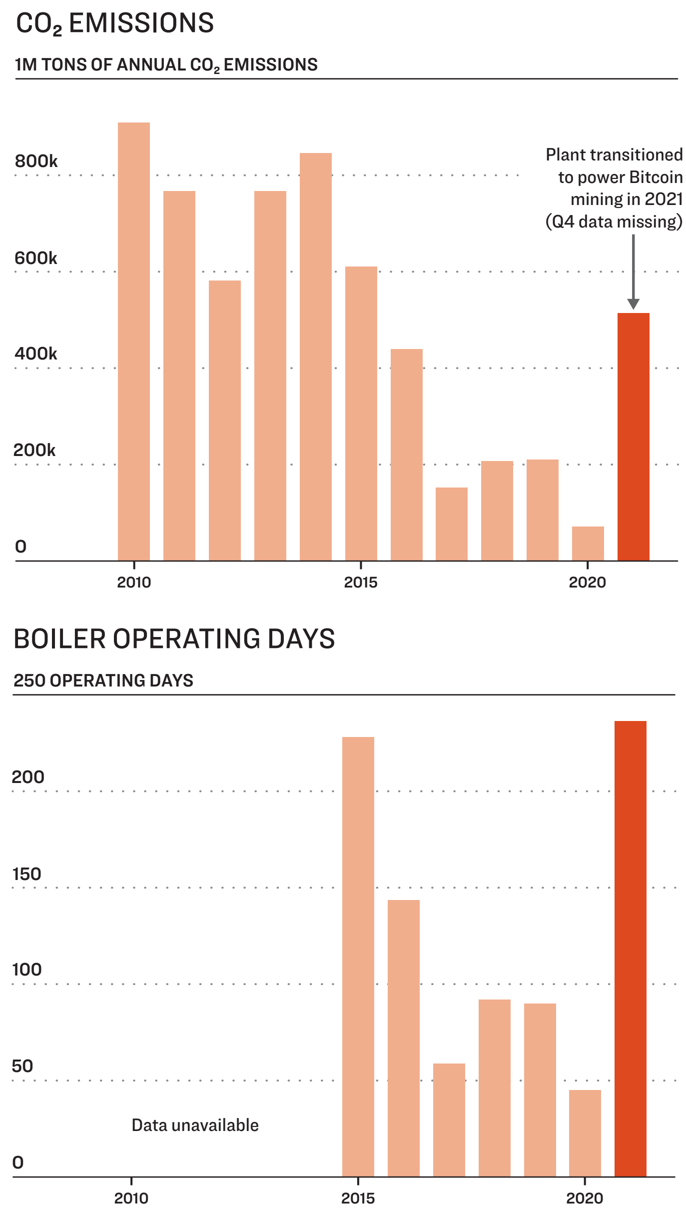
These arrangements, often not publicly available, can prolong the operation of coal- or gas-fired power plants that were otherwise likely to retire or even had an announced retirement date.

i. A Coal Plant in Hardin, Montana That Hardly Operated Powered Up to Mine Cryptocurrency

One prominent example of this practice is the Big Horn Data Hub operated by Marathon Digital Holdings at the 115 MW Hardin Generating Station, a coal plant just north of the Crow Indian Reservation in Big Horn County, Montana. Before cryptocurrency mining operations ramped up at Hardin, the plant had been slated to close permanently in 2018 and generated power for just 75 days per year on average from 2017 through 2020.[64] In late 2020, publicly-traded cryptocurrency mining company Marathon announced a partnership with the plant's operator, Beowulf Energy, to utilize roughly 37 MW of power from the plant to mine cryptocurrency around the clock. Hardin operated 323 days in 2021.[65]

The plant's operations were enormously profitable for Marathon, which won approximately 34 Bitcoin on December 1, 2021 alone[66] — equivalent to $1,945,786 at the time.[67] Hardin's neighbors were not so lucky. In 2021, nitrogen oxide emissions increased 842%, sulfur dioxide emissions increased 508%, and CO_2 emissions increased 850%.[68]

As Hardin plant powered Bitcoin mining, emissions spiked



Sources: Provided by the Montana Environmental Information Center from reports submitted to the Montana Department of Environmental Quality. Graphic is adapted from The Guardian.

As with all coal plants, delaying a retirement date and increasing operations to mine cryptocurrency increases all pollution from the plant. Additional years of operations mean millions of tons more of coal ash or coal combustion residuals (CCR) — a toxic solid waste byproduct of burning coal.[69]

In early April 2022, Marathon Digital announced that it would transition its operation at Hardin to other locations to use "more sustainable sources of power" and reduce its pollution by the end of 2022.[70] However, agreements between Marathon and Compute North suggest the miners were simply moved to a behind-the-meter operation at fossil gas-powered Wolf Hollow Generating Station in Texas.[71] And even in leaving, Marathon left millions of dollars' worth of infrastructure intact, "so another miner can come in right behind us with a minimal delay and then com[e] up to speed," according to its CEO.[72] The Hardin plant's owner is currently in discussions with potential tenants that are interested in moving into the Big Horn Data Hub.[73]

ii. A Coal Plant's Polluting Operations in Merom, Indiana Are Extended to Mine Cryptocurrency

Cryptocurrency mining may also help prolong the life of the Merom Generating Station, a 1,080 MW coal-fired power plant in southwest Indiana. Hoosier Energy, a generation and transmission rural electric cooperative that has owned the plant for around 40 years,[74] previously announced the plant would retire in May 2023.[75] Then, in February 2022, Hoosier Energy announced plans to sell the plant to Hallador (a coal-mining company) and purchase a portion of the plant's energy and capacity from the new owner.[76] Shortly thereafter, in May 2022, the public learned that AboutBit, a cryptocurrency mining company, would be constructing a new mining site adjacent to the Merom plant and purchasing 115 MW of electricity from WIN Energy, a distribution cooperative that purchases all of its power from Hoosier Energy.[77] It is unclear whether the PPA between WIN and AboutBit was known to Hallador, Hoosier Energy, or both, before the two parties reached an agreement on the sale of the plant, but it makes the Merom plant considerably more economically viable as a merchant generator than it would otherwise be.[78] In fact, AboutBit's co-founder responded to criticism about keeping a coal plant open by stating, "It's 100 percent correct. For anyone to say their crypto operation is green, unless they are 100 percent hydro, they can't make that claim. As an operation, it's not humanly possible."[79] Hallador also plans to reopen a coal mine in Knox County, Indiana, to supply this plant's extended operations.[80]

3. Retail Purchases of Electricity from the Grid

Some miners simply purchase energy from their local utility as retail customers. Miners seek out utilities where industrial electricity rates (which are often lower than residential rates on a cent per kWh basis) are particularly low.

One of the largest cryptocurrency mining companies, Riot Blockchain, only pays 2.5 cents per kWh for its electricity. These rates are roughly 10 to 11 cents less than the going residential rate,[81] and about 5 cents less than the large consumer rate.[82]

At the same time, miners often also participate in demand response programs, which will pay miners to stop drawing electricity during periods of high demand. Although such programs mitigate some of the impacts of mining on the grid, other customers must effectively pay miners to shut down, which may be extremely profitable for such large consumers like mining operations during extreme weather events than actually mining.[83] As described further below in Section VIII.D, while demand response programs are essential tools to mitigate the pressure the power grid faces from extreme weather events like heat waves, the vast amount of new and increasing load placed on the grid by cryptocurrency miners who often pay lower electricity rates than others, but then are paid very high rates for demand response are not fair to other electricity users.

The impacts on other ratepayers from discounted electricity rates provided to miners and from the payments to miners for demand response can be severe, which is discussed further below in Section VII.B.

4. Combusting Fossil Gas at Oil and Gas Wells

Many cryptocurrency mining companies are utilizing electricity generated from combusting fossil gas at oil and gas well pads. This type of mining operation can reopen orphaned wells, often in remote areas such as in rural South Dakota or western Pennsylvania, that should otherwise be plugged or capped to prevent methane and other pollution.[84] Some of these operations are literally off-the-map. One journalist visited a "small installation [in Kentucky], miles from the nearest paved road, [that] draws methane gas from a long abandoned well that [the miner] has fixed up with a generator and satellite internet . . . ."[85] The mobility and remoteness of these operations make them and their pollution extremely difficult to quantify.

This type of cryptocurrency mining also incentivizes further oil and gas drilling, as it converts what would be a loss for drillers ("waste" flared gas that could go to beneficial end uses or minimized) into a new source of revenue.[86] Some miners claim these operations are a kind of environmental mitigation because they use the "waste" flared gas to generate electricity.[87] As one professor at University of California, Santa Barbara, has observed, "This is basically a way to monetize flaring. It's not a way to stop flaring."[88]

Just one of the companies engaging in flare-based generation for cryptocurrency mining, Colorado-based Crusoe Energy, claimed in April 2022 to operate 86 "Digital Flare Mitigation" data centers in Montana, North Dakota, Wyoming, and Colorado, with more planned in

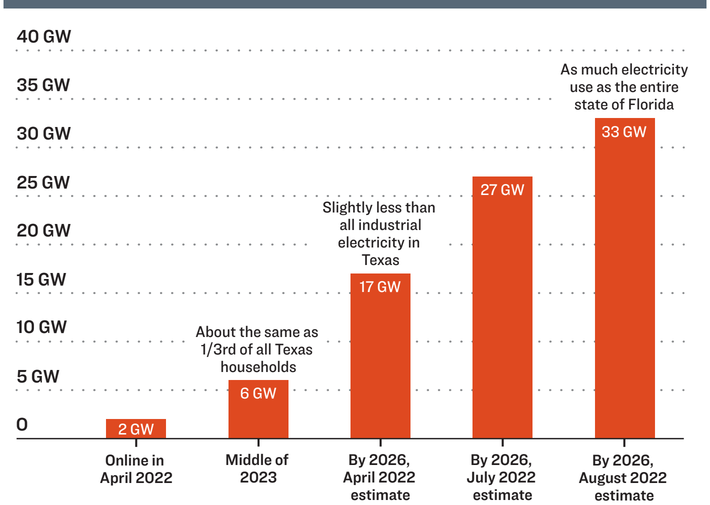
Texas and New Mexico.[89] Major oil companies have also expressed interest in these operations.[90] In March 2022, Exxon Mobil announced that it would consider expanding a North Dakota-based pilot program with aforementioned Crusoe Energy to Alaska, the Qua Iboe Terminal in Nigeria, Argentina's Vaca Muerta shale field, Guyana, and Germany, which would use up to 18 million cubic feet of gas per month.[91]

When regulators do locate and inspect wellhead miners, they can find violations of law. For example, in January 2022, inspectors from the Pennsylvania Department of Environmental Protection found 30 methane-gas-fired generators with an estimated capacity of more than 10 MW that were cryptocurrency mining without authorization.[92] In Adams County, Colorado, inspectors found four cryptocurrency mining operations at oil and gas wells operating without proper authorization.[93] Concerned about these operations and their pollution, in May 2022, the county "prohibit[ed] cryptocurrency / digital currency / electronic currency mining operations on oil and gas facilities."[94]

VI. The Climate and Energy Impacts of Cryptocurrency Mining in the United States are Substantial

The scale, and explosive growth, of cryptocurrency mining in the United States is hard to fully document, because most mining operations do not readily disclose their energy consumption, much less location and source of electricity. But both ground-up accounting and top-down estimates reveal the same trend: cryptocurrency mining operations have a substantial emissions impact. The most obvious way cryptocurrency mining increases global emissions is by driving huge increases in electricity demand. For example, Texas's grid operator, the Electric Reliability Council of Texas or ERCOT, recently disclosed that it expected nearly 6 GW of new cryptocurrency load to be interconnected by mid-2023.[95] ERCOT continues to adjust its forecasts of crypto-related load—announcing 17 GW by 2026 in April 2022,[96] to 27 GW by 2026 in July 2022,[97] to 33 GW by 2026 in August 2022.[98]

Texas Crypto Boom is Getting Even Bigger



Texas Blockchain Council. *ERCOT Large Flexible Load Task Force Meeting*, at 4 (April 22, 2022)

6 GW of cryptomining equipment operating at 85% load factor results in 44.7 TWh per year. Texas residential consumption in 2021 was 156.1 TWh. Source: Energy Information Administration, *Annual Electric Power Industry Report*, Form EIA-861. (Last accessed August 3, 2022).

33 GW of cryptomining equipment operating at 85% load factor results in 245.7 TWh per year. Total Florida consumption in 2021 was 244 TWh. Source: Energy Information Administration, *Annual Electric Power Industry Report*, Form EIA-861. (Last accessed August 3, 2022).

Based on the current grid generation mix and estimated Bitcoin energy consumption, we estimate Bitcoin mining in the United States is responsible for between 11 to 76 million annual excess tons of CO_2 in the last year, with a central estimate of 27.4 million tons CO_2.[99] For context, that is about three times as much CO_2 as was emitted by the largest coal plant in the United States in 2021.[100] The White House's OSTP arrives at a similar estimate, of about 21 to 35 million tons by mid-2022 from Bitcoin mining, and 25 to 50 million tons CO_2 from all cryptocurrency mining activity in the United States.[101] According to the U.S. House Committee on Energy and Commerce, the CO_2 emissions from global mining of Ethereum and Bitcoin in 2021 equaled the tailpipe emissions of more than 15.5 million gas-powered cars.[102]

In the absence of a comprehensive strategy to reduce all emissions from the power sector, adding this massive amount of new electricity demand will drive up emissions. Until the grid and all new generation build-out has been completely decarbonized, proof-of-work cryptocurrency miners will never exclusively rely on renewable energy to power their operations.

But cryptocurrency mining threatens to derail or reverse decarbonization in ways that go beyond simply adding electrical load. At a moment when the cost of fossil fuel generation exceeds wind or solar alternatives, the economic fundamentals of cryptocurrency mining distort the U.S. energy market and drive increased coal and gas generation.

The acceleration of cheap renewable energy in the U.S. pushed higher cost coal, gas, and nuclear plants out of service. As the cost and risk of retaining and operating coal plants increased, and the cost of new solar, wind, and storage—along with fossil gas—fell, coal plants retired in waves.[103] But to cryptocurrency miners, with their short-term focus on mining as much as possible, as quickly as possible, these same power plants look like an attractive, ready source of electricity, even if they do come with above-market rates. Ready access to transmission infrastructure, a low cost of acquisition, and utilities eager to offload liability make the purchase of otherwise uneconomic fossil fuel power plants a profitable choice for miners, at least in the short-term. In the long-term, acquisition of these power plants risks creating new long-lived environmental impacts and remediation obligations. And because cryptocurrency mining operations are focused on near-term margins, they are unlikely to foot the bill for these long-run social obligations.[104]

The largest partnerships between specific power plants and cryptocurrency mining operations we have been able to identify are at existing coal plants and gas plants that were on the verge of retirement, have struggled to find buyers, or were operating infrequently: Hardin (MT), Scrubgrass and Panther Creek (PA), Coal Creek (ND), and Merom (IN) (coal plants); and Greenidge and Fortistar North Tonawanda (NY), Odessa and Wolf Hollow (TX) (gas plants). In most cases, the resulting increased emissions of these power plants are directly attributable to the cryptocurrency mining operations that support their operations in part or in whole.[105]

These behind-the-meter operations are particularly pernicious but relatively rare. As discussed above, the majority of cryptocurrency mining operations appear to be served by electric utilities, taking service under a power purchase agreement or that utility's existing tariffs (i.e., retail rates). In both cases, energy is served by increasing the output of existing generators, or those on the operating margin, or adding new resources. In today's energy system, the operating margin is almost entirely composed of fossil generators that are able to serve incremental load.[106]

Marginal emissions, or the emissions that are associated with incremental additions or reductions in demand, vary across the country, primarily determined by the resource mix on the grid, and to a lesser extent market structures and local fuel costs. According to data aggregated by the EPA, these marginal emissions vary from half a short ton of CO_2 per MWh consumed in New England and California to just under one short ton of CO_2 per MWh in the Midwest / Central regions and Rocky Mountains, where coal dominates the margin.[107]

A 300 MW data center in Texas might be estimated to contribute 1.4 million tons of CO_2 to the atmosphere, while a similarly sized data center in North Dakota (not affiliated with a specific generator) might contribute more than 2 million tons of CO_2 to the atmosphere every year. In some cases, the net impact might be higher than the utility-wide average, such as when a utility procures from or constructs specific energy sources to serve its customers, and changes in the energy mix that serve the utility might be attributed to the new demand (at least financially).

It is at least theoretically possible for cryptocurrency miners to develop truly zero-emission sources of electricity. (See Section VIII.C below.) But simply purchasing energy from existing renewable sources is insufficient, because but for the cryptocurrency mining operation, energy from that renewable facility would be consumed by other customers. Additionality, or contracting for new clean energy sources, is key. Miners that fund *new* renewable development can fairly claim to be non-emitting. For example, Aspen Creek Digital announced in June 2022 that it is developing a 6 MW solar behind-the-meter cryptocurrency mining center in Colorado.[108] To the extent that Aspen actually builds new solar facilities and relies exclusively on the energy they produce, it is as close as feasible to a non-emitting mining facility, albeit a tiny fraction of overall cryptocurrency usage.[109] But as of this writing, we were unable to determine what, if any, steps have been taken to construct the facility.[110] The overwhelming majority of the 140 mining operations we were able to identify, in contrast, rely in whole or in part on fossil-fuel generation.[111]

VII. Cryptocurrency Mining Harms Communities and Electricity Ratepayers

A. Most Environmental Impacts from Cryptocurrency Mining Are Borne by Local Communities

The climate impacts of cryptocurrency mining will be felt globally, but the operations also have disproportionate and damaging impacts on local communities, as well as generating enormous quantities of electronic and packaging waste, which in turn cause toxic contamination where it is ultimately disposed.

1. Local Air Pollution

Cryptocurrency mining that relies on fossil fuel combustion for energy generation indirectly causes all of the air pollution impacts of the underlying combustion method. For coal combustion, this means fine particles, sulfur dioxide, nitrogen oxides, and air toxics; for gas, the biggest air pollution impact is typically nitrogen oxides. Where cryptocurrency mining occupies an existing generation plant, it is unlikely to add pollution controls unless compelled to do so. When cryptocurrency mining facilities use electricity from fossil-fueled grids, like most in the U.S. and especially so with a coal-heavy grid like Kentucky's, it increases the pollution in another community.

In fact, last year, the World Health Organization released new Global Air Quality Guidelines, finding that "[a]ir pollution is one of the biggest environmental threats to human health, alongside climate change." Air pollution exposure, especially to particulate matter, is estimated to cause 7 million premature deaths annually and result in the loss of millions more health years of life across the globe.[112]

2. Water Usage and Thermal Pollution

The environmental impacts of fossil-fueled cryptocurrency mining operations are not limited to climate and air pollution. Many cryptocurrency mining operations use water to cool their operations, whether at the site of the mining machines or the water use that comes with fossil-fueled electricity generation, or both.[113] The Fortistar North Tonawanda gas plant in New York, for example, will consume 500,000 gallons of water per day for cooling purposes once ramped up for full-time mining operations, approximately 12% of the City of North Tonawanda's current total water consumption.[114] This water will flow to the City's wastewater treatment facility, which is in need of $3 million in emergency repairs and $30 million for long term repairs, which will be borne by local residents.[115] The Greenidge gas plant, also in upstate New York, is permitted to discharge up to 134 million gallons of water, at temperatures up to 108 degree Fahrenheit, into the Keuka outlet at Seneca Lake.[116] This thermal pollution endangers health and wildlife habitability, including but not limited to potential harmful algal blooms, fish deaths, biodiversity loss and migration, oxygen depletion, direct thermal shock, and changes in dissolved oxygen.[117] And thermal pollution from the Merom coal plant in Indiana (which will supply 115 MW of power to a new AboutBit facility) has been associated with the "virtual collapse" of the largemouth bass population in the nearby Turtle Creek Reservoir.[118]

3. Fire and Safety Risk

Mining equipment operating 24 hours a day, 7 days a week in small, enclosed spaces generates tremendous amounts of heat, creating a fire risk.[119] The risks of fire at the facility can originate from "unsafe equipment, wiring failure, . . . overloading of electrical network[s], overheating of the equipment due to . . . incorrect cooling system[s]."[120] Cryptocurrency mining facilities often operate in low-tech environments, in previously unused warehouses, or old industrial sites.[121] Fires and fire risk are common enough as to drive a market in cryptocurrency mining insurance and industry "guidelines."[122]

There is also fire and explosion risk associated with electric grid equipment serving the mining operations, in addition to the mining facilities. For example, recently in Buffalo, New York, there was a fire and explosion from "faulty equipment" serving a mining operation.[123] Some localities have instituted new fire and safety regulations or instituted moratoria on the basis of fire risks for neighbors and damaged grid equipment not sized for the load.[124]

These fire risks are especially of concern in drier areas of the country where wildfires abound and especially in the dog days of summer, when drought warnings cover much of the country.[125]

4. Noise Pollution

While all fossil fuel plants entail air and water pollution, cryptocurrency mining introduces yet another local environmental harm: noise pollution.[126] Mining companies acknowledge this: Compass Mining's website explicitly states that, "Bitcoin mining isn't a quiet activity. . . A typical ASIC's noise levels range between 50 DB and 75 DB, or a noise level similar to a food blender or a loud vacuum."[127]

Neighbors have reported much worse:

- At a mining facility in **Limestone, Tennessee**, residents have described the noise as "like a jet engine idling on a nearby tarmac."[128] A commissioner who voted to approve the operation told a reporter that he has "never regretted a vote like this one. I sure wish I could take it back."[129]
- In **Cherokee County, North Carolina**, residents offer that the noise is "like living on top of Niagara Falls" and "like sitting on the tarmac with a jet engine in front of you. But the jet never leaves. The jet never takes off. . . . It's just constant annoyance."[130]
- In **Elk County, Pennsylvania**, a local farmer said, "My family, farm, and businesses have been severely impacted by the constant noise from the site, and it has led to death for some of my animals as well as health issues with my horses."[131]
- In **North Tonawanda, New York**, one neighbor described it as "that whistling and that howling and it's nonstop." Another resident stated "she continues to hear the whine one mile away from the plant.[132]
- In **Adel, Georgia**: "An inescapable drone that is driving many of them crazy. 'It's comparable to torture,' said [a] city councilor who has heard the noise and received complaints from constituents." One local resident offered, "'I wear earplugs inside my own house' . . . The noise sounds like 1,000 hair dryers blowing in unison."[133]
- In **Plattsburgh, New York**, one local resident described the "constant, high-frequency whine . . . 'like a small-engine plane getting ready to take off.' It wasn't just the decibels, but the pitch: 'It registers at this weird level, like a toothache that won't go away.'"[134]

5. Enormous Amounts of Electronic and Other Solid Waste

ASICs, the specialized machines used exclusively in the proof-of-work cryptocurrency mining process, have a limited lifespan, and recent changes in the hardware (to mine faster) potentially increase machine turnover and thus the annual amount of electronic waste.[135] Today, the average lifespan of a well-kept, maintained machine is projected to be around 3 to 5 years. In harsh or poor conditions, they can deteriorate in as little as a few months.[136]

Cryptocurrency mining results in enormous amounts of electronic waste.[137] This externality of cryptocurrency mining also suffers from a lack of data, but a recent estimate found that in 2021 alone, proof-of-work mining generated more than 30,000 metric tons of waste,[138] which is comparable to the e-waste produced by the whole country of the Netherlands.[139] Much of this waste is sent to low-income communities around the world who bear the harms of this toxic pollution but do not see any of the profits from the mining.[140]

When cryptocurrency mining operations first begin, there is also a tremendous amount of solid waste from installation and construction. One community in North Carolina, for example, needed to revise their solid waste ordinances after large amounts of solid waste could not be handled by the local waste processing center.[141]

B. Impacts on Electricity Prices for Local Residents and Businesses

In a similar vein to the problematic climate impacts emerging from proof-of-work cryptocurrency mining, these operations harm existing electricity customers both by increasing the total *quantity* of electricity needed on the grid and by introducing specific risks that are attributable to the intensity, portability, and extreme time-sensitivity of cryptocurrency mining operations. In this section, we explore the risks faced by utilities and their ratepayers, grid operators, and localities when energy-intensive cryptocurrency mining operations move in.

1. Utilities, and Their Customers, Face Unique Risks from Cryptocurrency Mining Operations

High-density electricity users such as miners frequently demand the construction of transmission and distribution lines, substation upgrades, and other infrastructure to facilitate the delivery of huge quantities of electricity to a new energy intensive mining rig.[142] Ratepayers may be left on the hook for these investments if and when a cryptocurrency mining operation abruptly leaves (as they are generally capable of doing).[143] For example, one cryptocurrency mining operation in Washington that declared bankruptcy in 2018 left more than $700,000 in unpaid utility and electricity bills.[144] Mining operations may leave solely because they can get a better deal on electricity somewhere else. For example, after the New York Municipal Power Authority increased rates for supplemental electricity used by high-density load customers in Plattsburgh because the rates for local residents there skyrocketed, many cryptocurrency miners moved west to Massena, increasing electricity costs in Massena.[145]

There is ample evidence of utilities expending significant sums to serve cryptocurrency mining operations — financial outlays that will be passed on as higher rates to the utility's other customers. Americans are already struggling to keep up with their electricity bills, particularly those living in disadvantaged communities. 25% of U.S. households (30.6 million) face a high energy burden (i.e., paying more than 6% of income on energy bills) and 13% of U.S. households (15.9 million) have a severe energy burden (i.e., paying more than 10% of income on energy).[146]

As an example of customers being stuck holding the bag for costly infrastructure upgrades, one need only look to Kentucky. There, the Kentucky Public Service Commission recently approved $12.7 million in transmission upgrades for Big Rivers Electric to provide service to Blockware Mining in Paducah, the costs of which will be allocated across all of Big Rivers' ratepayers.[147] These investments are often made instead of long-overdue transmission upgrades that would benefit ordinary ratepayers.

In addition to discounted infrastructure, Kentucky also offers discounted electricity rates to cryptocurrency mining operations.[148] Recently, Kentucky Power, a utility serving 165,000 consumers in 20 counties, recently requested additional discounted electric rates to as many as eight new cryptocurrency mining operations, which would add more than 395 MW of new load for a utility with approximately 80% coal generation.[149]

Yet many Kentucky residents and local businesses struggle with ever increasing energy burden from their bills.[150] As the executive director for Appalachians for Appalachia, recently said, "[l]ocal energy infrastructure is being pushed to the limit. Meanwhile these miners are receiving benefits that local business owners, and everyday people, are not being extended as well."[151]

Nebraska customers are also being forced to pick up the tab for cryptocurrency miners. Compute North operates cryptocurrency mining facilities where power is supplied by the Nebraska Public Power District. In 2020, the Power District spent $17.6 million, or 18% of its 2020 capital budget, constructing a transmission line and substation to increase the delivery capacity to the Compute North facilities from 30 MW to 100 MW.[152] This new infrastructure was built specifically to serve Compute North, not for general benefit — but retail electricity customers will likely subsidize the cost. Customers will do so as the $17.6 million is rolled into the Power District's revenue requirement *and* through residential rates that are higher per-kWh than Compute North itself pays.

Empirical evidence strongly supports the conclusion that cryptocurrency mining operations push electricity rates higher for the surrounding community. Several other localities have seen local electricity prices rise when proof-of-work cryptocurrency miners show up. For example, in Plattsburgh, New York, residents' electricity bills increased 30% when a mining boom came to town a few years ago.[153] A recent study found that Plattsburgh residents and small businesses paid $189 million and $90 million, respectively, more in electricity bills due to crypto's arrival.[154]

Some states, recognizing the risks of cryptocurrency mining's unique position as a new, unregulated industrial user, have begun requiring miners to pay for upgrades as opposed to passing those onto the community at large. Likewise, some utilities, recognizing the risks cryptocurrency mining operations pose to their existing customers, have begun to develop tariff provisions to mitigate these risks. In November 2021, Idaho Power became the first investor-owned utility to submit an application with its state regulator, the Idaho Public Utilities Commission, to create a separate class of "Speculative High-Density Load Customers," since the utility received at least 17 separate inquiries totaling 1,950 MW — roughly 52% of its until-then-record peak demand.[155] According to the utility, these inquiries reflected customers with: (1) high energy use and load factor; (2) the ability to relocate and disaggregate equipment to obtain favorable rates; (3) volatile load growth and load reduction; (4) high responsiveness to short-term economic signals or volatility; and (5) lack of demonstrated long-run financial viability.[156] To meet demand from these mining operations, Idaho Power would need to procure additional generation resources or wholesale energy purchases, but doing so risked over-procurement (and stranded assets) if and when these highly mobile and high-risk customers left or went out of business.[157] On June 15, 2022, the Idaho PUC approved Schedule 20 for Speculative High-Density Load[158] — finding that the new rate is "fair, just, and reasonable."[159] However, cryptocurrency mining company GeoBitmine LLC has challenged the new Schedule, leaving its ultimate fate uncertain.[160]

Similarly, prompted by approximately 150 MW of "crypto-mining related interest" in its service territory, Entergy Arkansas recently submitted a proposed tariff for "Large Power High-Load Density" customers. Entergy's filing provides more examples about how explosive growth of crypto's energy consumption can harm customers. According to testimony submitted by Entergy, a 15′ x 15′

x 30′ pod of mining machines in the New Orleans area used more energy than the nearby airport.[161] Entergy also described an incident in 2019 where a new cryptocurrency mining customer requiring significant facility upgrades opted to pay a monthly minimum for those upgrades under Entergy's tariff — only to move its shipping containers "virtually overnight" "shortly after taking service . . . effectively disappearing" and leaving Entergy unable to even reach the customer to recoup their upfront costs, forcing existing customers to pick up the bill.[162]

To prevent such interconnect-and-run incidents from recurring, Entergy Arkansas's rate filing proposes safeguards: to protect customers from a disappearing miner, new cryptocurrency customers would be required to pay a security deposit; contribute to any construction upfront; and post a surety bond or letter of credit.[163] And to address the potential increase in capacity requirement due to the influx of shipping containers full of mining equipment with insatiable energy demand, the cryptocurrency mining tariff would require miners to select between two interruptible rates that would allow Entergy or the grid operator to require the miner to cease operation on 30 minutes to an hour's notice ten to twenty times per year, ensuring the additional cryptocurrency load is available as a demand response resource and will not — at least in theory — add to Entergy's capacity obligations and require it to construct new generation resources.[164]

Some utilities have gone further in an effort to protect their existing ratepayers: the Chelan County Public Utility District in Washington instituted two moratoriums on new mining operations as well as a new rate structure to discourage miners from setting up shop within its footprint after the utility was overwhelmed by demand for cheap hydropower from crypto miners.[165] The New York Municipal Power Agency, an association of 36 municipal power authorities, petitioned the New York State Public Service Commission to prevent high-density load customers, specifically cryptocurrency companies, from requesting disproportionately large amounts of power, which according to those utilities could be up to 33% of a municipal utility's total load.[166] While not a utility, Missoula County, Montana adopted emergency "green" regulations to require cryptocurrency miners to purchase or build new sources of renewable energy to offset 100% of their energy demands.[167]

It remains to be seen whether the Arkansas Public Service Commission will approve Entergy's proposal, or whether the tariff's safeguards will be sufficient to protect Entergy's current customers from stranded transmission or generation asset costs. But utilities should consider incorporating elements of Entergy's proposed tariff or the Chelan County Public Utility District's proposed rate structure — upfront deposits, guarantees, or cost coverage for infrastructure investments; interruptible rates designed to avoid the need for new capacity buildout; and even temporary moratoria[168] as appropriate — as requests from new cryptocurrency mining customers accelerate. Fitch Ratings, a ratings agency that advises on the creditworthiness of both investor-owned and public power utilities, has already advised utilities as much.[169]

2. Rural Electrical Cooperatives and Cryptocurrency: A Costly Partnership for Ratepayers

One pattern that emerged in our research is the predilection of cryptocurrency miners for rural electric cooperatives. Rural electric cooperatives — which supply 13% of U.S. electricity to 42 million people over 56% of the U.S. land mass[170] — often lack the regulatory oversight that investor-owned utilities are subject to. Thus, rural electric cooperatives generally do not need to obtain approval from state or federal regulators to propose new rate structures or enter into large-scale contracts. Although regulation varies by state, many rural electric cooperatives have only minimal reporting requirements (such as a ten-year or integrated resource plan) to the state utility commission and most (but not all) are exempt from oversight by the Federal Energy Regulatory Commission with respect to their wholesale rates.[171] Cooperatives also lag investor-owned and municipal utilities in decarbonization; as of 2020, "six out of the top ten most carbon-intensive emitters were cooperatives."[172]

In theory, ratepayers are protected from excessive rates by cooperatives' governance structure and non-profit status. Ratepayers are also "members," who vote for a cooperative's board of directors and thus select its leadership. However, cooperative elections tend to be low-information and low-turnout, and incumbent leadership is rarely unseated. Further, under the cooperative model, if rates are higher than necessary to cover costs, any excess income is returned to member-customers in the form of "patronage capital" or "capital credits." In practice, as Representative Jim Cooper (TN) has described, cooperatives rarely provide a full and accurate accounting as to whether they have distributed patronage capital to member-customers.[173]

Without active engagement by customers (and greater transparency than cooperatives generally provide), cooperatives tend to increase sales rather than minimize rates.[174] Courting large-scale cryptocurrency mining operations is a surefire way to increase sales. The complex changing of ownership and related transactions surrounding the gigawatt-scale, coal-burning Merom Generating Station in Sullivan County, Indiana, previously discussed in Section V, is one example of a cooperative increasing electricity sales through partnership with cryptocurrency mining operations.[175] The upshot of the deal (which involves selling a coal plant to a coal mining company) is that a coal plant previously slated to retire in 2023 will now operate indefinitely.

Merom is not the only example of cooperatives entering into large-scale electricity sales to cryptocurrency mining operations with little or no transparency and at significant risk to their member-customers. Big Rivers Electric Cooperative reached a 100 MW power purchase agreement with Blockware Mining to supply its mining operation in Paducah, Kentucky.[176] According to local reporting, Big Rivers intends to spend $12.7 million on infrastructure upgrades at the proposed mining site.[177] And the Rayburn County Electric Cooperative in North Texas found that serving two cryptocurrency mines interested in connecting to the utility's service territory north and east of Dallas would require up to $40 million to fortify power lines to avoid blackouts while consuming enough electricity to power as many as 60,000 Texas homes.[178] As of this writing, it is unclear whether the Rayburn County Electric Cooperative followed through on these investments, especially considering that "upgrades to the grid threaten to drive up bills for consumers already shouldering price shocks for almost everything."[179]

3. Grid Impacts and Reliability

Proof-of-work cryptocurrency mining operations drawing energy from the grid are placing a mostly-unplanned-for load on already-strained grids across the country. In January 2022, Fitch Ratings issued research finding that "[d]igital asset or crypto currency mining in the US could pose power supply risks to public power utilities unless they are sufficiently mitigated."[180] This is largely due to cryptocurrency mining's energy intensity and ability to quickly scale operations up or down.

The sheer speed and magnitude of load growth associated with cryptocurrency mining is unprecedented and threatens the ability of both generation and transmission resources to get electrons where they are needed without overheating or unbalancing the physical infrastructure. For example, if mining operations for which we were able to find SEC reports and other data expand to the extent their literature suggests, by the fourth quarter of 2022, there could be up to 1,626 MW of demand directly for proof-of-work mining operations in New York State alone. Assuming these facilities operate 24/7/365, their annual energy use of over 14,000 GWh would be a whopping 9.5% of New York State's total 2020 electricity consumption.[181]

Perhaps the most worrying site of potential grid instability due to cryptocurrency mining load increases is Texas, and how that impacts Texans both from a safety perspective and financially. The instability of Texas's grid was exposed, with tragic consequences, by Winter Storm Uri in February 2021, in which at least 246 people lost their lives,[182] and 69% of Texans lost electricity for an average of 42 hours.[183] Evidence is also becoming public that cryptocurrency miners are taking advantage of such extreme weather. One cryptocurrency miner resold electricity valued at more than $125 million to the Texas grid during that storm and the state still owes the miner $86 million, with that amount likely to be paid by ordinary utility customers.[184]

A February 2022 report by five former Texas Public Utility Commissioners and a former regulatory advisor found that ERCOT still has not improved its ability to restart power plants during a blackout, improved its load forecasting and resource assessments (including accounting for extreme weather), or adequately winterized the state's gas system.[185] In 2021, an analysis by ERCOT found that four of the five extreme risk scenarios considered by ERCOT would leave the grid short of a significant amount of power.[186]

Yet, as of August 2022, 33 GW worth of cryptocurrency mining operations have applied to connect to the Texas grid over the next several years—a third more than ERCOT's announcement in April 2022. [187] This 33 GW figure represents 41% of ERCOT's record peak demand of 79.8 GW on July 20, 2022.[188] By some measures, this is equivalent to New York State's entire energy demand.[189] If the cryptomining facilities run at an 85% load factor, the would consume as much electricity as the entire state of Florida.[190] Wood Mackenzie predicts that Bitcoin mining could more than double the *rate* of demand growth in ERCOT's territory.[191]

Further impacting average Texans, it appears that cryptocurrency miners are buying electricity low and selling it high. As the Tech Transparency Project recently found: "Programs that appear to be unique in the country allow miners to leverage their contracts to resell electricity at massive mark-ups and collect millions of dollars in incentive payments from the state grid operator. . . . Some miners already view themselves as energy traders. One bitcoin miner called his company '[a]n energy arbitrage operation disguised as a bitcoin mining company.'"[192]

In response to the overwhelming influx of cryptocurrency mining, ERCOT has instituted new processes aimed at ensuring the system can handle the enormous load.[193] As a temporary measure, ERCOT will now require new, large cryptocurrency miners to seek permission to connect to the state's power grid and will require utilities to submit studies on the impact of miners and other large users on the grid.[194] Any project that will add 20 MW of demand on the site of a generator within the next two years, and any project that will add 75 MW of demand without its own power generation on site within the next two years, will have to undergo a review process.[195] Local officials are also sounding the alarm on grid instability that would be caused by cryptocurrency mining operations. For example, the City of Brenham's Planning and Zoning Committee said that the city's current power grid cannot sustain the amount of electricity required for large scale and commercial-like cryptocurrency mining setups, thus necessitating the committee halting the approval of more mining setups.[196]

4. Tax Incentives for Cryptocurrency Miners are Breaking the Bank

Making matters worse, some states provide additional subsidies or tax breaks in an effort to encourage cryptocurrency mining operations. Kentucky passed a law last year that waives taxes on energy purchases by cryptocurrency mining companies, while Wyoming exempted from taxes any natural gas used to power mobile mining rigs. In 2021 alone, a total of 33 states had bills supporting cryptocurrency developments and 17 enacted new laws to create working groups, provide tax breaks, and/or establish subsidies for cryptocurrency mining operations, according to the National Conference of State Legislatures.[197]

Kentucky has proven particularly short-sighted in offering benefits to cryptocurrency miners in addition to discounted electricity, offering cryptocurrency-specific tax incentives estimated to cost Kentucky taxpayers at least $9 million a year in lost revenue.[198] These tax incentives include "tax exemptions totaling 9 percent on electricity consumed at larger cryptocurrency mining operations, . . . sales-tax refunds on mining equipment, as well as potential incentives on income taxes and wage assessments."[199]

Kentucky is not alone. In Texas, the City of Corpus Christi is forgoing $7 million annually in sales tax and franchise fees, equating to $70,501,509 over ten years, to accommodate Bootstrap Energy's $1.1 billion cryptocurrency mining operation.[200] Bootstrap has contracted with AEP Texas for 600 MW.[201]

5. Reports of Cryptocurrency Mining Jobs Have Been Greatly Overstated

Despite the purported economic development justification for cryptocurrency mining incentive programs, these operations actually create few jobs. Most of the work that is created at cryptocurrency mining sites is hiring temporary workers to set up the mining machines; less than a dozen people may be required to maintain the operation. As a Berkeley Haas professor similarly observed: "These are warehouses full of computers and they only require one or two IT people to run the whole operation, so it's unlikely that it brings jobs or stimulates the economy."[202] And Fitch Ratings found "[c]ryptocurrency mining operations typically bring in very little additional economic benefits in the form of jobs or ancillary business to a local economy."[203]

Here are just a few examples of the meager job benefits of cryptocurrency mining operations:

- The **Blockware Mining** operation in Paducah, Kentucky will provide just 10 full-time jobs in its initial phase.[204]
- **Core Scientific**, with seven facilities, reported 205 full-time employees in the United States, as of December 31, 2021.[205]
- **Marathon Digital Holdings**, which mines cryptocurrency in Montana and Texas, has nine full-time employees, as of December 31, 2021.[206]
- **Stronghold Digital Holdings**, which mines cryptocurrency in Pennsylvania, has 16 full-time employees, as of March 24, 2022.[207]
- **AboutBit**'s $50 million facility adjacent to the Merom coal plant in Indiana is expected to create 15 jobs.[208]
- The **Greenidge** cryptocurrency mining operation in New York employed 5 union workers on site as of October 2021.[209]
- "A $1.9 billion facility by **FX Solutions** and **Atlas Power** near Williston, North Dakota, would create around 100 temporary construction jobs and support only 30 employees over the long-term. Meanwhile, the first stage of the project would draw 240 MW of electricity—roughly, the amount of energy needed to power the city of Fargo—and eventually ramping up to a powerhouse 700-megawatt scale."[210]
- "In Rockdale, Texas, during the BTC boom of 2017, a cryptocurrency mining company promised to build

the largest crypto mining facility in the world—one that could eventually be used for other data-driven applications and create more than 300 jobs. In reality, the facility only generated 14 of 350 promised jobs and was quickly scaled back."[211]

The municipalities who handled an earlier boom in cryptocurrency mining in the mid-2010s can attest to the lack of economic development benefits from cryptocurrency mining. The former mayor of Plattsburgh, New York has said that due to the automated nature of these servers, the new mines provided few local jobs: "when you look into it, and I have—[the jobs,] they just don't materialize."[212] "I'm pro-economic development, but the biggest mine operation has fewer jobs than a new McDonald's."[213] The former head of the Bonneville Power Administration and Chelan County Public Utility District testified before the U.S. House Energy and Commerce oversight subcommittee panel, stating that: "we heard substantial reservations from our community about supporting cryptocurrency mining due to . . . [the r]elatively low number of local jobs per unit of electricity consumed."[214]

For local communities, the above-described tax incentives and promise of jobs that do not materialize end up being a bad deal; a recent Forbes study estimated that cryptocurrency mining tax incentives end up costing counties and municipalities across the U.S. roughly $1 million per job.[215] As one reporter who interviewed community members in Kentucky observed: "Some see echoes of what they say were the worst elements of the now largely defunct coal industry: out-of-state money, absentee owners, and huge fortunes made with little wealth trickling down to local communities."[216]

VIII. Breaking Through the Bitcoin Myths

Proponents of proof-of-work cryptocurrency often make grandiose statements about how energy-intensive mining advances environmental and climate goals, using a variety of half-truths and cherry-picked information. In this section, we explore the narratives and messaging used by proof-of-work miners, identify the elements of truth that make some of these statements so confounding, and explore how climate and environmental advocates can probe these often deeply misleading statements.

Myth 1: Cryptocurrency Mining is Already Sustainable Because it is Located *Near* Clean Energy, or Because it Purchases Renewable Energy Certificates or Carbon Offsets

1. Claims of Co-Location

It is not uncommon for cryptocurrency mining companies and advocates to tout that, while their operations are energy intensive, they are "sustainable" or run on renewable energy.[217] One industry-funded organization, the Bitcoin Mining Council, claims 58% of energy used to power Bitcoin in 2020 was from renewable sources, based on selected companies' self-reporting.[218] The Cambridge Centre for Alternative Finance puts this number much lower—at 39%.[219]

What explains the discrepancy? In many cases miners are claiming (or implying) "renewable" energy simply by being in proximity to wind or solar farms with which they have no contractual relationship. In our opinion, they're greenwashing.[220]

For example, in Argo Blockchain's 2021 Sustainability Report, released August 18, 2022, the company claims that it "is taking action against climate change" by "select[ing] sustainable energy sources."[221] Argo's primary mining facility is the Helios facility, a 200 MW facility east of Lubbock, Texas. Argo does not hold a power purchase agreement with a renewable energy provider, instead noting that "Argo currently uses grid electricity in a low carbon part of the ERCOT market,"[222] and has purchased renewable energy certificates (RECs).[223]

But simply locating new demand in a region rich in renewable resources does not mean that the new demand is served by the renewable resources of that region. When a load is added to the grid, it is served by the generation available on the grid at the time electricity is consumed (unless it specifically causes new generation to be built for its exclusive use). Large loads, like cryptocurrency mining operations, can themselves cause changes in the generation mix as the grid dispatch patterns shift in response to the new load's requirements. The generators that adjust output in response to load changes will set the "marginal" emissions rate.[224] In almost every circumstance, new demand drives an instantaneous increase in the output of fossil generators.[225]

For example, the aforementioned Argo Helios facility in West Texas pays for market-based grid generation, and therefore drives changes in marginal generation in Texas, which is typically gas and coal. According to recent research from the Proceedings of the National Academies of Science, while the average emissions rate of all generation in West Texas has fallen to about 0.375 tCO_2/MWh, the marginal emissions rate holds steady at around 0.5 tCO_2/MWh, or equivalent to the output of a gas-fired generation station.[226] The current wind in West Texas will generate irrespective of whether Argo's Helios facility exists or not. Argo does not pay for incremental wind generation, and has not built wind to serve its facilities. Therefore, it drives existing fossil-based generation to increase its output—and results in an increase in emissions.

2. Claims of "Carbon Neutrality" by Purchasing Renewable Energy Certificates or Carbon Offsets

Co-location is not miners' only form of greenwashing. Miners often claim "carbon neutrality" when in fact they are simply purchasing offsets or renewable energy certificates—paying renewable generators elsewhere while increasing load on (and pollution from) fossil fuel plants locally.

Examples abound. In late 2021, at the opening of its massive Denton, Texas facility, Core Scientific claimed that it would "increase the Company's total power capacity to more than 800MW while remaining 100% net carbon-neutral."[227] This claim of carbon neutrality is entirely based on unbundled renewable energy certificates (RECs).[228] Prior to Denton, Core's largest facility was a 125 MW facility in Calvert City, Kentucky, opened in late 2019. Core Scientific's Calvert City facility holds a contract with the Tennessee Valley Authority, a provider whose resource mix is just 3% wind and solar.[229] And yet Core Scientific's claimed carbon neutrality is entirely based on RECs it purchases from wind farms in North Dakota.[230] Argo Blockchain, discussed above, too has purchased renewable energy certificates to offset its fossil generation.[231]

Separate from RECs, several mining companies rely on purchase of carbon "offsets" to advertise to the public and their investors that they are a sustainable operation. For example, Greenidge Generation LLC has claimed that it is "significantly reducing greenhouse gas emissions now," by purchasing voluntary carbon offsets, despite using a fossil gas plant 24 hours a day to mine cryptocurrency.[233] As a general matter, many carbon offsets programs are unverifiable and hard-to-measure, and in many instances, not actually reducing carbon pollution.[234] That being said, non-proof-of-work blockchain technology could be a key tool in properly verifying whether offsets are achieving

Claims of Carbon Neutrality via Voluntary REC Purchases

To drive clean energy buildout, some states have established renewable portfolio standards (RPS), that require a certain minimum amount of electricity to be generated by "renewable resources." Most states allow utilities to demonstrate compliance with RPS by retiring RECs. Utilities can either generate their own RECs through their own renewable resources, or can purchase RECs on the market. RECs can be purchased with or without the associated electricity. RECs that are purchased without the accompanying electricity are known as "unbundled RECs." Each REC represents the non-energy attributes of a megawatt-hour generated by renewable energy resources. In other words, when you purchase a REC, you're purchasing the legal right to claim all of the "renewableness" of that electricity. Often the REC will also include the avoided emissions value of that MWh of electricity. However, the avoided emissions value of any particular MWh of renewable energy is highly dependent on the grid mix and marginal resource at the time the MWh is generated. In other words, the avoided emissions value of a REC can vary from state to state, month to month, and hour to hour. Because clean energy deployment today far exceeds RPS standards in most states, there is a glut of RECs on the market. Some people and businesses purchase these excess RECs in order to claim their homes or businesses are powered by clean energy. In some cases, these REC purchases can effectively spur new clean energy development that offsets fossil energy: specifically, this can occur where the demand for the REC is incentivizing the construction of new, additional renewable electricity that would otherwise not be built. But in most cases, REC purchases provide little or no additionality: usually, REC sales revenues are not driving the decision about whether to build a new wind or solar facility. A clean energy project would have been built irrespective of the REC sale. Where the REC sale is not the result of additional, incremental clean energy development, it has little or no incremental climate benefit.[232]

reductions in pollution.[235] But, the key is to reduce pollution in the first place, not create a problem and then seek creative new ways to account for the harms.

Myth 2: Cryptocurrency Mining Uses Energy That's Being Wasted From Variable Wind and Solar Output

One of the most common storylines from cryptocurrency mining proponents is that cryptocurrency mining thrives on energy that would otherwise be wasted from "curtailed" solar and wind projects.[236] Curtailment for wind and solar projects occurs when an energy system produces more electricity than can be absorbed by demand at a particular moment, or more electricity than can safely fit on a transmission system. In these circumstances, grid operators will direct to generators to reduce, or cease operations. Wind and solar projects are particularly susceptible to curtailment because they have almost no cost to start and stop, unlike large thermal generators that may take hours to turn off, or even succumb to damage if turned off too quickly.

As renewable energy penetration has grown, so has curtailment. In California's electricity market (CAISO), curtailment has risen to 2.1 million MWh in 2022—or an 81% increase from 2021.[237]At a first glance, it might therefore appear that CAISO could handle a 200 MW cryptocurrency facility to harness the 1.5 million MWh of "wasted" energy in 2021.[238] In reality, curtailments are sporadic. Measured in five-minute increments in California, there were only 15% of hours in which curtailments rose above 200 MW in 2021.[239] In other words, a 200 MW mining facility in California could have only operated on "free" just energy 15% of the time, a daunting prospect for an industry that typically requires mining operations to operate around-the-clock to be profitable. A 2019 paper exploring cryptocurrency use of curtailed resources concluded that a cryptocurrency operation seeking to maximize profit by operating only on curtailed energy would only operate about half the time, and that a cryptocurrency mining operation scaled to consume all of the curtailed energy would lose an extraordinary amount of money.[240]

Even if absorbing curtailed wind and solar worked in theory, in practice it ignores that clean energy developers actively seek to avoid curtailment by integrating into regions not susceptible to oversupply. Further, utilities, states, and the federal government are working quickly to build transmission that would relieve congestion and constraints that can lead to curtailment. And, finally, energy storage (i.e., batteries) work to both absorb any excess clean energy *and* redeploy it during hours of need, presenting a far superior solution to the problem of curtailment.

Only in the edge cases where an extraordinary amount of clean energy is built without storage or sufficient transmission, or where cryptocurrency miners are willing to locate behind transmission constraints, run at thin capacity factors, and cease operations when transmission and/or storage come online does this thesis hold water. We are not aware of any cryptocurrency mining facilities currently operating in the U.S. that were built—or financed—with these constraints in mind.

Myth 3: Cryptocurrency Mining Incentivizes Clean Energy Development, or Helps to Decarbonize the Grid

Proof-of-work enthusiasts argue cryptocurrency mining will drive clean energy development and decarbonize the grid.[241] The most carefully constructed of these arguments essentially stipulates that the primary barrier to massive clean energy deployment is transmission congestion (causing curtailment and reduced economic margins for new renewable development) and integration (lengthy queues to interconnect to regional grids). Proponents argue that the incremental revenue from cryptocurrency mining could incentivize the development of wind and solar energy that would otherwise not be deployed, either because grid revenues are insufficient or because a location is transmission congested.

But this theory rests on the same faulty assumptions as the "waste electricity" thesis: that renewable developers will gamble on long-term transmission build-out and cryptocurrency miners will be willing to forgo mining (and profits) whenever wind or solar generation dips—and cease operations or limit itself to curtailed electricity once the renewable resource can serve a general load.

The leading thought paper on cryptocurrency mining as a driving force for more clean energy acknowledges that mining operations would likely "still mine with grid electricity during other periods when profitable to do so, so it wouldn't be entirely green from day one."[242] But more to the point, if a clean energy facility is built entirely to serve a cryptocurrency mine without respect to its ability to serve the remainder of the grid effectively—or at all—then it has little to no value in decarbonizing the remainder of the grid.

Moreover, there are other constraints to clean energy deployment beyond interconnection delays (or curtailment caused by inadequate transmission infrastructure): supply chain (i.e., materials), state or local policies, land use, and labor availability. To the extent cryptocurrency miners induce developers to locate wind and solar farms at non-grid useful locations that remove clean energy from the critical supply chain, they remove opportunities to decarbonize other elements of the grid.

Even if a mining operation did incentivize new renewable development in a location where interconnection delays were the only barrier to development, to further grid decarbonization, the mining operation would have to go away in a timeframe that is relevant for decarbonization. For that renewable resource to have decarbonization value, it must *offset* existing fossil fuel use in some way, either by reducing utilization of fossil fuel power plants, or enabling electrification of other end uses traditionally powered by fossil fuels, such as transportation or home heating. To realize that outcome, the cryptocurrency mining facility must cease to exist, allowing that electricity to flow to those other purposes. As of yet, no proof-of-work proponents have come forward with a solid plan that would allow a developer to build clean energy for an offtaker that expects to go out of business.

Instead, miners have done the opposite. For example, Compute North has recently announced that it has energized a new 280 MW mining facility near Odessa, Texas, which sits "behind the meter" at a wind farm.[243] The wind farm in question is King Mountain Wind Ranch,[244] a 278 MW wind farm built in 2001 and owned by FPL (NextEra).[245] For the last two decades, King Mountain has contributed to the larger Texas grid, and will now be taken *out* of circulation for grid use. So, while the Compute North facility may be able to legitimately claim that it uses primarily wind energy, this type of project is not additional and is not contributing to broader decarbonization of the energy system. Instead, it represents price seeking behavior from the wind farm owner, resulting in *less* overall renewable energy on the broader grid.

Myth 4: Cryptocurrency Mining "Acts Like a Battery"

Cryptocurrency mining proponents make the perverse claim that "Bitcoin mining is strengthening the grid,"[246] and "provide[s] critical grid reliability products usually provided by fossil fuel plants."[247]

Mining operations simply do not provide ancillary services, such as load balancing, that maintain the operability of the grid. They also do not provide storage capacity. Energy consumed by a mining operation cannot be exported or redeployed.

When miners talk about "grid benefits," they are actually touting an ability that *all* large-scale customers have: The ability to shut off in emergencies or periods of peak demand. In the middle of a heat wave causing high electricity demand, Texas Bitcoin miners voluntarily shut down their operations, curtailing 1,000 MW of load in mid-July 2022 for 3.5 hours.[248]

But is cryptocurrency miners' willingness to pause operations during times of high demand and grid strain really a grid service? As external experts put it: it's complicated.[249]

For most grids, the demand for electricity varies hour by hour, day to day, and month to month. On particularly hot or cold days, demand may spike well above normal use. The cost of maintaining capacity to serve those peak hours, and the cost of operating the most expensive generators to serve these peak hours, can be extreme—but failing to serve load during the highest moments of strain can be even more costly for customers. Utilities and grid operators often hold capacity in reserve simply to serve those peak conditions.[250] Paying a customer with non-essential energy needs to reduce their demand can be a way of aligning demand with supply and retaining reliability, a practice known as "demand response."[251]

Most industrial customers do not adjust their energy use based on the real-time price of electricity, which constitutes a relatively small portion of their overall costs (and thus any savings would be heavily outweighed by disruptions that might have cascading impacts on meeting production deadlines, etc.). Demand response payments help make non-price-responsive customers responsive: a manufacturing plant might incur substantial operational cost and product risk when it stops operation, or other types of data centers may impair customer services by ceasing operations. But cryptocurrency miners are only responsive to electricity prices, and have no other service provided to customers aside from processing cryptographic puzzles: if the cost of energy rises above their breakeven, they can simply cease operations without experiencing additional costs or inconvenience.[252]

Unless a demand response program is carefully calibrated to cryptocurrency miners' extremely low costs of temporality paused operations, miners effectively become energy traders, able to convert cheap electricity into cryptocurrency most hours, while also receiving high prices for foregone electricity during peak periods or emergencies. During this summer's heat wave in Texas,[253] Riot Blockchain announced that it received $9.5 million (equaling the value of 439 Bitcoin at the time) in demand response payments in July alone.[254] In addition to this hefty payout, Riot still was able to mine 318 Bitcoin that month.[255] In fact, demand response company Voltus estimates that a cryptocurrency mining company can generate up to 10% of its annual revenue by providing shutdown services to the grid.[256]

By increasing the demand on the grid, miners increase the need for demand response, the cost of such programs, and thus the cost of providing electricity to all other customers.[257] ERCOT's independent market monitor expects that Texans could be paying an extra $1.5 billion for electricity this year alone[258] — partially to pay cryptocurrency miners to shut down their operations during high demand.

As explained by Professor Severin Borenstein,

> *[T]he crypto mining business model is based on buying electricity at wholesale prices or on a real-time variable price tariff. They would already have a strong incentive to cut back during grid emergencies without the additional payments from the demand response program, especially in Texas with its $5000/MWh wholesale price cap. That means the mining companies get paid for taking demand off the grid that they never would have put on the grid at those high prices anyway.*[259]

Myth 5: Cryptocurrency Miners are No Worse than Any Other Electricity Users

Many miners will respond to critics of its insatiable need for energy by comparing it to other industries such as banking, telecommunications, or to data center operations.[260] But as described above, the huge premium placed on immediate access to large amounts of electricity without the long-term commitments necessary to finance renewable development attract cryptocurrency miners to fossil fuel sources, such as Hardin, Greenidge, Merom, Scrubgrass, or coal-heavy grids like Kentucky's.

Electricity demand in comparable sectors has not increased and, in some cases, even declined as energy efficiency increased.[261] For example, electricity demand by data centers has not increased, even though internet traffic and data center workloads have increased significantly.[262] In sharp contrast to cryptocurrency mining, data transmission networks and mobile communications networks are rapidly becoming more energy efficient.[263] However, even as ASICs have become more energy efficient than the hardware previously used for cryptocurrency mining, the efficiency gains have not resulted in decreased overall energy consumption because of the substantially increased scale of mining.[264]

Moreover, Bitcoin's ratio of energy consumption to human participation — people actually buying Bitcoin, holding it, or even working at mining facilities — is wildly larger than other electricity users. Bitcoin already uses half as much electricity as the entire global banking sector, according to one estimate, and will overtake the banking sector within two years if current trends continue.[265] One study estimates that the average electricity footprint of non-cash transactions by the global banking system is no more than 0.4 kWh, while the average electricity footprint per Bitcoin transaction ranges from 491.4 kWh to 765.4 kWh.[266] By some estimates, a single Bitcoin transaction uses more energy than 100,000 Visa transactions.[267]

IX. Recommendations to Mitigate the Risks of Proof-of-Work Cryptocurrency Mining

Proof-of-work cryptocurrency mining poses significant risks to grid stability, retail electricity rates, our climate, and local air and water quality. Therefore, policymakers and regulators at all levels of government, as well as utilities and impacted community members, should review proof-of-work cryptocurrency mining proposals carefully with these risks in mind.

Because the type of operations and impacts of cryptocurrency mining vary from community to community, solutions will necessarily be project-specific. As such, we offer the following high-level recommendations to policymakers, regulators, utilities, and impacted community members as they face the risks of proof-of-work cryptocurrency mining.[268]

LOCAL GOVERNMENTS, DECISION-MAKERS, AND COMMUNITY MEMBERS

Given the significant local impacts and outsized role of local decision-making in the approval process for cryptocurrency mining operations, local governments, including zoning and planning boards, as well as community members are on the front lines of the cryptocurrency mining boom. As such, local actors should approach proposals for new cryptocurrency mining facilities with an eye toward noise pollution, whether they truly create stable, good-paying jobs, what grid and infrastructure upgrades are needed, fire and safety risks, as well as increases in local air, water, and solid waste pollution.

- **Mitigate local air, water, and solid waste pollution.** In addition to any local air pollution from the electricity generated to power mining operations, mining operations can use significant amounts of water for cooling. In water-constrained areas of the country, local regulators should assess the consumptive needs of cryptocurrency mining operations, particularly if the mining operation uses municipal (i.e., treated) water supplies that might impact residential water costs. In addition, mining equipment, after their useful lives are over, contribute to significant e-waste pollution. The initial construction of a mining facility also creates a large amount of solid waste. Preventative measures can be taken to ensure recycling and proper waste handling. States and municipalities with climate laws and regulations on the books are well-situated to make some of these arguments.
- **Calibrate or forego economic development incentives.** Cryptocurrency mining operations offer relatively few local jobs. Prior to offering economic development incentives, local governments should require cryptocurrency miners to provide a guarantee for a high number of local jobs over a sustained period. Any tax incentives or local municipal utility incentives should be carefully weighed against a realistic assessment of job growth potential, as well as other costs borne by the community as a result of the operation.
- **Ensure miners bear their fair share of grid and infrastructure upgrade costs.** Large energy consumers such as cryptocurrency mining operations may require grid and infrastructure upgrades, which may be paid by local governments or all electric utility customers. Utility regulators and local governments should ensure that ratepayers and community members do not foot the bill for these projects unless they benefit the community as well.
- **Protect against fire and safety risks.** Cryptocurrency mining rigs can present a unique risk of overheating and fire risk. Local governments should ensure that facilities have the technical capacity to mitigate fire, and carry appropriate levels of insurance. Additionally, local governments in cold weather climates can require the excess heat from cryptocurrency mining operations to be recycled for local benefit.
- **Consider noise pollution mitigation.** Cryptocurrency mining operations can be extremely loud operations. Local governments can review, update, and enforce noise ordinances to mitigate noise levels.
- **Update local land use codes.** Planners and local leaders are working on model codes for communities. For example, the American Planning Association recently published a Zoning for Data Centers and Cryptocurrency Mining Guide.[269] Many zoning codes from communities who have already implemented such codes are available online as well, including from municipalities across the country.[270]

ELECTRIC UTILITY REGULATORS

Cryptocurrency mining operations in the United States have, thus far, sought to build new mining facilities in jurisdictions where energy costs are low and easy to access, and where regulators either encourage electricity consumption as economic opportunity (or supportive of utilities), or where there is relatively thin regulatory oversight. State and local utility regulators, including officials that oversee municipal utilities and rural electric cooperative board members, public utilities commissions, energy regulators, and regional energy system market monitors can provide critical ratepayer protections.

- Utility regulators should refuse to approve power purchase agreements with cryptocurrency mining operations unless those utilities can demonstrate the agreement will not adversely impact other ratepayers, including by raising rates or otherwise increasing costs. State regulators and lawmakers should work with non-jurisdictional utilities, such as municipal and cooperative utilities, to do the same.
- Utility regulators should ensure that cryptocurrency miners are not provided discounted rates, and instead allocate costs and adopt rates in a manner that protects existing consumers from higher wholesale costs, cost shifting, and stranded assets. In fact, several utilities have argued that cryptocurrency mining operations should face substantially higher rates than other industrial consumers given the short-term view of the industry. In the short run, new utility infrastructure may be required to support mining center interconnection, and over the long-run, utilities may need to procure new generation to serve substantial new load. Utilizing traditional “cost causation” principles, utility regulators should ensure that mining operations pay their fair share over the short- and long-run.

- Utility regulators should critically assess utility plans to increase or maintain obsolete capacity (such as old fossil generators) in response to cryptocurrency mining operations, and ensure that existing ratepayers are held harmless. These reviews can occur in resource planning, procurement, or rate proceedings, and through other regulator inquiries.
- Utility regulators should consider Systems Benefit Charges (SBCs), or on-bill surcharges to cryptocurrency mining operations, to fund mitigation measures and protect ratepayers against stranded asset costs.
- Utility regulators, market monitors, and federal electricity regulators should review the impact of cryptocurrency mining operations on regional resource adequacy and the cost to serve customers. In non-restructured (i.e., non-market-based) regions, utility regulators should assess if cryptocurrency mining impacts utility load forecasts and system costs. In restructured states, market monitors should assess the impact of mining operations and load increases on the wholesale cost of energy and grid congestion. This necessarily requires a comprehensive reporting requirement for mining operations to ensure accurate data needed for planning.
- State environmental and energy regulators should establish and require best management practices for high-density load energy users, including but not limited to energy efficiency requirements, power density limits that set caps on the number of kW of energy consumption or load per thousand square feet, and take service as fully interruptible load.

ELECTRIC UTILITIES AND GRID OPERATORS

- Utilities should develop rate structures for high-density energy users such as cryptocurrency miners that ensure those operations pay their fair share of infrastructure upgrades at the time of interconnection (either through a deposit requirement or other mechanism); incorporate interruptibility provisions to avoid, where possible, increases to the utility's capacity obligations necessitating new generation build-out; and protect customers from rate shocks due to either the magnitude of new requests or the sudden departure and resulting stranded assets.
- Independent system operators should develop guidance around the interconnection of large-scale, high-density electricity users, including emergency response rules, that prioritize the integrity of grid operations and treat cryptocurrency mining as the highly interruptible, "flexible" load it claims to be.

FEDERAL AND STATE POLICYMAKERS AND REGULATORS

- States should consider imposing a moratorium on cryptocurrency mining operations until the impacts on climate goals and energy costs can be ascertained and mitigated. New York State is already considering such a moratorium, and several municipalities have already implemented them. In the absence of a moratorium, state environmental regulatory agencies should take a hard look at fossil power plants purchased or primarily serving cryptocurrency operations, including whether those plants are properly operating under previously obtained permits. In states with oil and gas drilling, stronger and more proactive enforcement may be required to stop unpermitted flare mining operations.
- Below are additional options that state policymakers and regulators should consider:
    - Reviewing a cryptocurrency mining facility's local and state environmental permits, including local stormwater and solid waste permits, as well as air and water permits.
    - Establishing revenue assurance or bonding requirements as a way to protect customers in the event that a high-density-load customer does not pay its utility bills.
    - Regulating electronic waste and other solid waste from proof-of-work cryptocurrency mining operations.
    - Creating a registry for proof-of-work mining over a certain megawatt threshold and requiring those operations to disclose their energy source.
    - Establishing minimum energy efficiency limits, for both the mining rigs themselves or one set around a kWh per transaction or block.
    - Requiring public power authorities to halt all discounted energy provided to proof-of work mining operations.

Acknowledgements

"We would like to thank the following individuals for their review of and/or contributions to this paper: **Irene Weiser**, Fossil Free Tompkins; **Joseph Campbell** and **Yvonne Taylor**, Seneca Lake Guardian, a Waterkeeper Alliance Affiliate; **Pamela Wellner**, Amplify Eco; **Karen Edelstein**, FracTracker Alliance; **Lane Boldman**, Kentucky Conservation Committee; **Rob Altenburg**, PennFuture; **Anne Hedges**, Montana Environmental Information Center; **Michael Brune**, Change the Code, Not the Climate campaign; **Mini Saraswati**, Sierra Club; **Liz Moran**, **Thom Cmar**, **Angelica Navarro**, **Sean Woody**, **Trish Bosch**, **Maya DeGasperi**, and **Michael Worrall**, Earthjustice; as well as Global Energy Monitor. The Sierra Club also acknowledges the work of the Pennsylvania Environmental Law Project (**Ryan Baldwin**; **Matt Burner**; **CeCe Coffey**; **Nathaniel Edelheit-Rice**; **Ellen Heiman**; **Omar Khodor**; **Jessie Levin**; **Yuxuan** Liu; **Ronni Mok**; **Xiaoshu Ruan**; **Runrun Yang**; and **Michael Zschokke**) for their assistance in our initial investigation into this topic area. Finally, we would also like to thank the many partners we have been collaborating with on this issue."

Endnotes

1 Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/index.

2 *Id.* (recording energy consumption every quarter); a 700 MW power plant operating at 70% capacity factor (*i.e.*, average output) produces just over 1 TWh over a three-month period. Bitcoin prices fell from a high above $60,000/BTC in late 2021 to less than $20,000/BTC in third quarter 2022. CoinMarketCap, *Cryptocurrency Historical Data Snapshot* (last visited Aug. 25, 2022), https://coinmarketcap.com/historical.

3 Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/index.

4 IPCC, *Working Group III Contribution to the IPCC Sixth Assessment Report* (AR6), Chapter I, at 1-26:20-21 (2022), https://report.ipcc.ch/ar6wg3/pdf/IPCC_AR6_WGIII_FinalDraft_FullReport.pdf (IPCC Assessment Report) (citing Camilo Mora et al., *2018: Bitcoin emissions alone could push global warming above 2°C*, 8(11) Nat. Clim. Chang. 931 (Oct. 2018), https://www.researchgate.net/publication/328581842_Bitcoin_emissions_alone_could_push_global_warming_above_2C); *IPCC Assessment Report,* at 5-57 to 5-58, https://report.ipcc.ch/ar6wg3/pdf/IPCC_AR6_WGIII_FinalDraft_FullReport.pdf.

5 White House Office of Science and Technology Policy (OSTP), *Climate and Energy Implications of Crypto-Assets in the United States,* at 15 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

6 That is, if you added up all the "value" associated with cryptocurrencies based on their current exchange prices, Bitcoin holdings would constitute 40% of that total dollar amount. Based on top 200 cryptocurrencies by market capitalizations, as of July 31, 2022. CoinMarketCap, *Historical Snapshot - 31 July 2022,* https://coinmarketcap.com/historical/20220731/.

7 Hanna Lang, *Explainer: Understanding Ethereum's major 'Merge' upgrade* (Sept. 9, 2022), https://www.reuters.com/technology/understanding-ethereums-major-merge-upgrade-2022-09-09/.

8 Jeff Cox, *Bitcoin price falls after China calls for crackdown on crypto mining*, CNBC (updated May 22, 2021), https://www.cnbc.com/2021/05/21/bitcoin-falls-after-china-calls-for-crackdown-on-bitcoin-mining-and-trading-behavior.html; *China to shut down over 90% of its Bitcoin mining capacity after local ban, Global Times* (June 20, 2021), https://www.globaltimes.cn/page/202106/1226598.shtml.

9 Jerry Shih, *Bitcoin miners exit China, beat a path to the U.S. as crypto climate shifts, Seattle Times* (June 21, 2021), https://www.seattletimes.com/business/bitcoin-miners-exit-china-beat-a-path-to-the-u-s-as-crypto-climate-shifts/. Miners also migrated, to a lesser extent, to Kazakhstan. Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index; Bitcoin Mining Map* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/mining_map.

10 MacKenzie Sigalos, *How the U.S. became the world's new bitcoin mining hub,* CNBC (July 17, 2021), https://www.cnbc.com/2021/07/17/bitcoin-miners-moving-to-us-carbon-footprint.html.

11 The pace of migration of mining from China to the U.S. is spelled out starkly in the public filings of some mining companies. For example, such as. In Bit Digital's May 2022 prospectus, the company notes that "In October 2020, we commenced our strategy of migrating assets from China to North America. . . . From April through June 2021, we migrated 14,500 miners from China to the United States." Bit Digital, *Form 424B3, Prospectus,* at 10-11 (May 5, 2022), https://www.sec.gov/Archives/edgar/data/1710350/000121390022024123/ea159396-424b3_bitdigital.htm. To put this number in context, based on Bit Digital's portfolio of miners, each of which consumes between 2.1 and 3.4 kW, the three-month migration from China was equivalent to an instantaneous load of approximately 45 MW.

12 Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index; Evolution of Country Share* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/mining_map.

13 Authors' calculations based on estimated electricity consumption and U.S. share of Bitcoin mining operations in January 2022, from Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index, Bitcoin Mining Map* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/mining_map.

14 U.S. Energy Information Administration (U.S. EIA), *Electricity Data Browser: Retail Sales of Electricity* (last visited Sept. 10, 2022), https://www.eia.gov/electricity/data/browser/#/topic/5.

15 Marcus Lu, *After China's Crypto Ban, Who Leads in Bitcoin Mining?*, Visual Capitalist (Dec. 7, 2021), https://www.visualcapitalist.com/sp/after-chinas-crypto-ban-who-leads-in-bitcoin-mining/.

16 Alex de Vries *et al., Revisiting Bitcoin's carbon footprint,* 6(3) Joule 498 (Feb. 25, 2022), https://www.cell.com/joule/fulltext/S2542-4351(22)00086-1; *see also* BBC, *Bitcoin less green since China ban, research suggests* (Feb. 25, 2022), https://www.bbc.com/news/technology-60521975; Molly Taft, *Bitcoin Is Dirtier Than Ever, Gizmodo* (Feb. 25, 2022), https://gizmodo.com/bitcoin-worse-for-climate-1848593882; David Yaffe-Bellany, *Bitcoin Miners Want to Recast Themselves as Eco-Friendly*, N.Y. Times (Mar. 22, 2022), https://www.nytimes.com/2022/03/22/technology/bitcoin-miners-environment-crypto.html; Jael Holzman, *Crypto carbon emissions are getting worse, study says*, E&E News (Feb. 25, 2022), https://subscriber.politicopro.com/article/eenews/2022/02/25/crypto-carbon-emissions-are-getting-worse-study-says-00011867.

17 Alex de Vries *et al., Revisiting Bitcoin's carbon footprint*, 6(3) Joule 498 (Feb. 25, 2022), https://www.cell.com/joule/fulltext/S2542-4351(22)00086-1.

18 White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States*, at 23 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

19 White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States*, at 10-12 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

20 In fact, due to the increasing efficiency of mining machines continuously entering the system, the average reward is earned about every 9.9 minutes. Estimated as the January 2020 to September 2022 average time between blocks based on difficulty adjustments every 2,016 blocks. BTC.com, *Difficulty* (last visited Sept. 10, 2022), https://btc.com/stats/diff.

21 As stated by the mining company Bit Digital: "When bitcoin was first launched in 2009, miners were awarded 50 bitcoin if they first solved a new block; this award was halved to 25 bitcoin per new block in 2012, and halved again in 2016 to 12.5 bitcoin per new block. Most recently, in May 2020, the then prevailing reward of 12.5 bitcoin per new block was halved to 6.25 bitcoin. This reward rate is expected to next halve during 2024 to 3.125 bitcoin per new block and will continue to halve at approximately four-year intervals until all potential 21 million bitcoin have been mined. Miners with a greater hash rate have a higher chance of solving a block and receiving a bitcoin award. After a third halving of bitcoins in May 2020, our mining strategy has been to mine bitcoins as fast and as many as possible given there are less bitcoins and a lower efficiency of mining." Bit Digital, *Form 424B3, Prospectus*, at 7 (May 5, 2022), https://www.sec.gov/Archives/edgar/data/1710350/000121390022024123/ea159396-424b3_bitdigital.htm.

22 As of this writing, Bitcoin miners were processing 222 exahashes per second, or 222 quintillion guesses at the puzzle solution every second (i.e., 222,000,000,000,000,000,000 hashes/second). *See* Blockchain.com, *Total Hash Rate* (TH/s) (last visited Sept. 10, 2022), https://www.blockchain.com/charts/hash-rate. Specialized machines, developed specifically for this purpose, can now process between 50 and 200 trillion guesses (terahashes) each second, implying that there are between 1 and 4 million processors continuously churning. Individual mining machines draw between 2.5 and 5 kW (faster machines draw more), or about double or triple a standard space heater.

23 *See, e.g.*, Jon Huang *et al.*, *Bitcoin Uses More Electricity Than Many Countries. How is That Possible?* N.Y. Times (Sept. 3, 2021), https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html; David Lavie, *Bitcoin halving is how the supply of the world's largest cryptocurrency is controlled*, Business Insider (Aug. 16, 2022), https://www.businessinsider.com/personal-finance/bitcoin-halving.

24 BitInfoCharts, *Bitcoin Hashrate Historical Chart* (last visited Sept. 1, 2022), https://bitinfocharts.com/comparison/bitcoin-hashrate.html#alltime.

25 If mining machines could process between 1.5 to 16 million hashes per second (*see* @hashrateindex, Twitter (Mar. 15, 2022, 7:00 PM), https://twitter.com/hashrateindex/status/1503883768582483969) then ~6,000 to 7,000 miners could have generated 10 Gh/s.

26 BitInfoCharts, *Bitcoin Price in USD Historical Chart*, https://bitinfocharts.com/comparison/bitcoin-price.html#alltime.

27 For example, the Public Utility District No. 1 of Pend Oreille County typically averages 35 MW per month, whereas Allrise Capital and Blockchain LLC's cryptocurrency mining operation requested 220 MW per month, representing 6 times the amount of electricity the small utility typically covers. *See* Thomas Clouse, *Massive cryptocurrency mining operation planned at former Ponderay Newsprint mill*, Spokesman-Review (Mar. 11, 2022), https://www.spokesman.com/stories/2021/sep/16/massive-cryptocurrency-mining-operation-planned-at/. The cryptocurrency mining facility received a conditional use permit that allows for 100 MW to run 30,000 servers. Thomas Clouse, *Crypto mine in Usk gets conditional use permit from Pend Oreille County; opponents appeal*, Spokesman-Review (June 1, 2022), https://www.spokesman.com/stories/2022/jun/01/crypto-mine-in-usk-gets-conditional-use-permit-fro/.

28 NPR, *Cryptocurrency tech is vulnerable to tampering, a DARPA analysis finds* (June 21, 2022), https://www.npr.org/2022/06/21/1105815143/cryptocurrency-bitcoin-blockchain-security-tampering-darpa; Evan Sultanik et al., *Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers*, Trail of Bits, 8 (June 2022), https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf.

29 Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index; Historical Bitcoin Network Power Demand* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/index.

30 Includes Argo's Helios facility (200 MW), BitDeer Rockdale (170 MW), Riot Blockchain Rockdale (400 MW), Compute North Granbury (300 MW), Compute North McCamey (280 MW), Core Scientific Denton (300 MW), Genesis Digital Pyote (300 MW), and Lancium Abilene (200 MW).

31 Based on estimate from Riot Blockchain that a single 100 MW facility might host 28,000 Bitcoin mining machines. Riot Blockchain, Inc., *Forward Looking Statements*, 28 (June 16, 2022), https://d1io3yog0oux5.cloudfront.net/_3e5c4be455cdeba10dde03ac9c750ba5/riotblockchain/db/447/4204/pdf/Riot+Corp+Deck+-+June+22+-+vF.pdf.

32 U.S. EIA, *How much electricity does an American home use?* (Oct. 7, 2021), https://www.eia.gov/tools/faqs/faq.php?id=97&t=3.

33 Josh Zerlan, *Bitcoin as the Ultimate Democratic Tool*, Wired Magazine (2014), https://www.wired.com/insights/2014/04/bitcoin-ultimate-democratic-tool/.

34 Paul Kim, *ASIC mining: Computers built specifically for mining cryptocurrency*, Business Insider (Mar. 16, 2022), https://www.businessinsider.com/personal-finance/asic-mining; Lucas Wyland, *The 10 Best Bitcoin Mining Hardware Machines 2022*, Coin Ledger (Aug. 25, 2022), https://coinledger.io/tools/best-bitcoin-mining-hardware.

35 Jon Huang *et al., Bitcoin Uses More Electricity Than Many Countries. How is That Possible?* N.Y. Times (Sept. 3, 2021), https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html. In July 2021, just five mining pools controlled more than 80% of the hash power in Bitcoin. Jacob Wolinsky, *If You Think The Decentralized Blockchain Platforms Of Today Are Truly Decentralized, Think Again*, Yahoo! Finance (July 26, 2021) https://finance.yahoo.com/news/think-decentralized-blockchain-platforms-today-142927523.html.

36 Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market*, Nat'l Bureau of Econ. Rsch., Working Paper 29396, 22–23, Nat'l Bureau of Econ. Rsch., Working Paper 29396 (Oct. 2021) https://www.nber.org/papers/w29396 (note: this analysis was for the time period before China banned mining).

37 Riot Blockchain, *Form 10 Q, Quarterly Report*, at 13 (for period ending June 30, 2022). https://www.sec.gov/ix?doc=/Archives/edgar/data/1167419/000155335022000687/riot-20220630.htm. Today, the average lifespan of a well-kept, maintained machine is projected to be around 3 to 5 years. In harsh or poor conditions, they can deteriorate in as little as a few months. *Lumerin Blog: How to prolong your ASIC miner's lifespan*, Medium (Nov. 23, 2021), https://medium.com/lumerin-blog/how-to-prolong-your-asic-miners-lifespan-360b68140a04; Minery, *How Long Do ASICS Last?* (May 16, 2022), https://minery.io/blog/how-long-do-asics-last/.

38 *See, e.g.*, White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States,* at 10-12 & n.30 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf; David Lavie, *Bitcoin halving is how the supply of the world's largest cryptocurrency is controlled*, Business Insider (Aug. 16, 2022), https://www.businessinsider.com/personal-finance/bitcoin-halving.

39 *See, e.g.*, EZ blockchain, *EZ Smartbox Mobile Mining Container* (last visited Sept. 10, 2022). https://ezblockchain.net/smartbox/.

40 Marathon Digital Holdings. *Marathon Digital Holdings Announces Intent to Transition Hardin, Montana Bitcoin Mining Operations to More Sustainable Power Sources*. (Apr. 5, 2022) https://ir.marathondh.com/news-events/press-releases/detail/1282/marathon-digital-holdings-announces-intent-to-transition.

41 Eliza Gkritsi, *Bitcoin Mining Middleman Compass' Georgia Facilities to Close as Energy Prices Soar* (Sept. 1, 2022) https://www.coindesk.com/business/2022/09/01/bitcoin-mining-middleman-compass-georgia-facilities-to-close-as-energy-prices-soar/.

42 For example, Riot Blockchain disclosed the total number of cryptocurrency mining machines expected to be in use by the company by the end of 2022 (120,146 miners, utilizing approximately 370 MW of capacity in New York and Texas, but did not detail the fuel sources associated with that energy consumption. Riot Blockchain, Inc., *Form 10-K, Annual Report*, at 34 (for year ending Dec. 31, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001167419/000107997322000280/riot10k1221.htm.
Iris Energy claims to have 530 MW of capacity, split across three different facilities, but only discloses the capacity of one of those facilities, and it is only 30 MW. Iris Energy Ltd., *2021 Form F-1*, at 3, 7 (Nov. 10, 2021), https://www.sec.gov/Archives/edgar/data/0001878848/000114036121037466/ny20000275x9_f1a.htm.
See also Argo Blockchain plc., *2021 Form F-1*, at 3 (Nov. 10, 2021), https://www.sec.gov/Archives/edgar/data/0001841675/000110465921136647/tm2130707-7_f1a.htm;
Core Scientific, Inc., *Form 10-K, Annual Report*, at 148 (for year ending Dec. 31, 2021), https://www.sec.gov/Archives/edgar/data/1839341/000119312522088850/d268076d10k.htm.

43 Where the PPA is with an electric cooperative or municipal utility in states where cooperatives or municipal utilities are not required to file such plans (*e.g.*, Illinois), this information may be available only piecemeal or after-the-fact.

44 *See, e.g.*, Ind. Dep't Envt'l Mgmt, *Letter from Chief - Permits Branch to Plant Manager, Hoosier Energy* (Jan. 28, 2021), Doc. No. 83119775, https://ecm.idem.in.gov/cs/idcplg?IdcService=GET_FILE&dID=83119370&dDocName=83119775&Rendi%20tion=web&allowInterrupt=1&noSaveAs=1; N.Y. State Dep't Envt'l Conserv., *Permit Documentation for Notable Projects, Greenidge Station* (last visited Aug. 25, 2022), https://www.dec.ny.gov/permits/123728.html.

45 Fed. Energy Regulatory Comm'n (FERC), *Mergers and Sections 201 and 203 Transactions* (last updated Apr. 12, 2021), https://www.ferc.gov/electric/general-information/mergers-and-sections-201-and-203-transactions; FERC, *Forms 65 and 65A and Triennial Market Power Analysis Letters* (last updated Feb. 17, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001167419/000107997322000280/riot10k1221.htm; https://www.reginfo.gov/public/do/DownloadDocument?objectID=10176501.

46 FracTracker Alliance, *Status of known proof-of-work cryptocurrency mining operations in the U.S.* (Sept. 2022).

47 When an electrical load is placed "behind-the-meter," it is powered directly by a particular power plant, rather than from the grid, where electricity is generated by a suite of different power plants across a broader system. Because the plant's power (or a portion of it) flows directly to the mining operation without going onto the grid, the plant may be exempt from or subject to different monitoring and reporting requirements in a variety of respects than power plants "on the grid."

48 The White House's OSTP recently stated that "The 2020s are a decisive decade for climate action in the United States, and up to 100 GW of clean electricity capacity needs to be added to the grid every year to meet the demand of these newly electrified end uses." White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States*, at 17 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

49 Stronghold Digital Mining, Inc., *Form S-1, Registration Statement*, at 4, 7 (July 27, 2021), https://www.sec.gov/Archives/edgar/data/0001856028/000156459021038087/sdmi-s1.htm

50 Stronghold Digital Mining, Inc., *Form 10-K, Annual Report*, at 7 (for year ending Dec. 31, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001856028/000162828022007706/sdig-20211231.htm; Stronghold Digital Mining, Inc., *Form S-1, Registration Statement*, at 4, 7 (July 27, 2021), https://www.sec.gov/Archives/edgar/data/0001856028/000156459021038087/sdmi-s1.htm.

51 Waste coal is a low-energy-value product that, before environmental restrictions were passed, was often dumped in piles near mining sites. Pennsylvania has approximately 840 such sites and operators such as Stronghold claim that burning it for energy is "environmentally beneficial" because it encourages the removal of these piles, and the waste ash can be used for fill and reclamation projects. Pennsylvania has nine other coal waste plants where mining could increase their operations or extend their useful lives. *See, e.g.*, Evan D. Endres, *Waste Coal: Time to finish what we started*, PennFuture (Nov. 18, 2015), https://www.pennfuture.org/Blog-Item-Waste-Coal-Time-to-finish-what-we-started.

52 U.S. EIA, *Emissions by Plant and Region*, 2020 (Apr. 12, 2022), https://www.eia.gov/electricity/data/emissions/.

53 *See, e.g.*, U.S. EPA, *Clean Air Markets Program Data*, https://campd.epa.gov/; ABC News, *Bitcoin operation ignites debate around the waste from coal mining in Pennsylvania* (Jan. 25, 2022); https://abcnews.go.com/US/bitcoin-operation-ignites-debate-waste-coal-mining-pennsylvania/story?id=82246178.

54 *See, e.g.*, Penn. Dep't of Comm'y and Econ. Dev., *Coal Refuse Energy and Reclamation Tax Credit* (last visited Aug. 25, 2022), https://dced.pa.gov/programs/coal-refuse-energy-reclamation-tax-credit/; Penn. Pub. Util. Comm'n, *Alt. Energy and Economic Dev. in Pennsylvania AEPS Fact Sheet* (last visited Aug. 25, 2022), https://www.puc.pa.gov/general/consumer_ed/pdf/AEPS_Fact_Sheet.pdf

55 Stronghold Digital Mining, Inc., *Form S-1, Registration Statement*, at 100 (Jul. 27, 2021) https://www.sec.gov/Archives/edgar/data/0001856028/000156459021038087/sdmi-s1.htm (Net Cost of Power w/incentives as $17 versus $37 without).

56 U.S. Envt'l Prot. Agency (U.S. EPA), *Power Sector Emissions Data*, https://www.epa.gov/airmarkets/power-sector-emissions-data; U.S. EPA, *Clean Air Markets Program Data*, https://campd.epa.gov/ (filtering for Fortistar North Tonawanda Inc.).

57 *Id.*; Digihost Tech., Inc., *Title V and Title IV Permits Renewal Application, Fortistar North Tonawanda Cogeneration Facility*, at 5–6, 30 (Apr. 21, 2021); N.Y. State Dep't of Envt'l Conserv., *Fortistar North Tonawanda current Title V and Title IV Permits* (2016), https://www.dec.ny.gov/dardata/boss/afs/permits/929120005900013_r2.pdf. The local water consumption and thermal pollution from the plant is discussed further below.

58 N.Y. State Dep't of Envt'l Conserv., *Potential Envt'l Justice Area (PEJA) Communities*, https://www.arcgis.com/home/webmap/viewer.html?url=https://services6.arcgis.com/DZHaqZm9cxOD4CWM/ArcGIS/rest/services/PotentialEnvironmentalJusticeAreaPEJACommunities/FeatureServer&source=sd; U.S. EPA, *Envt'l Justice Screening and Mapping Tool*, https://ejscreen.epa.gov/mapper/.

59 U.S. EPA, *Power Sector Emissions Data*, https://www.epa.gov/airmarkets/power-sector-emissions-data; US EPA, *Clean Air Markets Program Data*, https://campd.epa.gov/ (filtering for Greenidge Generation LLC). These numbers do not include upstream emissions.

60 *Id.*

61 N.Y. State Dep't Envt'l Conserv., *Notice of Denial of Title V Air Permit, DEC ID: 8-5736-00004/00017, Greenidge Generation LLC—Greenidge Generating Station, Title V Air Permit Application*, at 15 (June 30, 2022), https://www.dec.ny.gov/docs/administration_pdf/greenidgefinal630.pdf; Earthjustice, *Press Release: New York State Denies Air Pollution Permit for Fossil Fuel-burning Crypto mining operation, Citing Energy-Intensity and Envt'l Concerns* (June 30, 2022), https://earthjustice.org/news/press/2022/new-york-state-denies-air-pollution-permit-for-fossil-fuel-burning-crypto-mining-operation-citing-energy.

62 *See, e.g.*, U.S. EPA, *Proposed Date to Cease Receipt of Waste for Greenidge Generation LLC Based on Interim Ineligibility Determination*, Docket ID No. EPA-HQ-OLEM-2021-0591 (Jan. 24, 2022), https://www.regulations.gov/document/EPA-HQ-OLEM-2021-0591-0002; Sruthi Gopalakrishnan, *In the Finger Lakes, a cryptocurrency mining plant billed as 'green' has a dirty coal ash problem*, Energy News Network (Aug. 25, 2022), https://energynews.us/2022/08/25/in-the-finger-lakes-a-bitcoin-mining-plant-billed-as-green-has-a-dirty-coal-ash-problem/; WXXI News, *Envt'l groups turn focus to Greenidge's water permits* (Sept. 2, 2022), https://www.wxxinews.org/local-news/2022-09-02/environmental-groups-turn-focus-to-greenidges-water-permits.

63 GlobeNews Wire, *Cipher Mining Provides Second Quarter 2022 Business Update* (Aug. 9, 2022) https://www.globenewswire.com/news-release/2022/08/09/2494732/0/en/Cipher-Mining-Provides-Second-Quarter-2022-Business-Update.html.

64 Alex Alley, *Bitcoin miner Marathon signs for coal-fired electricity in Montana*, Data Center Dynamics (Oct. 16, 2020), https://www.datacenterdynamics.com/en/news/bitcoin-miner-marathon-signs-coal-fired-electricity-montana/.

65 Data compiled from quarterly air monitoring reports filed with the Montana Dep't of Envt'l Quality.

66 Marathon Digital Holdings, *Press Release: Marathon Digital Holdings Announces Bitcoin Production and Mining Operation Updates for November 2021* (Dec. 3, 2021), https://ir.marathondh.com/news-events/press-releases/detail/1269/marathon-digital-holdings-announces-bitcoin-production-and.

67 Yahoo Finance, *Bitcoin USD (BTC-USD) Historical Prices* (as of Dec. 31, 2021), https://finance.yahoo.com/quote/BTC-USD/history/.

68 U.S. EPA, *Clean Air Markets Program Data*, https://campd.epa.gov/; *see also* Montana Envt'l Info. Center, et al., *Comments on Montana's Proposed Regional Haze State Implementation Plan for the 2nd Implementation Period* (Mar. 21, 2022), https://protectnps.org/wp-content/uploads/2022/03/Combined-MT-Regional-Haze-R2-Comment-Letter-Exhibits-2022-3-21_reduced-file-size.pdf.

69 Today, coal-fired power plants in the U.S. generate roughly 100 million tons of CCR every year. Recent industry data demonstrate that 92% of CCR ponds are polluting the underlying groundwater to levels that exceed federal drinking water standards. CCR contaminates groundwater with carcinogens, neurotoxins, developmental toxins and other dangerous chemicals including arsenic, boron, lithium, chromium, cobalt, lead, lithium, manganese, molybdenum, radium, mercury, and cadmium. This groundwater can flow to drinking water wells or pollute nearby surface water. *See, e.g.*, U.S. EPA, *Coal Ash*, https://www.epa.gov/coalash; *see also* U.S. News, *EPA Moves to Crack Down on Dangerous Coal Ash Storage Ponds* (Jan. 11, 2022), https://www.usnews.com/news/business/articles/2022-01-11/epa-moves-to-crack-down-on-dangerous-coal-ash-storage-ponds; Envt'l Integrity Project & Earthjustice, *Coal's Poisonous Legacy: Groundwater Contaminated by Coal Ash Across the U.S.* (Mar. 2, 2019, rev. July 11, 2019), https://environmentalintegrity.org/reports/coals-poisonous-legacy/; Kari Lydersen et al., *Cracking down on coal ash: Tough talk and tough choices*, E&E News (Aug. 24, 2022), https://energynews.us/2022/08/24/cracking-down-on-coal-ash-tough-talk-and-tough-choices/.

70 Tom Lutey, *Crypto miner plans to exit Hardin coal-fired power plant*, Billings Gazette (Apr. 6, 2022), https://billingsgazette.com/news/crypto-miner-plans-to-exit-hardin-coal-fired-power-plant/article_cd2ca444-929a-511d-913d-903fbc570498.html; Catarina Moura, *Marathon to move its Bitcoin miners from Montana to new locations with 'more sustainable' power sources*, The Block (Apr. 5, 2022), https://www.theblock.co/linked/140753/marathon-to-move-its-bitcoin-miners-from-montana-to-new-locations-with-more-sustainable-power-sources.

71 In April 2022, Compute North announced a new 300 MW cryptocurrency mining facility that would operate "behind-the-meter" at the Wolf Hollow gas-fired power plant in Granbury, TX. *See* Compute North, *Compute North Launches New 300MW Data Center In Granbury, Texas* (Apr. 8, 2022), https://www.computenorth.com/news_release/compute-north-launches-new-300mw-data-center-in-granbury-texas/; Dan Swinhoe, *Compute North breaks ground on 300MW data center in Granbury, Texas*, Data Center Dynamics (Apr. 12, 2022), https://www.datacenterdynamics.com/en/news/compute-north-breaks-ground-on-300mw-data-center-in-granbury-texas. With the need for Marathon to move its miners at the Hardin coal plant to meet its deadline of "redeploy[ing] Hardin-installed miners to renewable power facilities on or before September 30, 2022," it became suspiciously clear that Marathon was actually deploying miners to Compute North's Wolf Hollow operation. Marathon Digital Holdings, Inc., *Form 10-Q, Quarterly Report*, at 15 (for the period ended March 31, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001507605/000149315222012398/form10-q.htm; "On July 5, Marathon also expanded its hosting arrangements with Compute North to include an additional 42 megawatts of hosting capacity at Compute North's facility near Granbury, Texas." Marathon Digital Holdings, Inc., *Marathon Digital Holdings Secures Hosting Capacity to Support All 23.3 EH/s of Bitcoin Mining* (July 18, 2022), https://ir.marathondh.com/news-events/press-releases/detail/1289/marathon-digital-holdings-secures-hosting-capacit y-to.

72 Kayla Desroches, *As crypto company departs Hardin, what's next for the communities it leaves behind?* Yellowstone Public Radio (Apr. 28. 2022), https://www.ypradio.org/energy/2022-04-28/as-crypto-company-departs-hardin-whats-next-for-the-communities-it-leaves-behind.

73 *Id.*

74 Hoosier is a generation and transmission cooperative providing electric power to a 17-member electric distribution cooperative in central and southern Indiana, and one member cooperative in Illinois. *See* U.S. EPA, *Letter from Robert Hochstetler, V.P., Hoosier Energy, to Richard Kinch, US EPA* (Mar. 28, 2009), https://archive.epa.gov/epawaste/nonhaz/industrial/special/fossil/web/pdf/hoosier-merom.pdf.

75 Hoosier Energy, *2020 Integrated Resource Plan — Public Version Vol. I: Main Report*, at 89, 98 (Nov.2, 2020), https://www.in.gov/iurc/files/HoosierEnergy_IntegratedResourcePlan_Volume1_110220.pdf (Hoosier Energy's most recent Integrated Resource Plan stated: "Early retirement of Merom in 2023 provides substantial savings versus retaining the current portfolio through the study period" and "[b]y retiring Merom and replacing it with a number of smaller geographically diverse resources, all replacement portfolios improve Hoosier's single unit exposure relative to the current portfolio.").

76 *See* Hallador Energy Co., *Form 8-K/A, Current Report Amendment No. 1* (Feb. 18, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0000788965/000143774922006045/hnrg20220309_8ka.htm.

77 *See* Gerry Dick, *Startup to Establish Crypto Mining Facility in Sullivan County*, Inside IN Bus. (May 12, 2022), https://www.insideindianabusiness.com/articles/startup-to-establish-crypto-mining-facility-in-sullivan-county; *see also* Haley Cawthon, *AboutBit to Open New Crypto Mining Facility in Southern Indiana*, KYINNO (May 11, 2022), https://www.bizjournals.com/louisville/inno/stories/news/2022/05/11/aboutbit-merom-mining.html.

78 *See* Hallador Power Co. LLC, *Petition* Ex. A, at 4 (Test. of M. Elliott Batson), Ind. Util. Reg. Comm'n, Cause No. 45691 (Mar. 8, 2022), https://iurc.portal.in.gov/_entity/sharepointdocumentlocation/746eff84-fd9e-ec11-b3fe-001dd8017dcd/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=Verified%20Petition%20to%20Indiana%20Commission%20with%20Exhibit%20A.pdf; *see also* Hallador Power Co., LLC, *Application* (Apr. 11, 2022), FERC Docket No. ER22-1608, Accession No 2022-0411, https://elibrary.ferc.gov/eLibrary/filelist?accession_Number=20220411-5116&optimized=false; Hallador Energy Co., *Hoosier Energy announce agreement to transfer ownership of Merom Generating Station, multiyear PPA*, https://www.sec.gov/Archives/edgar/data/0000788965/000143774922006045/ex_345554.htm (Feb. 15, 2022); Benjamin Storrow & Jael Holzman, *Cryptocurrency's Climate Conundrum*, E&E News (May 18, 2022), https://www.eenews.net/articles/cryptocurrencys-climate-conundrum ("Some crypto miners, meanwhile, are unconcerned about criticism of their industry's environmental impact. Last week, a Kentucky-based crypto miner announced it had signed a deal to build a 115-MW facility outside an Indiana coal plant that had been slated to retire next year. Now, the plant will provide electricity to AboutBit's data mining operation as part of a five-year power contract, said Jay Chiang, the company's co-founder. Asked about critics' assertions that the deal could keep a polluting coal plant open, Chiang replied, 'It's 100 percent correct.' 'For anyone to say their crypto operation is green, unless they are 100 percent hydro, they can't make that claim,' he said. 'As an operation, it's not humanly possible.'. . . 'Is coal 100 percent bad? The answer is no. Does it cause environmental issues? Yes,' he said. . . .").

79 Benjamin Storrow & Jael Holzman, Cryptocurrency's Climate Conundrum, E&E News (May 18, 2022), https://www.eenews.net/articles/cryptocurrencys-climate-conundrum

80 *See* Gerry Dick, *Hallador Energy Co. reopens Knox County coal mine*, Inside Ind. Business (July 14, 2022), https://www.insideindianabusiness.com/articles/hallador-energy-co-reopens-knox-county-coal-mine; *see also* Hallador Power Co., *Response to FERC's Deficiency Letter of July 7th* (July 15, 2022), FERC Docket No. EC22-52, Accession No. 20220715-5204, https://elibrary.ferc.gov/eLibrary/filelist?accession_Number=20220715-5204&optimized=false (Hallador provided data on the concentration of coal mining ownership within the MISO region, purportedly in response to competitiveness concerns raised by FERC).

81 Judith Lewis Mernit, *Bitcoin's Intensive Energy Demands are Sparking a Crypto Backlash*, Yale Env't 360 (June 21, 2022), https://e360.yale.edu/features/bitcoins-intensive-energy-demands-spark-a-crypto-backlash.

82 Naureen S. Malik, *Texas crypto miners could require as much power as all of New York state*, Bloomberg (Aug. 26, 2022), https://www.bloomberg.com/news/articles/2022-08-26/texas-crypto-rush-may-need-as-much-power-as-entire-state-of-n-y ("Texas has some of the cheapest electricity rates for big consumers, averaging about 7.57 cents per kilowatt-hour in June, a third lower than the national average, according to the U.S. Energy Info. Administration.")

83 *Id.*

84 Seth Tupper, *Orphaned South Dakota gas wells could soon power bitcoin mining*, S.D. Public Broadcasting (Feb. 24, 2021), https://www.sdpb.org/blogs/politics-public-policy/orphaned-south-dakota-gas-wells-could-soon-power-bitcoin-mining/; Anne Danahy, *EPA Asks A Bitcoin 'Mining' Operation In Clearfield County For Info.*, Allegheny Front (July 22, 2022), https://www.alleghenyfront.org/epa-pennsylvania-bitcoin-mining-big-dog-energy-cryptocurrency/; *see* Midstream, Post, Linkedin (last visited Aug 26, 2022), https://www.linkedin.com/posts/midstream-enterprises-inc%2E_midstream-bitcoin-miningbitcoin-activity-6845779138238930944-NmBd?utm_source=linkedin_share&utm_medium=member_desktop_web.

85 Avi Asher-Schapiro, *Coal to Crypto: The Gold Rush Bringing Bitcoin Miners to Kentucky*, Thomson Reuters Found. (Mar. 14, 2022), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate.

86 Andrew R. Chow, *Fact-Checking 8 Claims About Crypto's Climate Impact*, Time Magazine (July 1, 2022), https://time.com/6193004/crypto-climate-impact-facts/.

87 *See, e.g.*, Sergio Chapa, *Cryptocurrency mining company eyes flared gas in Permian Basin*, Houston Chronicle (June 23, 2020), https://www.houstonchronicle.com/business/energy/article/Cryptocurrency-mining-company-eyes-flared-gas-in-15359750.php; Crusoe Energy, *Understanding the Problem Crusoe Solves* (Sept. 23, 2021), https://www.crusoeenergy.com/blog/3MyNTKiT6wqsEWKhP0BeY/understanding-the-problem-crusoe-solves.

88 Justine Calma, *Why fossil fuel companies see green in Bitcoin mining projects*, The Verge (May 4, 2022). https://theverge.com/2022/5/4/23055761/exxonmobil-cryptocurrency mining-bitcoin-methane-gas; Andrew R. Chow, *Fact-Checking 8 Claims About Crypto's Climate Impact*, Time Magazine (July 1, 2022), https://time.com/6193004/crypto-climate-impact-facts/.

89 Businesswire, *Crusoe Energy Systems Closes $505 Million in New Capital Led by Climate Technology Investors G2 Venture Partners, Prepares Launch of CrusoeCloud* (Apr. 21, 2022), https://www.businesswire.com/news/home/20220420005676/en/Crusoe-Energy-Systems-Closes-505-Million-in-New-Capital-Led-by-Climate-Technology-Investors-G2-Venture-Partners-Prepares-Launch-of-CrusoeCloud%E2%84%A2; Stephen Cunningham, *Bitcoin miners help US oil producers cut flaring*, Argus Media (Oct. 8, 2021), https://www.argusmedia.com/en/news/2261931-bitcoin-miners-help-us-oil-producers-cut-flaring.

90 Laila Kearney, *Oil drillers and Bitcoin miners bond over natural gas*, Reuters (May 21, 2021), https://www.reuters.com/business/sustainable-business/oil-drillers-bitcoin-miners-bond-over-natural-gas-2021-05-21/.

91 E&E News, *Exxon weighs taking gas-to-bitcoin pilot to 4 countries* (Mar. 25, 2022), https://subscriber.politicopro.com/article/eenews/2022/03/25/exxon-weighs-taking-gas-to-bitcoin-pilot-to-four-countries-00020188; Audrey Carleton, *Exxon Considering Expanding Bitcoin Mining Pilot to 4 Countries: Report*, Vice (Mar. 25, 2022), https://www.vice.com/en/article/xgdpwa/exxon-considering-expanding-bitcoin-mining-pilot-to-4-countries-report.

92 Penn. Dep't of Envt'l Prot., *Notice of Violation to Big Dog Energy*, LLC (Jan. 7, 2022); *see also* Bill Shannon & Yanni Tragellis, *Crypto mining raises concerns in Clearfield County*, WTAJ (Feb. 10, 2022), https://www.wearecentralpa.com/news/local-news/crypto-mining-raises-concerns-in-clearfield-county/.

93 John Aguilar, *The crude marriage of oil drilling and bitcoin mining gets a wary eye from Adams County*, Denver Post (July 18, 2022), https://www.denverpost.com/2022/07/18/cryptocurrency-mining-adams-county-oil-gas/.

94 Adams County, Oil & Gas Info., https://www.adcogov.org/oil-and-gas-information; Memo from Jenni Hall, Director of Community & Economic Development to CED Staff, Re: *Interpretation of Use — Oil and Gas Cryptocurrency / Digital Currency / Electronic Currency Mining, Adams County* (May 25, 2022), https://www.adcogov.org/sites/default/files/2022.05.25%20Cryptocurrency%20Mining%20Interpretation_Signed.pdf. Out of the 14 local governments that responded to the Colorado Oil and Gas Conservation Commission's survey about cryptocurrency mining, five counties — Adams, Boulder, Larimer, Thorton, and Arapahoe — all offered that "gas to crypto" operations would not be permitted in their jurisdictions. Mark Jaffe, *Oil and gas and cryptocurrency miners are Colorado's new odd couple. And they're making quite a bit of coin.*, Colorado Sun (Aug. 29, 2022), https://coloradosun.com/2022/08/29/oil-gas-cryptocurrency-bitcoin-mining/.

95 Electric Reliability Council of Texas, Inc. (ERCOT), *Large Flexible Load Task Force. Overview of Large Load Interconnection Requests (Interim Process)*, at 2 (Apr. 26, 2022), https://www.ercot.com/files/docs/2022/04/25/InterimLargeLoadInterconnectionProcess_AggregateData_04262022.pptx; Naureen S. Malik, *Crypto Miners' Electricity Use in Texas Would Equal Another Houston*, Bloomberg (Apr. 27, 2022), https://www.bloomberg.com/news/articles/2022-04-27/crypto-miners-in-texas-will-need-more-power-than-houston.

96 Naureen S. Malik, *Crypto Miners' Electricity Use in Texas Would Equal Another Houston*, Bloomberg (Apr. 27, 2022), https://www.bloomberg.com/news/articles/2022-04-27/crypto-miners-in-texas-will-need-more-power-than-houston; Jeremy Blackman, *Investors are swarming to crypto in Texas. Can the state's fragile grid deliver?* Houston Chronicle (May 16, 2022), https://www.houstonchronicle.com/politics/texas/article/Investors-are-swarming-to-crypto-in-Texas-Can-17176539.php.

97 Justine Calma, *Texas' Fragile Grid Isn't Ready for Crypto Mining's Explosive Growth*, The Verge (July 14, 2022), https://www.theverge.com/2022/7/14/23206795/bitcoin-crypto-mining-electricity-texas-grid-energy-bills-emissions.

98 Naureen S. Malik, *Texas crypto miners could require as much power as all of New York state*, Bloomberg (Aug. 26, 2022), https://www.bloomberg.com/news/articles/2022-08-26/texas-crypto-rush-may-need-as-much-power-as-entire-state-of-n-y.

99 Aggregate Bitcoin energy use data, from August 1, 2021 through July 31, 2022, is sourced from the Cambridge Bitcoin Electricity Consumption Index, with a daily estimated power consumption at an estimated 85% load factor and assuming ~38% of Bitcoin mining occurred in the United States in 2022. Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index: Bitcoin network power demand* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/index; Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index: Bitcoin Mining Map* (last visited Aug. 25, 2022), https://ccaf.io/cbeci/mining_map (CBECI fraction of consumption by region). National marginal emissions rate from is from EPA's Avoided Emissions and Generation Tool (AVERT). U.S. EPA, *Emission Rates from AVERT* (Mar. 2022), https://www.epa.gov/system/files/documents/2022-03/avert_emission_rates_03-29-22.xlsx. *See also* White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States*, at 21 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf (estimating 25-50 million tons in the United States).

100 CO_2 emissions from Scherer coal plant (3,564 MW) in 2021, derived from U.S. EPA's Clean Air Markets Program Data (last visited Sept. 10, 2022), https://campd.epa.gov/data/custom-data-download.

101 White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States*, at 21 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf. OSTP relies on EPA's eGRID "non-baseload GHG emissions" rate, a 2007 methodology of assessing marginal emissions rates. Today, EPA recommends using AVERT, a more sophisticated approaches for marginal emissions rates. *See* U.S. EPA, *Greenhouse Gases Equivalencies Calculator - Calculations and References* (last visited Sept. 10, 2022), https://www.epa.gov/energy/greenhouse-gases-equivalencies-calculator-calculations-and-references). eGRID's national "non-baseload" emissions rate for 2020 is 1,400 $lbsCO_2$/MWh, while AVERT's national marginal emissions rate is 1,534 lbs/MWh, or nearly 10% higher. Current values at U.S. EPA, *Avoided Emission Rates Generated from AVERT* (last visited Sept. 10, 2022), https://www.epa.gov/avert/avoided-emission-rates-generated-avert.

102 U.S. House of Rep. Committee on Energy & Commerce Staff, *Memorandum re: Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchain*, at 5 (Jan. 17, 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Briefing%20Memo_OI%20Hearing_2022.01.20.pdf (citing Forex Suggest, *Global Impact of Crypto Trading*, https://forexsuggest.com/global-impact-of-crypto-trading/ (Jan. 10, 2022); U.S. EPA, *Greenhouse Gas Emissions from a Typical Passenger Vehicle* (Mar. 2018), https://www.epa.gov/greenvehicles/greenhouse-gas-emissions-typical-passenger-vehicle).

103 Elesia Fasching & Suparna Ray, *Coal will account for 85% of U.S. electric generating capacity retirements in 2022*, US EIA (Jan. 11 2022), https://www.eia.gov/todayinenergy/detail.php?id=50838.

104 As Steve Wright noted in his response to congressional representatives, "With cryptocurrency mining the utility is financially exposed to providing transmission and distribution which generally requires a capital investment spread over a long-life asset. The utility is also financially exposed if it is either building generation that could go unutilized or underutilized or by committing generation to serve cryptocurrency load that would otherwise be sold for a higher long-term value. This is particularly a problem for a consumer owned utility where the infrastructure investments are being made in effect by the people who live in the service territory." See Stephen Wright, Additional Questions for the Record re: Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains, at 1, https://docs.house.gov/meetings/IF/IF02/20220120/114332/HHRG-117-IF02-Wstate-WrightS-20220120-SD001.pdf.

105 Mining operations at existing hydroelectric facilities are more complicated to parse. To the extent that the facility would have otherwise marketed its energy to the broader grid and remained viable, the cryptomining operation might be utilizing a low emissions resource that would have otherwise displaced fossil consumption. However, if the hydroelectric facility would have otherwise been abandoned but for the favorable pricing offered by the cryptocurrency mine, it may have little emissions impact.

106 The PJM Regional Transmission Organization, which tracks marginal resources, states that "in 2021, coal units were 14.1 percent and natural gas units were 71.7 percent of marginal resources. In 2020, coal units were 17.5 percent and natural gas units were 72.6 percent of marginal resources." Monitoring Analytics, LLC, *State of the Market Report for PJM, Vol. 1*, at 22 (Mar. 10, 2022), https://www.monitoringanalytics.com/reports/PJM_State_of_the_Market/2021/2021-som-pjm-vol1.pdf.

107 U.S. EPA, *Avoided Emission Rates Generated from AVERT*, https://www.epa.gov/avert/avoided-emission-rates-generated-avert (AVERT-based marginal emissions rates for 2021 from "uniform energy efficiency" profile).

108 Daniel Swinhoe, *Aspen Creek Digital Corporation launches 6MW cryptomine in Colorado Data Center Dynamics* (June 28, 2022), https://www.datacenterdynamics.com/en/news/aspen-creek-digital-corporation-launches-6mw-cryptomine-in-colorado/.

109 Even in this case, because the biggest current barrier to renewable development in the U.S. are supply chain constraints, even this solar development likely displaces building facilities that would otherwise serve the grid. *See* Nichola Groom, *U.S. solar industry warns of slowdown due to supply chain disruptions, tariff uncertainty*, Reuters (Apr. 28, 2022), https://www.reuters.com/world/us/us-solar-industry-warns-slowdown-due-supply-chain-disruptions-tariff-uncertainty-2022-04-28/#:~:text=April%2028%20(Reuters)%20%2D%20The,from%20Southeast%20Asia%20hit%20home.

110 Aspen Creek Digital Corp., *Homepage* (last visited Aug. 26, 2022), https://acdigitalcorp.com/.

111 As further explained by Steve Wright in response to congressional representatives, cryptomining companies are pushed toward fossil-fired resources because (1) "fossil fuel plants are finding it more difficult to operate and have been increasingly curtailed or shut down prior to end of life," thus creating opportunities to "restart or increase fossil fuel plants when they can get revenues greater than variable and fixed operations and maintenance costs;" (2) "fossil fuel resources are dispatchable translating to a high probability of being available around the clock;" and (3) electricity prices. *See* Stephen Wright, *Additional Questions for the Record re: Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains*, at 2, https://docs.house.gov/meetings/IF/IF02/20220120/114332/HHRG-117-IF02-Wstate-WrightS-20220120-SD001.pdf.

112 World Health Organization, *New WHO Global Air Quality Guidelines aim to save millions of lives from air pollution* (Sept. 22, 2021), https://www.who.int/news/item/22-09-2021-new-who-global-air-quality-guidelines-aim-to-save-millions-of-lives-from-air-pollution; *see also* U.S. EPA, *Research on Health Effects from Air Pollution* (last updated Feb. 16, 2022), https://www.epa.gov/air-research/research-health-effects-air-pollution

113 Many facilities also consume additional electricity to cool their operations. The White House OSTP estimated recently that "[e]lectricity for cooling can add anywhere from a low percentage (for cool climates) to over 100% of the electricity consumed by the computing equipment itself." White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States*, at 13 (Sept. 8, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf (citing Stoll *et al.*, *The Carbon Footprint Of Bitcoin*, Cell Press 3, 1–15 (Feb. 16, 2019), https://doi.org/10.2139/ssrn.3335781; Alex De Vries, *Bitcoin's energy consumption is underestimated: A market dynamics approach*. Energy Res. Soc. Sci. 70, 101721 (Dec. 2020), https://doi.org/10.1016/j.erss.2020.101721; Cambridge Centre for Alt. Finance, *Cambridge Bitcoin Electricity Consumption Index*, https://cbeci.org/).

114 City of N. Tonawanda, *Public Notice, Digihost Full Envt'l Assessment Form*, at 5 (Aug. 12, 2021), https://www.northtonawanda.org/documents/legal%20notice/fortistar%20amended%20seqr_2.pdf (the City's current usage averages 4 million gallons per day).

115 Thomas J. Prohaska, *North Tonawanda asks for $30 million in emergency aid to repair sewer plant*, Buffalo News (Mar. 12, 2022), https://buffalonews.com/news/local/government-and-politics/north-tonawanda-asks-for-30-million-in-emergency-aid-to-repair-sewer-plant/article_91b32598-a145-11ec-b35d-7314fe498fd0.html.

116 N.Y. State Dep't of Envt'l Conserv, *Greenidge Generation Station: Water Withdrawal*, DEC Permit No. 8-5736-00004/00015, https://www.dec.ny.gov/chemical/123048.html.

117 U.S. EPA, *Nat'l Pollutant Discharge Elimination System — Cooling Water Intake Structures at Existing Facilities & Phase I Facilities*, 76 Fed. Reg. 22,174, 22,246 (proposed Apr. 20, 2011), https://www.federalregister.gov/documents/2011/04/20/2011-8033/national-pollutant-discharge-elimination-system-cooling-water-intake-structures-at-existing; U.S. EPA, *Harmful Algal Blooms and Drinking Water Factsheet* (last visited July 11, 2022) https://www.epa.gov/sites/default/files/2016-11/documents/harmful_algal_blooms_and_drinking_water_factsheet.pdf; *see generally* Steven C. Chapra, *Surface Water-Quality Modeling*, McGraw-Hill (1997).

118 *See* Paul Moore, *What Happened to Turtle Creek's Trophy Bassing*, Game & Fish Magazine (Oct. 4, 2010), https://www.gameandfishmag.com/editorial/fishing_bass-fishing_in_0510_02/243162; Hendrix, *The Ups-and-Downs of Fishing Turtle Creek*, Dubois Cty. Herald (May 24, 2019), https://www.duboiscountyherald.com/sports/local/the-ups-and-downs-of-fishing-turtle-creek/article_8fbf5caa-f629-5e3f-8959-88775a5cc1c6.html; Ind. Div. of Fish & Wildlife, *Animal Info. Series: Largemouth Bass (Micropterus salmoides)* (2012), https://www.in.gov/dnr/fish-and-wildlife/files/fw-largemounth_bass.pdf.

119 Titan, *Immersion cooling for ASIC miners: What is it and how does it work?* (Feb. 10, 2022), https://titan.io/immersion-cooling-for-asic-miners-what-is-it-and-how-does-it-work/; Hive OS, *Prepare your ASICS for hot summer days*, Medium (June 15, 2020), https://medium.com/hiveon/prepare-your-asics-for-hot-summer-days-f57c77015820.

120 N2Global, *Fire Safety in Cryptocurrency Mining: Case Study* (Oct. 22, 2021), https://www.n2global.net/en/media-room/news-highlights/fire-safety-at-cryptocurrency-mining-case-study-by; Levitt Safety, *Protect Your Cryptocurrency Mine With These Fire Mitigation Tactics* (Mar. 28, 2022), https://www.levitt-safety.com/blog/cryptocurrency-mining/.

121 See Rich Miller, *Fire at Bitcoin Mine Destroys Equipment*, Data Center Knowledge (Nov. 6, 2014), https://www.datacenterknowledge.com/archives/2014/11/06/fire-bitcoin-mine-destroys-equipment.

122 Amir Rubin, *Is Bitcoin Mining Insurable, Examples and Loss Characteristics*, AREPA, at 14-16 (2021), https://www.arepa.com/media/xtsbufex/arepa-whitepaper-bitcoin.pdf; Rebecca Heilweil, *Now Might Be a Good Time to Think About Crypto Insurance*, Vox (June 17, 2022), https://www.vox.com/recode/23171782/crypto-terra-ust-celsius-meltdown-crash-insurance; Levitt Safety, *Protect Your Cryptocurrency Mine With These Fire Mitigation Tactics* (Mar. 28, 2022), https://www.levitt-safety.com/blog/cryptocurrency-mining/.

123 Turner Wright, *3K+ Bit Digital hosting partner's crypto miners go offline after explosion and fire*, Cointelegraph (May 20, 2022), https://cointelegraph.com/news/3k-bit-digital-hosting-partner-s-crypto-miners-go-offline-after-explosion-and-fire.

124 *See, e.g.*, Pia Singh, *Bitcoin miners flocked to an upstate New York town for cheap energy — then it got complicated*, CNBC (June 24, 2021), https://www.cnbc.com/2021/06/24/bitcoin-miners-flocked-to-upstate-new-york-for-cheap-energy-then-it-got-complicated.html ("We've put in a whole set of building and safety codes"); *PUD Board Acts To Halt Unauthorized Bitcoin Mining*, NCWLife News (Apr. 2018) https://www.ncwlife.com/news/pud-board-acts-to-halt-unauthorized-bitcoin-mining/article_f013c62b-15a4-5665-ad39-113a61d5503c.html (citing fire risk as a factor).

125 Angela Fritz & Judson Jones, *Half the country is in drought, and no region has been spared*, CNN (Aug. 4, 2022), https://www.cnn.com/2022/08/04/weather/drought-map-northeast-texas-climate/index.html.

126 *See, e.g.*, Jeff Keeling, *Professor: Bitcoin mining's model brings not just noise, but environmental cost that's under scrutiny*, WJHL (updated May 19, 2021), https://www.wjhl.com/news/local/professor-Bitcoin-minings-model-brings-not-just-noise-but-environmental-cost-thats-under-scrutiny/; Robert Houk, *Officials press bitcoin company to find a solution to noise issues*, Johnson City Press (Aug. 23, 2021), https://www.johnsoncitypress.com/news/officials-press-bitcoin-company-to-find-a-solution-to-noise-issues/article_78e62c44-0434-11ec-af1c-bf43ccb2b545.html; Andy Koen, *Noise complaint over crypto mining business led City to buy new equipment*, KOAA News (Jul. 26, 2019), https://www.koaa.com/news/covering-colorado/noise-complaint-over-crypto-mining-business-led-city-to-buy-new-equipment; Andy Fox, *What's That Noise? One of world's largest bitcoin facilities is too loud, VB neighbors say*, Wavy (Aug. 15, 2018), https://www.wavy.com/news/whats-that-noise-one-of-worlds-largest-Bitcoin-facilities-is-too-loud-vb-neighbors-say/; *Norway Council may shut down noisy bitcoin miner*, The Local (Aug. 21, 2018), https://www.thelocal.no/20180821/norway-council-may-shut-down-noisy-Bitcoin-miner/.

127 Compass Mining, *The Basics of Mining Bitcoin at Home* (Aug. 20, 2021), https://compassmining.io/education/how-to-mine-bitcoin-at-home-basics/.

128 Kevin Williams, *An Appalachian town was told a bitcoin mine would bring an economic boom. It got noise pollution and an eyesore*, Wash. Post (Mar. 18, 2022), https://www.washingtonpost.com/business/2022/03/18/bitcoin-mining-noise-pollution-appalachia/.

129 *Id.*

130 Kevin Williams, *A neighborhood's cryptocurrency mine: 'Like a jet that never leaves"*, Wash. Post (Aug. 31, 2022), https://www.washingtonpost.com/business/interactive/2022/cryptocurrency-mine-noise-homes-nc/.

131 Brian D. Stockman, *Bitcoin mine brings heated residents to Ridgway Township meeting*, Ridgway Record (Jun. 22, 2022), https://www.ridgwayrecord.com/news/bitcoin-mine-brings-heated-residents-to-ridgway-township-meeting/article_00184b60-f27e-11ec-8220-134307a1c971.html.

132 Rob Hackford, *Tough questions about North Tonawanda cryptocurrency facility*, WRGZ (Mar. 16, 2022), https://www.wgrz.com/article/news/local/complaints-continue-about-north-tonawanda-cryptocurrency-facility-erie-avenue/71-3f0949bc-9aed-49dd-abad-2fd95dd855db; Rick Pfeiffer, *Public weighs in on high-energy use zoning*, Niagara Gazette (Aug. 25, 2022), https://www.niagara-gazette.com/news/public-weighs-in-on-high-energy-use-zoning/article_25b936dc-0e1b-11ed-b4e4-030009e8482f.html; (50 people who lived close to the mining facility complained about the facility's noise impacts).

133 Vipal Monga, *Bitcoin Mining Noise Drives Neighbors Nuts—a Giant Dentist Drill That Won't Stop*, Wall Street Journal (Nov. 12, 2021), https://www.wsj.com/articles/bitcoin-mining-noise-drives-neighbors-nuts-giant-dentist-drill-that-wont-stop-11636730904.

134 Lois Parshley, *How Bitcoin mining devastated this New York town*, MIT Tech. Review (Apr. 18, 2022), https://www.technologyreview.com/2022/04/18/1049331/bitcoin-cryptocurrency-cryptomining-new-york/.

135 Joachim Klement, *Geo-Economics: The Interplay between Geopolitics, Econ., and Investments*, CFA Inst. Rsch. Found., at 200 (Apr. 2021), https://www.cfainstitute.org/-/media/documents/book/rf-publication/2021/geo-economics-full.pdf; Mark Peplow, *Bitcoin poses major electronic-waste problem*, Chem. & Eng'g News (Mar. 14, 2019), https://cen.acs.org/environment/sustainability/Bitcoin-poses-major-electronic-waste/97/i11; Economic Times, *Bitcoin mining generates tonnes of e-waste: Study* (Sept. 21, 2021), https://economictimes.indiatimes.com/markets/cryptocurrency/bitcoin-mining-generates-tonnes-of-e-waste-study/articleshow/86391133.cms.

136 Lumerin Protocol, *How to prolong your ASIC miner's lifespan*, Medium (Nov. 23, 2021), https://medium.com/lumerin-blog/how-to-prolong-your-asic-miners-lifespan-360b68140a04; Minery, *How Long Do ASICs Last?* (May 16, 2022), https://minery.io/blog/how-long-do-asics-last/.

137 For background into the public health and environmental concerns surrounding electronic waste, *see generally* Megan Avakian, *E-waste: An Emerging Health Risk*, Nat'l Inst. of Env't Health Scis. (Feb. 2014), https://www.niehs.nih.gov/research/programs/geh/geh_newsletter/2014/2/spotlight/ewaste_an_emerging_health_risk_.cfm; U.S. EPA, *Cleaning Up Electronic Waste (E-Waste)* (last updated Nov. 2, 2021), https://www.epa.gov/international-cooperation/cleaning-electronic-waste-e-waste.

138 Alex de Vries & Christian Stoll, *Bitcoin's growing e-waste problem*, 175 Res., Conserv. & Recycling 105901 (Dec. 2021), https://www.sciencedirect.com/science/article/abs/pii/S0921344921005103?dgcid=author.

139 *Id.*; BBC, *Bitcoin mining produces tons of waste* (Sept. 20, 2021), https://www.bbc.com/news/technology-58572385; Digiconomist, *Bitcoin Elec. Waste Monitor* (last visited Aug 29, 2022), https://digiconomist.net/Bitcoin-electronic-waste-monitor/.

140 Peter Howson & Alex de Vries, *Preying on the poor? Opportunities and challenges for tackling the social and env't threats of cryptocurrencies for vulnerable and low-income communities*, 84 Energy Rsch. & Soc. Sci. 102394 (2022), https://www.sciencedirect.com/science/article/abs/pii/S2214629621004813.

141 Cherokee Scout, *Landfill cracking down on foam' from crypto mining* (July 26, 2022), https://www.cherokeescout.com/local-newsletter/landfill-cracking-down-foam-crypto-mining ("The revisions include language that bans materials such as polyethylene, polypropylene and similar types of packing materials from commercial haulers from any nonresidential point of origin. . . . [since this] 'incompressible foam cannot be compacted with our compactor.'").

142 For example, in Idaho, investor-owned utility Idaho Power requested that cryptominers prepay for required infrastructure upgrades to prevent stranded assets on remaining ratepayers when the economics of cryptocurrency change. Idaho Pub. Utils. Comm'n, *Application of Idaho Power Co. for Authority to Establish a New Schedule to Serve Speculative High-Density Load Customers*, at 13-14, Case No. IPC-E-21-27 (Nov. 4, 2021), https://puc.idaho.gov/Fileroom/PublicFiles/ELEC/IPC/IPCE2137/CaseFiles/20211104Application.pdf; *see also* Justine Calma, *Texas' Fragile Grid Isn't Ready for Crypto Mining's Explosive Growth*, The Verge (July 14, 2022), https://www.theverge.com/2022/7/14/23206795/bitcoin-crypto-mining-electricity-texas-grid-energy-bills-emissions ("Unfortunately, the costs for building out all this infrastructure are often passed on to consumers — particularly if it's done at a huge scale under a rushed timeline as crypto mining might demand.").

143 Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid.

144 U.S. House Committee on Energy & Commerce Staff, *Memorandum re: Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains*, at 9 (Jan. 17, 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Briefing%20Memo_OI%20Hearing_2022.01.20.pdf.

145 McKenzie Delisle, *Mining operation moves out of city for winter*, Press-Republican (Nov. 11, 2019), https://www.pressrepublican.com/news/local_news/mining-operation-moves-out-of-city-for-winter/article_4c86c044-4e1e-5ad6-8e6d-0ad19b875e35.html.

146 Ariel Drehobl *et al.*, *How High are Household Energy Burdens?* Am. Council for an Energy-Efficient Economy, at ii (Sept. 2020), https://www.aceee.org/sites/default/files/pdfs/u2006.pdf.

147 Ky. Pub. Serv. Comm'n, Order, *In re: Elec. App'n of Big Rivers Elec. Corp. for a Certificate of Pub. Convenience & Necessity to Construct a 161 kV Transmission Line in McKracken Cty., Ky.*, Case No. 2021-002705 (Jan. 14, 2022), https://psc.ky.gov/order_vault/orders_2022/202100275_01142022_01.pdf.

148 *Id.*; Ky. Pub. Serv. Comm'n, Order, *In re: Elec. Tariff Filing of Big Rivers Elec. Corp. & Jackson Purchase Energy Corp.*, Case No. 2021-00282 (Oct. 14, 2021), https://psc.ky.gov/pscscf/2021%20Cases/2021-00282//20211014_PSC_ORDER.pdf.

149 Ky. Pub. Serv. Comm'n, Application, *In re: Elec. Application of Ky. Power Co. for an Ord. Approving the Co.'s Amended Tariff E.D.R.*, Case No. 2022-00181 (Jun. 9, 2022), https://psc.ky.gov/pscecf/2022-00181/lmscott%40aep.com/06092022040357/KPCO_Application.pdf.

150 Ky. Energy & Env;t Cabinet, *Energy Affordability*, https://eec.ky.gov/Energy/Programs/EnergyAffordability/Pages/default.aspx ("While Kentucky has relatively low energy prices, it does have areas with high energy burdens that can threaten a household's ability to pay for energy, and force tough choices between paying energy bills and buying food, medicine, or other essentials."); Emily Bennett, *WSAZ Investigates | Kentucky Power bill spike*, WSAZ (Jan. 28, 2022), https://www.wsaz.com/2022/01/28/wsaz-investigates-kentucky-power-bill-spike/ (explaining that Kentucky Power ratepayers saw a major increase in their electric bills in January 2022); Avi Asher-Schapiro, *Coal to Crypto: The Gold Rush Bringing Bitcoin Miners to Kentucky*, Thomson Reuters Found. (Mar. 14, 2022), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate.

151 Avi Asher-Schapiro, *Coal to Crypto: The Gold Rush Bringing Bitcoin Miners to Kentucky*, Thomson Reuters Found. (Mar. 14, 2022), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate.

152 Neb. Public Power District, 2021 Financial Report, at 6, https://docs.nppd.com/2021FinancialReport.pdf; Peter Maloney, *Bitcoin mining operation to add flexible load to NPPD's area*, Am. Public Power Ass'n (Mar. 17, 2021), https://www.publicpower.org/periodical/article/bitcoin-mining-operation-add-flexible-load-nppds-area.

153 Matteo Benetton *et al.*, *When Cryptocurrency Comes to Town: High Electricity-Use Spillovers to the Local Economy*, SSRN, at 3 (May 2021, last updated Aug. 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720.

154 *Id.* at 1, 5.

155 See Application of Idaho Power Co. for Authority to Establish a New Schedule to Serve Speculative High-Density Load Customers, at 5, Idaho Pub. Util. Comm'n Case No. IPC-E-21-37 (Nov. 4, 2021), https://puc.idaho.gov/Fileroom/PublicFiles/ELEC/IPC/IPCE2137/CaseFiles/20211104Application.pdf.

156 *Id.* at 3.

157 *Id.* at 14.

158 Idaho Power, *Compliance Filing—Tariff Schedule 20*, Idaho Pub. Util. Comm'n Case No. IPC-E-21-37 (Jun. 15, 2022), https://puc.idaho.gov/Fileroom/PublicFiles/ELEC/IPC/IPCE2137/CaseFiles/20220705Final%20Approved%20Tariffs.pdf.

159 Idaho Pub. Util. Comm'n, *Order No. 35428*, at 6, Case No. IPC-E-21-37 (Jun. 15, 2022), https://puc.idaho.gov/Fileroom/PublicFiles/ELEC/IPC/IPCE2137/OrdNotc/20220615Final_Order_No_35428.pdf.

160 GeoBitmine, *Petition for Reconsideration*, at 2, Idaho Pub. Util. Comm'n Case No. IPC-E-21-37 (Jul. 6, 2022), https://puc.idaho.gov/Fileroom/PublicFiles/ELEC/IPC/IPCE2137/Intervenor/Geobitmine/20220706Petition%20for%20Reconsideration.pdf; Ethan Howland, *GeoBitmine challenges Idaho Power's 'discriminatory' rate for cryptocurrency mining facilities*, Utility Dive (Jul. 7, 2022), https://www.utilitydive.com/news/geobitmine-idaho-power-cryptocurrency-mining-rate/626724/; Katelyn Weisbrod, *Bitcoin Mining Startup in Idaho Challenges Utility on Rates for Energy-Gobbling Data Centers*, Inside Climate News (Aug. 2, 2022), https://insideclimatenews.org/news/02082022/bitcoin-crypto-mining-idaho/.

161 *In the Matter of the Application of Entergy Arkansas, LLC for a Proposed Tariff Regarding Large Power High-Load Density ("Crypto Mining"), Direct Testimony of D. Andrew Owens*, at 8 (Jul. 28, 2022), Ark. Pub. Serv. Comm'n, Docket No. 22-032-TF, http://www.apscservices.info/pdf/22/22-032-TF_16_1.pdf.

162 *Id.* at 13 .

163 *Id.*

164 *Direct Testimony of Caleb Bales*, at 7-8 (Jul. 28, 2022), Ark. Pub. Serv. Comm'n, Docket No. 22-032-TF, http://www.apscservices.info/pdf/22/22-032-TF_17_1.pdf.

165 Steve Wright, *Testimony Before the Subcommittee on Oversight and Investigations*, at 2, 5, U.S. House Committee on Energy and Commerce (Jan. 20, 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Wright_OI_2022.01.20.pdf; *see also* Stephen Wright, *Questions for the Record re: Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains* (Jan. 20, 2022), https://docs.house.gov/meetings/IF/IF02/20220120/114332/HHRG-117-IF02-Wstate-WrightS-20220120-SD001.pdf.

166 Paul Ciampoli, *Public power can charge cryptocurrency firms higher rates: N.Y. PSC*, Am. Public Power Ass'n (Mar. 16, 2018), https://www.publicpower.org/periodical/article/public-power-can-charge-cryptocurrency-firms-higher-rates-ny-psc.

167 David Erickson, *Missoula County adopts emergency 'green' regulations for cryptocurrency; operators protest*, Missoulian (Apr. 4, 2019), https://missoulian.com/news/local/missoula-county-adopts-emergency-green-regulations-for-cryptocurrency-operators-protest/article_57dd537d-b267-5443-aa67-822358a1e666.html; David Erickson, *Bitcoin mining company announces plans for 50-megawatt data center in Polson*, Missoulian (Jun. 3, 2022), https://missoulian.com/news/local/bitcoin-mining-company-announces-plans-for-50-megawatt-data-center-in-polson/article_8da1ad15-ebf1-5cba-9158-35406e649073.html.

168 *See, e.g.*, Jacob Elkin, *New Sabin Center White Paper Assesses the New York State Executive Branch's Authority to Enact a Moratorium on the Permitting of Consolidated Proof-Of-Work Cryptocurrency Mining Facilities*, Columbia Law School Sabin Center for Climate Change Law (Mar. 21, 2022), https://blogs.law.columbia.edu/climatechange/2022/03/21/new-sabin-center-white-paper-assesses-the-new-york-state-executive-branchs-authority-to-enact-a-moratorium-on-the-permitting-of-consolidated-proof-of-work-cryptocurrency-mining-facilities/.

169 Fitch Ratings, *Crypto Mining Poses Challenges to Public Power Utilities* (Jan. 24, 2022), https://www.fitchratings.com/research/us-public-finance/crypto-mining-poses-challenges-to-public-power-utilities-24-01-2022 ("Digital asset or crypto currency mining in the US could pose power supply risks to public power utilities unless they are sufficiently mitigated. . . Crypto mining is energy intensive and requires a considerable amount of power that can significantly increase a utility's overall electrical load. Utilities must balance the revenue prospect of increased electrical sales with the commitment to procure or generate large amounts of power for crypto mining operations.").

170 Gabriel Pacyniak, *Greening the Old New Deal: Strengthening Rural Electric Cooperative Supports and Oversight to Combat Climate Change*, Missouri Law Review, 413 (2020), https://scholarship.law.missouri.edu/mlr/vol85/iss2/20/.

171 Cooperatives that receive financing from the Rural Utility Service (RUS) of the U.S. Department of Agriculture or sell less than 4 million MWh of electricity per year (and any cooperative owned by members who meet one or both of these qualifications) are exempt from FERC oversight under the Federal Power Act. As a lender, RUS does impose some requirements on cooperatives, however, these are primarily designed to ensure repayment, rather than protect ratepayers. *See* 16 U.S.C.A. § 824(f) (West 2015).

172 Gabriel Pacyniak, *Greening the Old New Deal: Strengthening Rural Electric Cooperatives Supports and Oversight to Combat Climate Change*, Missouri Law Review, 415 (2020), https://scholarship.law.missouri.edu/mlr/vol85/iss2/20/.

173 Jim Cooper, *Policy Essay: Electric Co-Operatives: From New Deal to Bad Deal?* 45 Harv. J. on Legis. 335, 352, 361 (2008), https://harvardjol.com/wp-content/uploads/sites/17/2013/10/335-376_Cooper1.pdf.

174 *See id.* at 349.

175 Haley Cawthon, *AboutBit to open new crypto mining facility in Southern Indiana*, Business Journals (May 11, 2022), https://www.bizjournals.com/louisville/inno/stories/news/2022/05/11/aboutbit-merom-mining.html. As of this writing, the Merom sale is still subject to FERC approval under Section 203 of the Federal Power Act. *See In re* Hallador Power Co., LLC, FERC Docket No. EC22-52.

176 Kenzie Dillow, *Cryptocurrency mining company expanding; Utility company investing millions in Paducah*, WSILTV (Jun. 9, 2021), https://www.wsiltv.com/news/consumer/cryptocurrency-mining-company-expanding-utility-company-investing-millions-in-paducah/article_5a08198a-fba2-5c89-aa8a-1a30502fe567.html.

177 David Zoeller, *Bitcoin mining company plans Paducah expansion*, Kentucky Today (Oct. 6, 2021), https://www.kentuckytoday.com/state/bitcoin-mining-company-plans-paducah-expansion/article_bea8ae26-7bc7-5994-b703-d26745cc9d27.html.

178 Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid.

179 *Id.*

180 Fitch Ratings, *Crypto Mining Poses Challenges to Public Power Utilities* (Jan. 24, 2022), https://www.fitchratings.com/research/us-public-finance/crypto-mining-poses-challenges-to-public-power-utilities-24-01-2022.

181 Provided by Fossil Free Tompkins. *See also* N.Y. State Senate Finance Committee & Assembly Ways and Means Committee, *Joint Leg. Hearing in the Matter of the 2022–2023 Exec. Budget on Envt'l Conservation*, at 2:31:32 (Feb. 1, 2022), https://www.youtube.com/watch?v=NaB5hqsEqMM&t=9092s (New York State Energy Research and Development Authority President Doreen Harris stated, "There could be a very significant impact on New York's load resulting from crypto, depending on the penetration of the resource."); Lois Parshley, *How Bitcoin mining devastated this New York town: Between rising electricity rates and soaring climate costs, cryptomining is taking its toll on communities*, MIT Tech. Review (Apr. 18, 2022), https://www.technologyreview.com/2022/04/18/1049331/bitcoin-cryptocurrency-cryptomining-new-york/ (One town official in Plattsburgh "recalls one prospector calling to see if he could get five gigawatts—'I said, "Excuse me. That's a quarter of what New York state uses on a given day!"' Plattsburgh was soon receiving a major mining application every week.").

182 Erica Proffer, *Here is why death totals from Winter Storm Uri may vary*, KVUE (Feb. 15, 2022), https://www.kvue.com/article/weather/winter-storm/here-is-why-death-totals-from-winter-storm-uri-may-vary/269-f2bf277f-74d9-443b-ab2e-ff89f336f3ec.

183 Chris Stipes, *New Report Details Impact of Winter Storm Uri on Texans*, Univ. of Houston (Mar. 29, 2021), https://uh.edu/news-events/stories/2021/march-2021/03292021-hobby-winter-storm.php.

184 Tech Transparency Project, *Cryptocurrency Miners' Sweetheart Deal with Texas Threatens an Already Fragile Grid* (July 21, 2022), https://www.techtransparencyproject.org/sites/default/files/Crypto%20Texas%20Report.pdf (citing Riot Blockchain, Inc., *Form 10-Q, Quarterly Report* (Aug. 23, 2021), https://seekingalpha.com/filing/5677790); Fortune, *How Riot Blockchain capitalized on a hot Texas summer to make more money selling power than mining crypto*, https://fortune.com/2022/08/13/riot-blockchain-bitcoin-mining-texas-electric-grid-subsidy/ (Aug. 13, 2022) ("For many hours, spot prices soared so high that Riot could sell power to Ercot for 50 or more times the low fixed price it was paying" for electricity to mine cryptocurrency).

185 Cynthia & George Mitchell Found., *Statement: Never Again One Year Late: A Reliability Report Card* (Feb. 14, 2022), https://www.cgmf.org/blog-entry/475/Statement-Never-Again-One-Year-Later-%7C-A-Reliability-Report-Card.html. *See also* Cynthia & George Mitchell Found., *Report: Never Again: How to Prevent Another Major Texas Electricity Failure* (Jun. 3, 2021), https://cgmf.org/blog-entry/435/REPORT-%7C-Never-Again-How-to-prevent-another-major-Texas-electricity-failure.html.

186 ERCOT, *Seasonal Assessment of Resource Adequacy for the ERCOT Region (SARA) Winter 2021/2022* (Nov. 19, 2021), https://www.ercot.com/files/docs/2021/11/19/SARA_Winter2021-22.pdf; Erin Douglas, *Texas grid vulnerable to blackouts during severe winter weather, even with new preparations, ERCOT estimates show*, Texas Tribune (Nov. 20, 2021), https://www.texastribune.org/2021/11/20/texas-grid-ercot-winter-estimates/.

187 Naureen S. Malik, *Texas crypto miners could require as much power as all of New York state*, Bloomberg (Aug. 26, 2022), https://www.bloomberg.com/news/articles/2022-08-26/texas-crypto-rush-may-need-as-much-power-as-entire-state-of-n-y.

188 ERCOT, *Fact Sheet* (July 2022), https://www.ercot.com/files/docs/2022/02/08/ERCOT_Fact_Sheet.pdf.

189 Naureen S. Malik, *Texas crypto miners could require as much power as all of New York state*, Bloomberg (Aug. 26, 2022), https://www.bloomberg.com/news/articles/2022-08-26/texas-crypto-rush-may-need-as-much-power-as-entire-state-of-n-y.

190 33 GW of cryptomining equipment operating at 85% load factor results in 245.7 TWh per year. Total Florida consumption in 2021 was 244 TWh. Source: Energy Information Administration, Annual Electric Power Industry Report, Form EIA-861. (Last accessed August 3, 2022). https://www.eia.gov/electricity/data/eia861/

191 MacKenzie Sigalos, *Bitcoin miners say they're helping to fix the broken Texas electric grid—and Ted Cruz agrees*, CNBC (updated Dec. 5, 2021), https://www.cnbc.com/2021/12/04/bitcoin-miners-say-theyre-fixing-texas-electric-grid-ted-cruz-agrees.html.

192 Tech Transparency Project, *Cryptocurrency Miners' Sweetheart Deal with Texas Threatens an Already Fragile Grid*, at 2-3 (July 21, 2022), https://www.techtransparencyproject.org/sites/default/files/Crypto%20Texas%20Report.pdf (citing Alex Liegl (@alexanderliegl), Twitter (Aug. 6 2020), https://twitter.com/alexanderliegl/status/1291395637318234112).

193 Naureen S. Malik, *Crypto Miners in Texas Need 'Approval to Energize' in New Grid Hurdle*, Bloomberg (Mar. 30, 2022), https://www.bloomberg.com/news/articles/2022-03-30/texas-crypto-miners-need-approval-to-energize-in-grid-hurdle.

194 *Id.*

195 Bloomberg Wire, *Texas now requiring crypto miners to seek 'approval to energize' before plugging into grid*, Dallas Morning News (Mar. 30, 2022), https://www.dallasnews.com/business/energy/2022/03/30/texas-now-requiring-crypto-miners-to-seek-approval-to-energize-before-plugging-into-grid/; Chris Reeder & Miguel Suazo, *ERCOT Now Requires Cryptocurrency Miners to Provide Info. on Their Impact to the Texas Power Grid*, JDSupra (Apr. 6, 2022), https://www.jdsupra.com/legalnews/ercot-now-requires-cryptocurrency-6065651/.

196 Morgan Riddell, *Brenham officials discuss cryptocurrency and their ability to sustain energy demands that come with it*, KBTX (Mar. 28, 2022), https://www.kbtx.com/2022/03/29/brenham-officials-discuss-cryptocurrency-their-ability-sustain-energy-demands-that-come-with-it/.

197 Josh Saul, *Georgia is becoming the new hot spot for growing crypto in the U.S.—and Bitcoin miners are taking notice*, Fortune (Feb. 7, 2022), https://fortune.com/2022/02/07/georgia-hot-spot-bitcoin-mining-us-crypto-energy/.

198 Avi Asher-Schapiro, *Coal to crypto: The gold rush bringing bitcoin miners to Kentucky*, Thomson Reuters Found. (Mar. 14, 2022), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate; *see also* Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market*, Nat'l Bureau of Econ. Rsch., Working Paper No. 29396, at 4 (Oct. 2021), https://www.nber.org/system/files/working_papers/w29396/w29396.pdf ("The top 10% of [cryptocurrency] miners control 90% [of mining] and just 0.1% (about 50 miners) control close to 50% of mining capacity.").

199 Bill Estep, *Kentucky's digital gold rush. What's behind the crypto mining boom in coal country?* Lexington Herald Leader (Apr. 21, 2022), https://www.kentucky.com/news/state/kentucky/article259880855.html.

200 Bootstrap Energy, LLC, *Project Corpus Christi Energy Park*, at 22–24 (Mar. 25, 2022), https://corpuschristi.legistar.com/View.ashx?M=F&ID=10675758&GUID=10B47135-9684-416F-A8C0-D46E8AA2B5AE; *see also* City of Corpus Christi, *Agenda Memorandum re Disannexation and Amendment Industrial District #2 Boundaries*, at 2 (Mar. 3, 2022) https://corpuschristi.legistar.com/View.ashx?M=F&ID=10666001&GUID=E7BE68AC-B0F7-4198-B758-739D20E1814D ("However, staff's financial analysis concludes the City will forego $70,501,509 over a ten-year period if the same development were constructed and operated outside of an Industrial District Agreement in the city limits.").

201 City of Corpus Christi, *Agenda Memorandum re Disannexation and Amendment Industrial District #2 Boundaries*, at 2 (Mar. 3, 2022) https://corpuschristi.legistar.com/View.ashx?M=F&ID=10666001&GUID=E7BE68AC-B0F7-4198-B758-739D20E1814D.

202 Laura Counts, *Power-hungry cryptocurrency miners push up electricity costs for locals*, Berkeley Haas (Aug. 3, 2021), https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-locals/ (quoting Assistant Professor Giovanni Compiani, one of the co-authors of Matteo Benetton *et al.*, *When Cryptocurrency Comes to Town: High Electricity-Use Spillovers to the Local Economy*, SSRN, at 3 (Aug. 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720).

203 Fitch Ratings, *Crypto Mining Poses Challenges to Public Power Utilities* (Jan. 24, 2022), https://www.fitchratings.com/research/us-public-finance/crypto-mining-poses-challenges-to-public-power-utilities-24-01-2022.

204 *See* Ky. Pub. Serv. Comm'n, Case No. 2021-00282, I*n re: Elec. Tariff Filing of Big Rivers Elec. Corp. and Jackson Purchase Energy Corp.*, Order at 12 (Oct. 14, 2021), https://psc.ky.gov/pscscf/2021%20Cases/2021-00282//20211014_PSC_ORDER.pdf.

205 Core Scientific, Inc., *Form 10-K, Annual Report*, at 11 (for year ending Dec. 31, 2021)), https://www.sec.gov/ix?doc=/Archives/edgar/data/1839341/000119312522088850/d268076d10k.htm.

206 In its Form 10-K, Marathon offers that its stock value of $3.1 billion is based on the closing sale price of registrant's common stock as quoted on the Nasdaq Capital Market on June 30, 2021. *See* Marathon Digital Holdings, Inc., *Form 10-K, Annual Report*, at 1, 19 (for year ending Dec. 31, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001507605/000149315222006446/form10-k.htm.

207 Stronghold Digital Mining, Inc., *Form 10-K, Annual Report*, at 16 (for year ending Dec. 31, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001856028/000162828022007706/sdig-20211231.htm.

208 Alex Brown, *Startup to Establish Crypto Mining Facility in Sullivan County*, Inside Ind. Business (May 11, 2022), https://www.insideindianabusiness.com/articles/startup-to-establish-crypto-mining-facility-in-sullivan-county.

209 Susan Arbetter, *Greenidge Generation permit renewal draws supporters, critics over cryptocurrency mining*, NY State of Politics (Oct. 13, 2021), https://nystateofpolitics.com/state-of-politics/new-york/politics/2021/10/13/greenidge-generation-permit-renewal-draws-supporters--critics-over-cryptocurrency-mining. In contrast, Finger Lakes region's driving economic engine, where Greenidge is located, is agriculture and tourism. This generates $3 billion into New York's economy annually and supports approximately 60,000 jobs—all of which rely heavily on clean air and water. Sen. Gillibrand, *Legislation To Designate Finger Lakes Region As A National Heritage Area Passes Key Committee* (Mar. 12, 2018), https://www.gillibrand.senate.gov/news/press/release/senator-gillibrands-legislation-to-designate-finger-lakes-region-as-a-national-heritage-area-passes-key-committee; *see also* Tourism Economics, *Economic Impact of Visitors in New York* (2019), https://www.fingerlakes.org/sites/default/files/Research%20Center/Oxford%20Economics/Finger-Lakes-2019-NYS-Tourism-Economic-Impact.pdf; Tourism Economics, *The Economic Impact of Tourism in New York* (2018), https://assets.simpleviewinc.com/simpleview/image/upload/v1/clients/fingerlakesvc/NYS_Tourism_Impact_2018_Finger_Lakes_CLIENT_294d3cec-3088-4351-bf64-2439830d34d1.pdf.

210 Adam Willis, *Large-scale crypto mining data center planned for western North Dakota oil patch*, In Forum (Jan. 26, 2022), https://newsroom.inforum.com/business/large-scale-crypto-mining-data-center-planned-for-western-north-dakota-oil-patch.

211 U.S. House Committee on Energy & Commerce Staff, *Memorandum re Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains*, at 9 (Jan. 17, 2021), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Briefing%20Memo_OI%20Hearing_2022.01.20.pdf.

212 Pia Singh, *Bitcoin miners flocked to an upstate New York town for cheap energy — then it got complicated*, CNBC (June 24, 2021). https://www.cnbc.com/2021/06/24/bitcoin-miners-flocked-to-upstate-new-york-for-cheap-energy-then-it-got-complicated.html.

213 Lois Parshley, *How Bitcoin mining devastated this New York town: Between rising electricity rates and soaring climate costs, cryptocurrency mining is taking its toll on communities*, MIT Tech. Review (Apr. 18, 2022), https://www.technologyreview.com/2022/04/18/1049331/bitcoin-cryptocurrency-cryptomining-new-york/.

214 Steve Wright, *Testimony Before the Subcommittee On Oversight And Investigations*, House Energy and Commerce Committee, at 3 (Jan. 20, 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Wright_OI_2022.01.20.pdf.

215 David Jeans, *Data in the Dark: How Big Tech Secretly Secured $800 Million in Tax Breaks for Data Centers*, Forbes (Aug. 19, 2021), https://www.forbes.com/sites/davidjeans/2021/08/19/data-in-the-dark-how-big-tech-secretly-secured-800-million-in-tax-breaks-for-data-centers/?sh=2e6992fc6b43.

216 Avi Asher-Schapiro, *Coal to crypto: The gold rush bringing bitcoin miners to Kentucky*, Thomson Reuters Found. (Mar. 14, 2022), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate.

217 Bitcoin Mining Council, *Bitcoin Mining Council Survey Confirms year on year improvements in sustainable power mix* (Apr. 25, 2022), https://bitcoinminingcouncil.com/bitcoin-mining-council-survey-confirms-year-on-year-improvements-in-sustainable-power-mix-and-technological-efficiency/.

218 Laurie Clarke, *How do we solve bitcoin's carbon problem?* Guardian (Jan. 30, 2022), https://www.theguardian.com/technology/2022/jan/30/how-do-we-solve-bitcoins-carbon-problem.

219 Cambridge Centre for Alt. Finance, *3rd Global Cryptoasset Benchmarking Study*, at 11 (Sept. 2020), https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/.

220 Claiming carbon neutrality on the basis of proximity is not the only way miners have inflated their environmental credentials. For example, Riot Blockchain, one of the largest single Bitcoin miners in the United States, in a response to a Senate inquiry, cites its smaller Massena, New York existing hydro-connected facility as a "sustainable energy source" and cites the average generating mix of Texas for its much larger Whinstone facility, claiming that since wind and solar comprise 28% of the grid, that it is somehow supporting renewables. Riot Blockchain, Inc., Letter from Jason Les, Chief Executive Officer of Riot Blockchain, Inc., to U.S. Senators and Representatives (Feb. 24, 2022), https://www.warren.senate.gov/imo/media/doc/Riot%20Response%20Letter%202.24.20223.pdf. Similarly, in early 2022, Marathon announced its "commitment" for its "mining operations to be 100% carbon neutral by the end of 2022." Marathon Digital Holdings, *Marathon Digital Holdings Announces Intent to Transition Hardin, Montana Bitcoin Mining Operations to More Sustainable Power Sources* (Aug. 5, 2022), https://ir.marathondh.com/news-events/press-releases/detail/1282/marathon-digital-holdings-announces-intent-to-transition. However, the mining company is served by a coal-heavy utility in North Dakota (Otter Tail Power, through a hosting agreement with Applied Blockchain) as well as a direct agreement with a gas plant in Texas (Wolf Hollow, through a hosting agreement with Compute North in Granbury, TX).

221 Argo Blockchain LLC, *2021 Sustainability Report*, at 6 (Aug. 18, 2022), https://assets.website-files.com/61817e625cc1f4f31f76f168/62fd4268c4845b503ae68e2b_Argo%202021%20Sustainability%20Report%20v9%20WEB.pdf.

222 *Id.* at 11.

223 *Id.* at 4, 7. For this particular instance, it is worthwhile to note that voluntary RECs (such as those in Texas) are created as an additional value stream from producers that have typically built cost-effective clean energy and are seeking incremental revenues. Texas RECs are the lowest cost (and least meaningful) RECs in the nation. Amanda Luhavalja, *Texas Renewable Energy Credit Markets Advance; Green-E Prices Back Off*, S&P Global Market Intelligence (Aug. 28, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/texas-renewable-energy-credit-markets-advance-green-e-prices-back-off-60107962.

224 Marginal emissions rates have been the subject of study for well over a decade. Kris R. Voorspools & William D. D'haeseleer, *The Influence of the Instantaneous Fuel Mix for Electricity Generation on the Corresponding Emissions*, 25 Energy 1119-38 (2000), https://doi.org/10.1016/S0360-5442(00)00029-3; EPA offers a tool designed for state air regulators to assess the value of clean energy programs by assessing the marginal emissions value of the programs. U.S. EPA, *Avoided Emissions and Generation Tool* (AVERT), https://www.epa.gov/avert.

225 For an example, imagine a system with only two generators: a nuclear power plant with effectively constant output, and a gas-fired power plant that ramps up to meet peak loads, and turns down at night. Assuming there is enough excess in the system, a new load entering the system will drive an increase in the output of the gas plant, as the nuclear plant is unable to adjust upwards. The average emissions rate of the system would reflect the combined emissions rate of the nuclear plant and the gas plant; but the incremental load had no bearing on the operations of the nuclear plant. Therefore, the emissions that matter are the marginal emissions—i.e., the emissions rate of the gas plant alone.

226 S. P. Holland et al., *Why Marginal CO_2 Emissions Are Not Decreasing For US Electricity: Estimates and Implications For Climate Policy* (Feb. 14, 2022), https://www.pnas.org/doi/full/10.1073/pnas.2116632119.

227 Core Scientific, *Press Release, North American Blockchain Infrastructure Leader Core Scientific to Expand Current Capacity With New 300MW Denton, Texas Data Center* (Oct. 7, 2021), https://corescientific.com/press/north-american-blockchain-infrastructure-leader-core-scientific-to-expand-current-capacity-with-new-300mw-denton-texas-data-center/.

228 Core Scientific, Inc., *Form 10-K, Annual Report*, at 5 (for year ending Dec. 31, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/1839341/000119312522088850/d268076d10k.htm

229 *Id.* at 8; Tenn. Valley Auth., *TVA at a Glance* (last visited Aug. 29, 2022), https://www.tva.com/about-tva/tva-at-a-glance.

230 Core Scientific, Inc., *Form 10-K, Annual Report*, at 6 (for year ending Dec. 31, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001839341/000119312522088850/d268076d10k.htm.

231 Argo Blockchain, LLC, 2021 *Sustainability Report*, at 6 (Aug. 18, 2022), https://assets.website-files.com/61817e625cc1f4f31f76f168/62fd4268c4845b503ae68e2b_Argo%202021%20Sustainability%20Report%20v9%20WEB.pdf.

232 For more about RECs, *see, e.g.*, S&P Global, *Problematic corporate purchases of clean energy credits threaten net zero goals*, https://www.spglobal.com/esg/insights/problematic-corporate-purchases-of-clean-energy-credits-threaten-net-zero-goals; Bloomberg, *Flawed Renewable Energy Credits Are Derailing Climate Efforts* (June 9, 2022), https://www.bloomberg.com/news/articles/2022-06-09/flawed-renewable-energy-credits-are-derailing-climate-efforts.

233 Greenidge Generation Holdings Inc., *Greenidge Generation Bitcoin Mining Operation To Be Carbon Neutral in 2021 and Beyond* (May 14, 2021), https://www.prnewswire.com/news-releases/greenidge-generation-bitcoin-mining-operation-to-be-carbon-neutral-in-2021-and-beyond-301291782.html; Peter Mantius, *Greenidge Wows Wall Street With Story of 'Carbon Neutral' Bitcoin Mining; But Is It Only 'Window Dressing?'*, Waterfront Online (Aug. 26, 2021), https://waterfrontonline.blog/2021/08/26/greenidge-wows-wall-street-with-story-of-carbon-neutral-bitcoin-mining-but-is-it-little-more-than-window-dressing/.

234 HBO, *Carbon Offsets: Last Week Tonight with John Oliver*. Season 9 - Episode 21 (Aug. 22, 2022), https://pressroom.warnermedia.com/na/video/carbon-offsets-last-week-tonight-john-oliver?language_content_entity=en; Raphael Calel *et al.*, *Do carbon offsets offset carbon?* Centre for Climate Change Econs. & Policy, at 1 (Nov. 2021), https://www.lse.ac.uk/granthaminstitute/wp-content/uploads/2021/11/working-paper-371-Calel-et-al..pdf.

235 For more on blockchain-enabled offset tracking, *see, e.g.*, Andrew Bruce, *The Near-Term Future Of Blockchain: Tracking Carbon Offsets*, Forbes (Aug. 16, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/08/16/the-near-term-future-of-blockchain-tracking-carbon-offsets/?sh=2cebf2585790; Akshat Rathi & Natasha White, *The Biggest Crypto Effort to End Useless Carbon Offsets Is Backfiring*, Bloomberg (Apr. 7, 2022), https://www.bloomberg.com/news/articles/2022-04-07/the-biggest-crypto-effort-to-end-useless-carbon-offsets-is-backfiring; Justine Calma, *Crypto Can't Fix Carbon Offsets — But Crypto Fans Are Trying Anyway*, The Verge (Aug. 18, 2022), https://www.theverge.com/2022/8/18/23310254/carbon-offset-credits-crypto-tokens-adam-neumann-wework.

236 *See, e.g.*, Wattum Mgmt., *Bitcoin Mining as a Solution to the Energy Curtailment Dilemma* (Sept. 21, 2021), https://wattummanagement.com/blog/bitcoin-mining-as-a-solution-to-the-energy-curtailment-dilemma/; Russell Gold, *Bitcoin Miners Could Save the Texas Grid—or Sink It*, Texas Monthly (Aug. 2022), https://www.texasmonthly.com/news-politics/texas-bitcoin-mining-solar-power-grid/; Nic Carter & Ross Stevens, *Bitcoin Net Zero* (Sept. 2021), https://assets.website-files.com/614e11526f6630959fc98679/616df63a27a7ec339f5e6a80_NYDIG-BitcoinNetZero_SML.pdf; @MinersetCrypto, *Bitcoin is the ultimate green tech*, Twitter (Apr. 22, 2022), https://twitter.com/MinersetCrypto/status/1517555906896175107; Margot Paez & Troy Cross, *Bitcoin and the Energy Transition*, Bitcoin Policy Inst. (last visited Aug. 29, 2022), https://uploads-ssl.webflow.com/627aa615676bdd1d47ec97d4/62f41b9ce54e014f9869efa7_OSTP.docx.pdf.

237 California Independent System Operator (CAISO), *Managing Oversupply* (2022), http://www.caiso.com/informed/Pages/ManagingOversupply.aspx. Based on January—July 2022 data.

238 Per author's calculation, 200 MW at an 85% load factor for one year is ~1.5 million MWh (200 MW * 8760 hours * 0.85). which matches the total curtailment of solar and wind from January 2021 to December 2021 = 1.5 million MWh. CAISO, *Managing oversupply*, http://www.caiso.com/informed/Pages/ManagingOversupply.aspx; CAISO, *Production and Curtailments Data—Monthly*, http://www.caiso.com/Style%20Library/caiso/csv/curtailmentsMonthly.csv.

239 Author's calculation from CAISO, *Production and Curtailments Data—2021* (last visited Aug. 29, 2022), http://www.caiso.com/Documents/ProductionAndCurtailmentsData_2021.xlsx. There were 15,675 five-minute intervals in 2021 where curtailment for solar and wind were >= 200 MW. Since there are 105,120 five-minute intervals in a year, that is equivalent to just under 15%.

240 *See* Rui Shan & Yaojin Sun, *Bitcoin Mining to Reduce the Renewable Curtailment: A Case Study of CAISO*, at 6 Fig. 3 (Aug. 7, 2019), http://dx.doi.org/10.2139/ssrn.3436872.

241 *See generally* Square Bitcoin Clean Energy Initiative, *Bitcoin is Key to an Abundant, Clean Energy Future* (Apr. 2021) https://assets.ctfassets.net/2d5q1td6cyxq/5mRjc9X5LTXFFihlITt7QK/e7bcba47217b60423a01a357e036105e/BCEI_White_Paper.pdf; Sean Stein Smith, *Crypto Power Usage Is Helping To Spur Renewable Energy Investments*, Forbes (June 5, 2022), https://www.forbes.com/sites/seansteinsmith/2022/06/05/crypto-power-usage-is-helping-to-spur-renewable-energy-investments/?sh=64dc7eef2cb6; Brady Dale, *Industry argues how bitcoin drives demand for renewables*, Axios (May 24, 2022), https://www.axios.com/2022/05/24/crypto-bitcoin-mining-industry-demand-for-energy-renewables; Ariana Garcia, *The Texas grid can survive a boom in cryptocurrency mining—but for how long?* Houston Chronicle (Nov. 1, 2021), https://www.chron.com/politics/article/texas-power-grid-crypto-mining-16572771.php.

242 Square Bitcoin Clean Energy Initiative, *Bitcoin is Key to an Abundant, Clean Energy Future* (Apr. 2021) https://assets.ctfassets.net/2d5q1td6cyxq/5mRjc9X5LTXFFihlITt7QK/e7bcba47217b60423a01a357e036105e/BCEI_White_Paper.pdf.

243 Compute North, *Compute North Begins Energization of 280MW TIER 0™ Data Center Colocated on West Texas Wind Farm* (Aug. 8, 2022), https://www.computenorth.com/news_release/compute-north-begins-energization-of-280mw-tier-0-data-center-co-located-on-west-texas-wind-farm/.

244 Marathon Digital Holdings, *Form 10-Q, Quarterly Report* (June 30, 2022), https://ir.marathondh.com/sec-filings/all-sec-filings/content/0001493152-22-021799/form10-q.htm.

245 U.S. EIA, *Form 860. 2021 Early Release. File 3_2_Wind_Y2021_Early_Release.* https://www.eia.gov/electricity/data/eia860/xls/eia8602021ER.zip.

246 Texas Blockchain Council, *Bitcoin Mining* (last visited Aug. 29, 2022), https://texasblockchaincouncil.org/bitcoin-mining.

247 Lancium Balancing Energy, Lancium Breaks Ground On First Clean Campus In Fort Stockton, Texas (Sept. 15, 2021), https://lancium.com/press-release/lancium-breaks-ground-on-first-clean-campus-in-fort-stockton-texas/.

248 Robert Walton, *Texas Expands Industrial Demand Response Program As Grid Goes to the Brink of Rolling Outages*, Utility Dive (July 15, 2022), https://www.utilitydive.com/news/texas-expands-industrial-demand-response-program-as-grid-goes-to-the-brink/627358/.

249 Robert Walton, *Bitcoin mining as a grid resource? 'It's complicated."*, Utility Dive (Feb. 17, 2022), https://www.utilitydive.com/news/bitcoin-mining-as-a-grid-resource-its-complicated/617896/.

250 U.S. EIA, *Reserve electric generating capacity helps keep the lights on* (June 1, 2012), https://www.eia.gov/todayinenergy/detail.php?id=6510.

251 U.S. Dep't of Energy, *Demand Response*, https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/demand-response.

252 Ironically, in touting their extreme flexibility to load interruptions, proof-of-work currency miners are acknowledging the limited benefits of their operations—only the company's Bitcoin accretion rate, and therefore profit margin, notices the interruption.

253 ERCOT issued "conservation appeals" to Texas ratepayers and business on July 10, 2022 and July 13, 2022 –along with a statement on May 13, 2022, to calm anxiety by Texans of blackouts during unseasonably hot weather during the month of May. *See* ERCOT, *ERCOT Issues Conservation Appeal to Texans and Texas Businesses* (July 10, 2022), https://www.ercot.com/news/release?id=90030206-5cf5-db8e-13d1-f8fe2bd0128f; ERCOT, *REVISED: ERCOT Issues Conservation Appeal to Texans and Businesses* (July 13, 2022), https://www.ercot.com/news/release?id=f91df9ae-7a4d-5148-36b1-d7bd1f0f5bb4; ERCOT, *Statement by Electric Reliability Council of Texas Interim CEO, Brad Jones on current grid conditions* (May 13, 2022), https://www.ercot.com/news/release?id=8b772e9e-51d0-4c3c-e653-1e5079f28e89.

254 David Pan, *Bitcoin Miner Made Millions in Credits by Shutting Rigs During Texas Heat*, Bloomberg (Aug. 3, 2022), https://www.bloomberg.com/news/articles/2022-08-03/bitcoin-miner-made-millions-by-shutting-rigs-during-texas-heat.

255 Riot Blockchain, *Riot Blockchain Announces July 2022 Production and Operations Updates* (Aug. 3, 2022), https://www.riotblockchain.com/news-media/press-releases/detail/135/riot-blockchain-announces-july-20.

256 Eamon Barrett, *Texas Bitcoin Miners Are Getting Paid To Shut Down and Give Electricity Back to the Power Grid*, Fortune (July 12, 2022), https://fortune.com/2022/07/12/texas-bitcoin-miners-paid-shut-down-power-grid-electricity-blackout-heat/.

257 *See, e.g.*, MacKenzie Sigalos, *Bitcoin miners say they're helping to fix the broken Texas energy grid — and Ted Cruz agrees*, CNBC (Dec. 5, 2021), https://www.cnbc.com/2021/12/04/bitcoin-miners-say-theyre-fixing-texas-electric-grid-ted-cruz-agrees.html ("Miners commit to buying a certain amount of power, and either use it for mining if the grid doesn't need it, or sell it back at a profit if the grid demands it."); Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid ("Upgrades to the power system will be needed because the grid 'can't handle all of this new load,' said Evan Caron, a former power trader in Austin who invests in energy technology. New investments in the transmission system are typically shared among Ercot's consumers and show up in their utility bills."); Chris Tomlinson, *Crypto could raise Texas electric prices if not planned well*, Houston Chronicle (Apr. 15, 2022), https://www.houstonchronicle.com/business/columnists/tomlinson/article/Crypto-could-raise-Texas-electricity-prices-if-17081552.php ("Crypto-miners often brag they can shut down in five seconds if the grid needs the power, but rising cryptocurrency values make voluntarily 'saving the grid' less attractive. Miners are enrolling in ERCOT programs where they are paid to shut down, creating an additional cost."); Sabrina Toppa, *In Texas, an Influx of Crypto Miners May Mean Higher Elec. Bills for Consumers*, The Street (Mar. 16, 2022), https://www.thestreet.com/crypto/news/in-texas-the-influx-of-crypto-miners-may-mean-higher-electricity-bills (explaining that "upgrades to the local electricity grid may soon involve an increase in electricity fees for consumers across the Lone Star state"); Karin Rives, *Crypto mining industry's greening campaign raises new questions*, S&P Global (May 4, 2022), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/crypto-mining-industry-s-greening-campaign-raises-new-questions-69679254 ("concerns are growing that the industry could be using too much of the state's wind capacity and could drive up power prices for homes and businesses."); *see also* Ariana Garcia, *The Texas grid can survive a boom in cryptocurrency mining—but for how long?* Houston Chronicle (Nov. 1, 2021), https://www.chron.com/politics/article/texas-power-grid-crypto-mining-16572771.php.

258 Robert Walton, *Conservative approach to Texas grid operations could cost consumers $1.5B this year, says market monitor*, Utility Dive (June 24, 2022), https://www.utilitydive.com/news/texas-grid-ercot-market-monitor-consumers-puc/626018/.

259 Severin Borenstein, *Crypto Mining for a More Stable Grid?* Energy Inst. at Haas (Mar. 21, 2022) (emphasis added), https://energyathaas.wordpress.com/2022/03/21/crypto-mining-for-a-more-stable-grid/.

260 Bitcoin Mining Council, *Global Bitcoin Mining Data Review: Q2 2022*, at Slide 8 (July 2022), https://bitcoinminingcouncil.com/wp-content/uploads/2022/07/2022.07.19-BMC-Presentation-Q2-22-Presentation.pdf ("Bitcoin mining energy use is only 0.15% when compared to the world's total energy."). The figures used in this comparison are misleading because they compare Bitcoin energy against all other consumptive energy purposes, including electricity, transportation and shipping, industry, heating, cooling, agriculture, and cooking. According to the Bitcoin Mining Council, Bitcoin already consumes 253 billion kWh, or 1% of global electricity production, Bitcoin Mining Council, *Global Bitcoin Mining Data Review* at 6; *see* U.S. EIA, *International Data World Electricity* (last visited Aug. 29, 2022), https://www.eia.gov/international/data/world/electricity/electricity-generation.

261 Andrew R. Chow, *Fact-Checking 8 Claims About Crypto's Climate Impact*, Time Magazine (July 1, 2022), https://time.com/6193004/crypto-climate-impact-facts/.

262 George Kamiya, *Data Centres and Data Transmission Networks*, International Energy Agency (Nov. 2021), https://www.iea.org/reports/data-centres-and-data-transmission-networks.

263 Joshua Aslan *et al.*, *Electricity Intensity of Internet Data Transmission: Untangling the Estimates*, 22(4) J. of Indus. Ecology 785 (2017), https://onlinelibrary.wiley.com/doi/10.1111/jiec.12630; Albrecht Fehske *et al.*, *The global footprint of mobile communications: The ecological and economic perspective*, 49(8) IEEE Commc'n Mag., at 55-62 (Aug. 2011), https://ieeexplore.ieee.org/document/5978416.

264 Neel Dhanesha, *The daunting task of making cryptocurrency climate-friendly*, Vox (Apr. 18, 2022) ("There hasn't been any time in the history of bitcoin where increasing machine efficiency led to less energy consumption," said Alex de Vries, founder of the website Digiconomist, which tracks the sustainability of cryptocurrencies."), https://www.vox.com/recode/23005493/cryptocurrency-bitcoin-climate-friendly. Further, standard energy efficiency requirements will not be sufficient. As the value of mining rewards has increased, more sophisticated mining equipment has developed. *See, e.g.*, Namcios, *News Intel Launches New Bitcoin Mining Chip, Blockscale*, Bitcoin Magazine (Apr. 4, 2022), https://bitcoinmagazine.com/business/intel-launches-new-bitcoin-mining-chip-blockscale.

265 Rachel Rybarczyk *et al.*, *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question*, Galaxy Digital, at 8, 13 (May 2021), https://docsend.com/view/adwmdeeyfvqwecj2.

266 Alex de Vries, *Renewable Energy Will Not Solve Bitcoin's Sustainability Problem*, 3(4) Joule 893 (Apr. 2019), https://www.sciencedirect.com/science/article/pii/S254243511930087X.

267 Raynor de Best, *Bitcoin average energy consumption per transaction compared to that of VISA as of April 25, 2022*, Statista (Apr. 25, 2022), https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/. In fact, the latest data from Statista finds that 1 Bitcoin transaction is equal to 2,188.59 kWh of energy, whereas 100,000 VISA transactions account for 148.63. By this estimate, 1 Bitcoin transaction could actually account for 1.47 million VISA transactions (2,188.59 / 148.63 = 14.72 * 100,000 = 1.47 million).

268 These recommendations do not include the wholesale move away from proof-of-work cryptocurrencies, which would reduce electricity consumption from cryptocurrencies tremendously.

269 David Morley, *Zoning for Data Centers and Cryptocurrency Mining*, Am. Planning Ass'n (Jun. 2022), https://www.planning.org/publications/document/9249180/.

270 *See, e.g.*, Chelan Cnty., WA. Pub. Util. Dist., *Cryptocurrency Zoning & Planning Discussion — UPDATE*, https://www.chelanpud.org/docs/default-source/commission/outreach-on-cryptocurrency.pdf; Missoula Cnty., MT, *Cryptocurrency Mining Zoning Regulations* (Feb. 2021), https://www.missoulacounty.us/home/showpublisheddocument/72870/637460579331670000; Josh Blaschke, *Brenham Planning and Zoning to Consider Prohibiting Commercial Crypto Mining at Homes*, KWHI (Mar. 28, 2022), https://kwhi.com/2022/03/28/brenham-planning-and-zoning-to-consider-prohibiting-commercial-crypto-mining-at-homes/; Becky Long, *No Commercial Crypto Mining Allowed*, Clay County Progress (Aug. 4, 2022), https://www.claycountyprogress.com/local/no-commercial-crypto-mining-allowed; Robert C. Peck *et al.*, *Ordinance Prohibiting Cryptocurrency Mining Industries from Operating in Clay County* (Aug. 4, 2022) https://www.clayconc.com/_files/ugd/fe4bcd_163aefda66f243cfb4f8c41bd27ebce5.pdf; *Local Law, Cryptocurrency and Data Mining, Village of Rouses Point, NY*, https://ecode360.com/RO0588/laws/LF1301408.pdf; *Plattsburgh cryptocurrency regulations unveiled*, Sun Community News (Oct. 12, 2018), https://suncommunitynews.com/news/67515/plattsburgh-cryptocurrency-regulations-unveiled/; Rick Pfeiffer, *Council Approves High Energy Use Zoning Code Changes*, Niagara Gazette (July 5, 2022), https://www.niagara-gazette.com/news/local_news/council-approves-high-energy-use-zoning-code-changes/article_0e52c27e-fccd-11ec-a5e9-2fedad86de16.html; Andrew Sullivan, *Lansing Pursues Zoning Changes to Prohibit Crypto Mining*, Ithaca.com (Feb. 10, 2022), https://www.ithaca.com/news/lansing/lansing-pursues-zoning-changes-to-prohibit-crypto-mining/article_0105f92e-89c3-11ec-a7bd-f3306528469b.html.

Attachment B

Responses by Local Advocates and Public Interest Organizations to OSTP RFI on the Energy and Climate Implications of Digital Assets (May 2022)

May 9, 2022

VIA ELECTRONIC SUBMISSION
Office of Science & Technology Policy
Eisenhower Executive Office Building
[redacted]

Re: The Energy and Climate Implications of Digital Assets

Thank you for the opportunity to provide comments on the Request for Information ("RFI") on the Energy and Climate Implications of Digital Assets. 87 Fed. Reg. 17,105 (Mar. 25, 2022). Please accept these national comments on behalf of the undersigned organizations.

Overview

Our organizations are grateful for the Biden Administration's commitment to combatting the climate crisis and addressing the detrimental impacts of digital currency on electricity use and climate pollution.[1] Digital currencies that rely on "proof-of-work" to validate transactions undermine your efforts to promote energy efficiency and to reduce climate pollution and will instead use more and more electricity and generate more and more climate pollution. As the Intergovernmental Panel on Climate Change ("IPCC") warned in April, digital currencies like Bitcoin are likely to "be a major global source of CO2 if the electricity production is not decarbonised."[2]

Unlike vehicles or manufacturers subject to energy efficiency standards or pollution limits, miners of digital currencies that rely upon proof-of-work are not required to use energy more efficiently or to power their mining operations with renewable energy and have little incentive to do so. Instead, miners can and increasingly do rely upon fossil fuel energy sources to generate and use more and more electricity. Digital currencies like Bitcoin also generate significant amounts of electronic waste and are contributing to supply-chain challenges in the semiconductor industry.

We urge you to use the Administration's regulatory tools to curb the electricity use and climate pollution associated with digital currencies that rely on "proof-of-work" and to work with legislators to address the energy and climate impacts of digital currencies. In particular, we urge you to subject permits related to cryptocurrency mining to stringent environmental reviews, to create a registry of mining operations, to set energy efficiency standards for digital currencies, to establish power density limits, and to limit financial transactions which increase climate pollution, interrupt critical supply chains, or limit the availability and affordability of electricity for essential industries.

Bitcoin's Growing Use of Electricity

Soaring electricity use by some digital currencies is a "**growing concern**," according to the IPCC.[3] Using powerful computers to solve complex puzzles to generate new cryptocurrency is called "**proof-of-work**."[4] Once puzzles are solved, new cryptocurrency coins are added to the blockchain. Deploying powerful computers to solve complex puzzles uses growing amounts of electricity.[5]

Although electricity use can be difficult to measure, experts at the University of Cambridge estimate that Bitcoin mining consumes 153.67 terawatt hours ("TWh") per year—which is more electricity than what is used by countries like Sweden and Poland, and more electricity than Americans use to power our lights and televisions.[6] In the six weeks since the Biden Administration issued this Request for Information, the annual estimated electricity use associated with Bitcoin has increased by 12 TWh.

Bitcoin's Use of Electricity is Growing Faster than Comparable Sectors

Between 2017 and 2022, electricity demand for Bitcoin increased from 7 TWh in April 2017 to 151.2 TWh in April of 2022—a 20-fold increase in just five years.[7] If this trend continues over the next five years, Bitcoin could use as much electricity as Japan and India combined. By contrast, during the same period, electricity demand by comparable sectors has not increased and, in some cases, even declined.[8]

For example, electricity demand by data centers has not increased, even though internet traffic and data center workloads have increased significantly.[9] In sharp contrast to Bitcoin, data transmission networks and mobile communications networks are rapidly becoming more energy efficient.[10]

Bitcoin already uses half as much electricity as the entire global banking sector, according to one estimate, and will overtake the banking sector within two years if current trends continue.[11] One study estimates that the average electricity footprint of non-cash transactions by the global banking system is no more than 0.4 kWh, while the average electricity footprint per Bitcoin transaction ranges from 491.4 kWh to 765.4 kWh.[12] By some estimates, a single Bitcoin transaction uses more energy than 100,000 Visa transactions.[13]

Bitcoin's Growing Climate Pollution

U.S.-based Bitcoin miners are already responsible for one quarter of the global greenhouse gas emissions caused by Bitcoin mining.[14] Although miners use a variety of power sources to provide electricity for their computers, mining for cryptocurrencies like Bitcoin results in far more greenhouse emissions than validation methods employed by other digital currencies. The electricity used to mine Bitcoin in 2020 resulted in almost **60 million tons** of carbon dioxide emissions, according to one estimate.[15] The carbon dioxide emissions from mining Ethereum and Bitcoin in 2021 equaled the tailpipe emissions of more than 15 million gas-powered cars.[16]

Other Digital Currencies Use Less Electricity and Produce Less Climate Pollution

Currently, Bitcoin uses two-thirds of all the energy consumed by cryptocurrencies.[17] Other digital currencies use less electricity and produce less climate pollution than digital currencies like Bitcoin. For example, cryptocurrencies using "proof-of-stake" generally require **far less electricity** than those using proof of work.[18] The energy consumed per transaction is "two-to-three orders of magnitude" lower than that of Bitcoin, or an amount similar to the energy consumption of VisaNet.[19] Another analysis found proof of stake uses 75% less energy than proof-of-work, and Ethereum estimates that moving from proof-of-work to proof-of-stake will reduce the electricity use of their digital currency by 99.95%.[20]

Expected Increase in Electricity Use and Climate Pollution

As the price of cryptocurrency increases, the incentive to use more and more powerful computers grows—as does the amount of electricity these computers consume. The development of mining "pools" has created an "arms race" that has significantly increased electricity consumption.[21] As computing power increases, the Bitcoin protocol adjusts to make the puzzle more difficult to solve—using more and more electricity.[22] Increasing demand for electricity is a feature of Bitcoin, not a bug. Indeed, the Bitcoin protocol is "energy-intensive" by design.[23] As Bitcoin prices increase and Bitcoin puzzles become harder to solve, electricity use will increase.

Increased Cryptocurrency Mining Threatens Critical Supply Chains

A global shortage of semiconductor chips, or integrated circuits, has impacted more than 100 industries, including the electric vehicle industry. A contributing factor has been Bitcoin miners replacing earlier mining hardware with an application-specific integrated circuit ("ASIC") to improve speed and efficiency.

Demand for ASICs is expected to grow substantially in the next few years, compounding shortages in semiconductor chips and potentially offsetting efforts to boost domestic production of semiconductor chips.[24]

Proof-of-work Cryptocurrency Mining Harms Local Communities

By increasing electricity use and providing an incentive to extend the life of fossil fuel sources of energy, Bitcoin miners are increasing climate pollution and electricity prices—harming local communities.[25] Mining operations in upstate New York increased electric bills by about $165 million for small businesses and $79 million for individuals.[26]

Examples include:

- at least two waste-coal plants in Pennsylvania that have sharply increased capacity, local air and water pollution,[27] and greenhouse gas emissions since they were bought by a private equity fund in 2021;
- a coal-fired power plant in Montana that had previously filed for bankruptcy and was barely operating and then began operating and polluting full-time;[28]
- two gas-fired power plants in upstate New York that powered up rarely – only in heat waves and cold snaps;[29]
- mining powered by a grid that is nearly 70% coal-powered in Kentucky;[30]
- and orphaned gas wells in South Dakota.[31]

On the western shores of Seneca Lake, among the productive vineyards and farms of the Finger Lakes, is the Greenidge Generation Station. In its first year of mining operations, Greenidge operated seven fold more than the year prior and its CO_2 emissions increased 479%.[32] In addition, significant amounts of extremely hot water are now discharged from the plant, and the plant is permitted to discharge 134 million gallons of water daily into Seneca Lake at temperatures of up to 108 degrees Fahrenheit.[33] This thermal pollution endangers health and wildlife habitability, including but not limited to potential harmful algal blooms, fish deaths, migration and loss of biodiversity, oxygen depletion, direct thermal shock, and changes in dissolved oxygen.

A similar story can be told about the Big Horn Data Hub operated by Marathon Digital Holdings, a publicly traded cryptomining company, at the Hardin Coal Plant in Hardin, Montana, where in 2021, compared to the prior year, NOx emissions increased 842%, SO_2 emissions increased 508%, and CO_2 emissions increased 850%.[34] Because coal plants spew toxic air pollution and coal ash contamination, the neighboring Crow Indian Reservation is most disproportionately impacted by local environmental issues.[35]

The former Mayor of Plattsburgh New York commented: "… the automated nature of these servers meant that the new mines provided few local jobs."[36] And as one of the authors of a Berkeley Hass study similarly observed: "These are warehouses full of computers and they only require one or two IT people to run the whole operation, so it's unlikely that it brings jobs or stimulates the economy."[37]

Proof-of-work Cryptocurrency Mining Will Not Accelerate Transition to Renewable Energy

Experts **agree** that Bitcoin will not aid the transition to renewable electricity.[38] Cryptomining requires a steady source of power, so miners are seeking cheap sources of electricity generated by burning coal and natural gas. Unless renewable electricity like wind and solar is paired with large-scale battery storage, renewables are not an attractive option for miners. Actual use of renewable energy by Bitcoin miners has fallen in recent years, according to one estimate.[39]

More importantly, there is no way to ensure that cryptocurrencies that use proof-of-work will switch to clean energy. Unlike industries subject to pollution or energy efficiency standards, electricity use by miners and their climate pollution are not subject to state or federal limits. In addition, there is little incentive for proof-of-work cryptocurrency miners to reduce their electricity use. Voluntary, unenforceable "accords" are not binding on individual miners and rely on unverifiable and hard-to-measure offsets.[40]

Proof-of-work Cryptocurrency Mining Generates Significant Electronic Waste

Digital currencies like Bitcoin generate significant amounts of electronic waste. In 2021, Bitcoin generated more than 30,000 metric tons of electronic waste,[41] which is comparable to the e-waste produced by the whole country of the Netherlands.[42] The mining devices used for proof-of-work quickly go obsolete, often lasting less than two years, and recent changes in the hardware used by miners has made the generation of e-waste more likely.[43] The e-waste generated from proof-of-work mining is significant, and experts predict it will continue to increase as proof-of-work mining operations increase in scale.[44] Much of this waste is sent to low-income communities around the world who bear the harms of this toxic waste.[45]

*** * * * * * * ***

Due to the harmful climate and energy externalities from proof-of-work mining, we propose the following ideas for consideration as potential mitigation strategies to be further explored.

EPA Must Subject Proof-of-work Cryptocurrency Mining Permits to Stringent Reviews

We urge the Biden Environmental Protection Agency ("EPA") to institute stringent reviews of every air and water permit issued or renewed for any proof-of-work mining operations. The Clean Air Act, as well as state climate and environmental review laws, contains provisions for the EPA to deny permits or modify permits to institute severe constraints on air and water pollution from proof-of-work cryptocurrency mining operations in order to protect local communities.[46]

We urge the EPA to institute rules and regulations to mitigate the harms of cryptocurrency mining e-waste disposal in large quantities. We also urge the EPA to review its powers under the Noise Control Act of 1972 and the Quiet Communities Act of 1978 to protect the public health and welfare, by setting insulation requirements to mitigate the enormous noise pollution generated by the hundreds to thousands of mining rigs set up at each location.[47]

OMB Must Create a Registry for Proof-of-work Cryptocurrency Mining Operations

We encourage the Office of Management and Budget's Office of Information and Regulatory Affairs to create a registry for proof-of-work mining operations over a certain threshold. Determining which sites have begun proof-of-work mining is difficult to ascertain, whether it be at a power plant, connecting to the grid, at a fracked gas wellhead, or otherwise. Many of the most noxious mining operations can operate as-of-right under preexisting and permissive air and water permits or zoning regulations, despite the change in operations and the negative impacts to local residents and the climate.

A registry would allow for transparency to help with the public commenting processes and can inform other agencies' work. It could also inform the Federal Energy Regulatory Commission and/or the Regional Transmission Organizations and Independent System Operators, as well as utilities that may need to serve that additional power load to better plan and prevent or mitigate the potential strain such operations will place on the grid.[48] For example, the Electric Reliability Council of Texas ("ERCOT") recently required new large cryptocurrency miners to seek permission to connect to the state's power and required utilities to submit studies on the impact of miners and other large users on the grid because it all could not be tracked.[49] One important component of this would be to ensure that operations that mine cryptocurrency disclose their energy sources and quantities, with specificity. Many cryptocurrency mining operations advertise the use of renewable energy to mine, without detailing the source or amount of the energy used.

DOE Must Set Energy Efficiency Standards for Proof-of-work Cryptocurrency Miners

We encourage the Department of Energy ("DOE") to study how to implement or make recommendations on how best to institute reforms for high-density-load businesses like proof-of-work crypto miners. In particular, we encourage the DOE to study how to implement or make recommendations on how best to institute energy efficiency limits based on kilowatt-hour ("kWh") per transaction or block. A minimum energy efficiency limit set around a kWh per transaction or block could ensure that the methodology to mine blockchain/cryptocurrency is the best available technology and uses the least amount of energy. The efficiency limit should tighten over time to eventually eliminate proof-of-work mining.[50]

We also encourage the DOE to study how to implement or make recommendations on how best to institute power density limits, based on the number of kilowatts of energy consumption or load per thousand square feet. A power density limit could be set at an initial limit and tightened over time to allow existing operations to adjust operations over time to mitigate their impacts. We further encourage the DOE to study how to implement or make recommendations on how best to institute reforms such as increasing System Benefit Charge surcharges or adjusting Renewable Energy Credit purchase requirements for any proof-of-work mining operations that have added more than, for example, a certain megawatt hour per year load.

Finally, we encourage the DOE to study how to implement or make recommendations on how best to protect low-cost public power allocations to be siphoned to proof-of-work mining operations at the expense of local ratepayers.

Financial Regulators Must Act to Address Climate Pollution and Economic Impacts of Bitcoin

Financial regulators should use existing tools under the Securities Exchange Act, the Commodity Exchange Act, and the Federal Trade Act to require greater transparency regarding electricity use and climate pollution, to place limits on the environment limits posed by these digital assets; to combat misleading claims regarding the environmental impacts of digital currencies; and to address the serious risks Bitcoin poses to supply chains and electricity prices and availability.

We agree that digital currencies like Bitcoin are securities and commodities subject to jurisdiction of the Securities & Exchange Commission ("SEC") and Commodity Futures Trading Commission ("CFTC"), and that digital currencies like Bitcoin are subject to the greenhouse gas reporting requirements recently announced by the SEC.[51] The CFTC should also take steps to require greater reporting,[52] and the SEC and the CFTC should use the CFTC's broad power to address the impacts of Bitcoin on critical supply chains and electricity prices.[53] In particular, both the SEC and CFTC[54] have statutory authority over listing standards for registered securities exchanges and commodity futures exchanges. Finally, the Federal Trade Commission should take steps to limit unfair or deceptive claims related to the climate impacts of digital currencies.

In particular, the SEC and CFTC should use listing standards for registered securities exchanges to require digital assets to meet environmental and electricity standards, such as limits on the amount of electricity that can be used for mining. While Bitcoin requires hundreds of kilowatt hours of energy per transaction, some digital assets require less than 1 kilowatt hour.[55] Requiring registered exchanges only to list digital assets whose transactions consume electricity below a certain energy-efficient standard would drive innovation or a transition to other methods of validation.

* * * * * * *

Thank you for the opportunity to provide these comments.

Sincerely,

Environmental Working Group	Earthjustice	Greenpeace
League of Conservation Voters	Sierra Club	Friends of the Earth
Seneca Lake Guardian	Milwaukee Riverkeeper	

[1] Exec. Order No. 14067, 87 Fed. Reg. 14,143 (Mar. 9, 2022).

[2] IPCC, Working Group III Contribution to the IPCC Sixth Assessment Report (AR6), Chapter I, at 1-26 (2022), https://report.ipcc.ch/ar6wg3/pdf/IPCC_AR6_WGIII_FinalDraft_FullReport.pdf (citing Camilo Mora et al., 2018: Bitcoin emissions alone could push global warming above 2°C, 8(11) Nat. Clim. Chang. 931 (2018), doi:10.1038/s41558-018-0321-8).

[3] IPCC, Working Group III Contribution to the IPCC Sixth Assessment Report (AR6), Chapter 5, at 5-57–5-58 (2022), https://report.ipcc.ch/ar6wg3/pdf/IPCC_AR6_WGIII_FinalDraft_FullReport.pdf.

[4] Coinbase, *What is "proof of work" or "proof of stake"?*, https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake?utm_source=google_search_nb&utm_medium=cpc&utm_campaign=9943088770&utm_content=127915792732&utm_term=&utm_creative=580583551399&utm_device=c&utm_placement=&utm_network=g&utm_location=9016855&gclid=CjwKCAjwxOCRBhA8EiwA0X8hizjdQWUC0lYoK4I2qwuuqKannuPGiZopNiaJy6SWsPSItfqmEInxghoCm1AQAvD_BwE (last visited May 4, 2022).

[5] Laurie Clarke, *How do we solve bitcoin's carbon problem?*, The Guardian (Jan. 30, 2022), https://www.theguardian.com/technology/2022/jan/30/how-do-we-solve-bitcoins-carbon-problem.

[6] Cambridge Centre for Alternative Finance, *Cambridge Bitcoin Electricity Consumption Index*, at 'Comparisons' page, https://ccaf.io/cbeci/index/methodology (last visited May 4, 2022).

[7] *Id.*

[8] Hass McCook, *A critical assessment of the Bitcoin mining industry, gold production industry, the legacy banking system, and the production of physical currency* (July 15, 2014), https://bitcoin.fr/public/divers/docs/Estimation_de_la_durabilite_et_du_cout_du_reseau_Bitcoin.pdf.

[9] George Kamiya, *Data Centres and Data Transmission Networks*, International Energy Agency (Nov. 2021), https://www.iea.org/reports/data-centres-and-data-transmission-networks.

[10] Joshua Aslan et al., Electricity Intensity of Internet Data Transmission: Untangling the Estimates, 22(4) J. of Indus. Ecology 785 (2017), https://onlinelibrary.wiley.com/doi/10.1111/jiec.12630; Albrecht Fehske et al., The global footprint of mobile communications: The ecological and economic perspective, 49(8) IEEE Commc'n Mag. 55 (2011), https://ieeexplore.ieee.org/document/5978416.

[11] Rachel Rybarczyk, Drew Armstrong & Amanda Fabiano, *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question*, Galaxy Digital (May 2021), https://docsend.com/view/adwmdeeyfvqwecj2; *see also* Cambridge Centre for Alternative Finance, *Cambridge Bitcoin Electricity Consumption Index*, https://ccaf.io/cbeci/index/methodology (last visited May 4, 2022).

[12] Alex de Vries, Renewable Energy Will Not Solve Bitcoin's Sustainability Problem, 3(4) Joule 893 (Apr. 2019), https://www.sciencedirect.com/science/article/pii/S254243511930087X.

[13] Statista, Bitcoin average energy consumption per transaction compared to that of VISA as of April 25, 2022, https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/. In fact, the latest data from Statista finds that 1 Bitcoin transaction is equal to 2,188.59 kWh of energy, whereas 100,000 VISA transactions account for 148.63. By this estimate, 1 Bitcoin transaction could actually account for 1.47 million VISA transactions (2,188.59 / 148.63 = 14.72 * 100,000 = 1.47 million).

[14] Alex de Vries et al., *Revisiting Bitcoin's carbon footprint*, 6(3) Joule 498 (2022), https://www.sciencedirect.com/science/article/abs/pii/S2542435122000861.

[15] ForexSuggest.com, *Global Impact of Crypto Trading*, https://forexsuggest.com/global-impact-of-crypto-trading/.

[16] Committee on Energy & Commerce, Memorandum, at 5 (Jan. 17, 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Briefing%20Memo_OI%20Hearing_2022.01.20.pdf (citing Forex Suggest, *Global Impact of Crypto Trading*, forexsuggest.com/global-impact-ofcrypto-trading/ (accessed Jan. 10, 2022);EPA, Greenhouse Gas Emissions from a Typical Passenger Vehicle (Mar. 2018), www.epa.gov/greenvehicles/greenhouse-gas-emissions-typicalpassenger-vehicle).

[17] Ulrich Gallersdorfer et al., Energy Consumption of Cryptocurrencies Beyond Bitcoin, 4 Joule 1839, 1843 (2020), https://www.sciencedirect.com/science/article/pii/S2542435120303317.

[18] ForexSuggest.com, *Global Impact of Crypto Trading*, https://forexsuggest.com/global-impact-of-crypto-trading/.

[19] Moritz Platt et al., The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work, at 5 (Apr. 4, 2022), https://arxiv.org/pdf/2109.03667.pdf.

[20] Rong Zhang & Wai Kin, Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake, at 5–6, J. Phys.: Conf. Ser. (2020), https://www.researchgate.net/publication/343011650_Evaluation_of_Energy_Consumption_in_BlockChains_with_Proof_of_Work_and_Proof_of_Stake/link/5f13fc814585151299a6effd/download; Carl Beekhuizen, *Ethereum's energy usage will soon decrease by ~99.95%*, ethereum foundation blog (May 18, 2021), https://blog.ethereum.org/2021/05/18/country-power-no-more/.

[21] Lin William Cong, Zhiguo He & Jiasun Li, Decentralized Mining in Centralized Pools, at 3, 4, National Bureau of Economic Research ("NBER"), Working Paper 25592 (Feb. 2019), https://www.nber.org/papers/w25592. An estimated 60% of mining is controlled by the top 4 companies that own the mining pools. BTC.com, *Pool Distribution*, https://btc.com/stats/pool (last visited May 5, 2022). NBER found that the top 10% of cryptominers control 90% of mining and just 0.1% (about 50 miners) control close to 50% of all mining. Igor Makarov & Antoinette Schoar, Blockchain Analysis of the Bitcoin Market, NBER, Working Paper 29396 (Oct. 2021), https://www.nber.org/papers/w29396; *see also* Emily Graffeo, *Bitcoin Is Still Concentrated in a Few Hands, Study Finds*, TIME (Oct. 25, 2021), https://time.com/6110392/bitcoin-ownership/; Paul Vigna, *Bitcoin's 'One Percent' Controls Lion's Share of the Cryptocurrency's Wealth*, The Wall Street Journal ("WSJ") (Dec. 20, 2021), https://www.wsj.com/articles/bitcoins-one-percent-controls-lions-share-of-the-cryptocurrencys-wealth-11639996204; https://www ft.com/content/4f8044bf-8f0f-46b4-9fb7-6d0eba723017; Khristopher J. Brooks, *Bitcoin has its own 1% who control outsized share of wealth*, CBS News (Dec. 21, 2021), https://www.cbsnews.com/news/bitcoin-cryptocurrency-wealth-one-percent/; Gregory Zuckerman, *Mainstream Hedge Funds Pour Billions of Dollars Into Crypto*, WSJ (Mar. 9, 2022), https://www.wsj.com/articles/mainstream-hedge-funds-pour-billions-of-dollars-into-crypto-11646808223.

[22] "To keep the average time for solving a puzzle constant…the difficulty of the cryptographic puzzles is periodically adapted to the total computing power of the network." Johannes Sedlmeir et al., The Energy Consumption of Blockchain Technology: Beyond Myth, 62(6) Bus. Inf. Syst. Eng. 599, 602 (2020), https://link.springer.com/content/pdf/10.1007/s12599-020-00656-x.pdf.

[23] *Id.* at 601.

[24] MarketWatch, *Global ASIC Miners Market Size 2022 Industry Development Plans, Emerging Demand, Industry Share, Leading Players Strategy, Trends, Demands, Drivers and Growth Opportunity Outlook till 2028* (Apr. 8, 2022), https://www marketwatch.com/press-release/global-asic-miners-market-size-2022-industry-development-plans-emerging-demand-industry-share-leading-players-strategy-trends-demands-drivers-and-growth-opportunity-outlook-till-2028-2022-04-28#:~:text=The%20ASIC%20Miners%20market%20is,be%20worth%20millions%20of%20dollars.

[25] *See* Ken Cook, *The local environmental disasters that inconvenience bitcoin's apologists*, Environmental Working Group (Apr. 11, 2022), https://www.ewg.org/news-insights/news/2022/04/local-environmental-disasters-inconvenience-bitcoins-apologists.

[26] Matteo Benetton, Giovanni Compiani & Adair Morse, When cryptomining comes to town: High electricity-use spillovers to the local economy, at 1,4, SSRN (Feb. 17, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720.

[27] *See* the Letter submitted by PennFuture, et al. (May 2, 2022).

[28] *See* the Letter submitted by the Montana Environmental Information Center, et al. (May 9, 2022).

[29] *See* the Letter submitted by Seneca Lake Guardian, et al. (May 9, 2022).

[30] *See* the Letter submitted by the Kentucky Conservation Committee, et al. (May 9, 2022).

[31] Seth Tupper, *Orphaned South Dakota gas wells could soon power bitcoin mining*, South Dakota Public Broadcasting (Feb. 24, 2021), https://www.sdpb.org/blogs/politics-public-policy/orphaned-south-dakota-gas-wells-could-soon-power-bitcoin-mining/.

[32] The year before Greenidge changed the operations at the plant to begin mining.

[33] N.Y. State Dep't of Env't Conservation, Water Withdrawal Permit, DEC Permit No. 8-5736-00004/00015 (effective 09/11/2017), https://treichlerlawoffice.com/water/greenidge/WaterPermit_Final_2017-09-11_.pdf; Seneca Lake Guardian, Facts Matter: Greenidge Bitcoin Mining Expansion (Mar. 10, 2021), https://senecalakeguardian.org/Facts-Matter-Greenidge-Bitcoin-Mining.

[34] *See* the Letter submitted by the Montana Environmental Information Center *et al.*, at Table "Hardin Generating Station Operational and Emissions Data from 2017 to 2021" (May 9, 2022) (Data from EPA's Air Markets Program Database, https://ampd.epa.gov/ampd/).

[35] Kayla Desroches, *As crypto company departs Hardin, what's next for the communities it leaves behind?*, Yellowstone Public Radio (Apr. 28. 2022), https://www.ypradio.org/energy/2022-04-28/as-crypto-company-departs-hardin-whats-next-for-the-communities-it-leaves-behind; *see generally* Letter submitted by the Montana Environmental Information Center *et al.* re the Climate & Energy Impacts of Digital Assets in Montana (May 9, 2022). In early April 2022, Marathon Digital announced that it would transition its operation at Hardin to other locations. However, Marathon's CEO stated that the company is leaving the Big Horn Data Hub and millions of dollars' worth of infrastructure intact, "so another miner can come in right behind us with a minimal delay and then com[e] up to speed[.]" Tom Lutey, *Crypto miner plans to exit Hardin coal-fired power plant*, Billings Gazette (Apr. 6, 2022), https://billingsgazette.com/news/crypto-miner-plans-to-exit-hardin-coal-fired-power-plant/article_cd2ca444-929a-511d-913d-903fbc570498 html.

[36] Lois Parshley, *How Bitcoin mining devastated this New York town: Between rising electricity rates and soaring climate costs, cryptomining is taking its toll on communities.* MIT Technology Review, (Apr. 18, 2022), https://www.technologyreview.com/2022/04/18/1049331/bitcoin-cryptocurrency-cryptomining-new-york/ (last visited May 6, 2022).

[37] Laura Counts, *Power-hungry cryptominers push up electricity costs for locals*, Berkeley Haas (Aug. 3, 2020), https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-locals/ (quoting Asst. Prof. Giovanni Compiani, University of Chicago's Booth School of Business); Matteo Benetton, Giovanni Compiani & Adair Morse, *When cryptomining comes to town: High electricity-use spillovers to the local economy*, at 1,4, SSRN (Feb. 17, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720.

[38] *See* Alex de Vries, *Renewable Energy Will Not Solve Bitcoin's Sustainability Problem*, 3 Joule 891 (2019), https://www.cell.com/joule/pdf/S2542-4351(19)30087-X.pdf.

[39] Alex de Vries et al., Revisiting Bitcoin's carbon footprint, 6(3) Joule 498 (2022), https://www.sciencedirect.com/science/article/abs/pii/S2542435122000861.

[40] *See* Crypto Climate Accord, *Make Crypto Green*, https://cryptoclimate.org/ (last visited May 5, 2022).

[41] Alex de Vries & Christian Stoll, *Bitcoin's growing e-waste problem*, 175 Res., Conservation and Recycling 105901 (Dec. 2021), https://www.sciencedirect.com/science/article/abs/pii/S0921344921005103?dgcid=author.

[42] BBC, *Bitcoin mining produces tons of waste* (Sept. 20, 2021), https://www.bbc.com/news/technology-58572385; Alex de Vries & Christian Stoll, *Bitcoin's growing e-waste problem*, 175 Res., Conservation & Recycling 105901 (Dec. 2021), https://www.sciencedirect.com/science/article/pii/S0921344921005103; Digiconomist, *Bitcoin Elec. Waste Monitor*, https://digiconomist net/Bitcoin-electronic-waste-monitor/ (last visited May 5, 2022).

[43] Joachim Klement, *Geo-Economics: The Interplay between Geopolitics, Econ., and Investments*, at 200 (Apr. 2021); Mark Peplow, *Bitcoin poses major electronic-waste problem*, Chem. & Eng'g News (Mar. 14, 2019), https://cen.acs.org/environment/sustainability/Bitcoin-poses-major-electronic-waste/97/i11; The Econ. Times, *Bitcoin mining generates tonnes of e-waste: Study* (Sept. 21, 2021), https://economictimes.indiatimes.com/markets/cryptocurrency/bitcoin-mining-generates-tonnes-of-e-waste-study/articleshow/86391133.cms.

[44] Mark Peplow, *Bitcoin poses major electronic-waste problem*, Chem. & Eng'g News (Mar. 14, 2019), https://cen.acs.org/environment/sustainability/Bitcoin-poses-major-electronic-waste/97/i11.

[45] Peter Howson & Alex de Vries, *Preying on the poor? Opportunities and challenges for tackling the social and env't threats of cryptocurrencies for vulnerable and low-income communities*, 84 Energy Rsch. & Soc. Sci. 102394 (2022), https://www.sciencedirect.com/science/article/abs/pii/S2214629621004813.

[46] Comments from Seneca Lake Guardian, The Comm. to Preserve the Finger Lakes, Fossil Free Tompkins, Sierra Club, and Earthjustice in Opposition to the Draft Title V Air Permit for Greenidge Generating Station, located at 590 Plant Road, Dresden, New York 14441 (Permit ID: 8-5736-00004/00017) (Nov. 19, 2021), https://earthjustice.org/sites/default/files/files/2021-11-19_slg-cpfl-fft-sc-ej-comments-to-dec.pdf.

[47] Vipal Monga, *Bitcoin Mining Noise Drives Neighbors Nuts—a Giant Dentist Drill That Won't Stop*, The Wall Street J. (Nov. 12, 2021), https://www.wsj.com/articles/bitcoin-mining-noise-drives-neighbors-nuts-giant-dentist-drill-that-wont-stop-11636730904.

[48] For example, the Electric Reliability Council of Texas ("ERCOT") estimates that proof-of-work crypto mining alone will account for 6 several GWs of new demand over the next two years. Naureen S. Malik, *Crypto Miners' Elec. Use in Texas Would Equal Another Houston*, Bloomberg (Apr. 27, 2022) ("About 17 gigawatts worth of crypto miners have inquired about plugging into Texas's grid, according to Brad Jones, ERCOT's interim chief executive officer. 'That's about the equivalent of load of two-and-a-half New York Cities….'"), https://www.bloomberg.com/news/articles/2022-04-27/crypto-miners-in-texas-will-need-more-power-than-houston; Borenstein, Severin, *Crypto Mining for a More Stable Grid?*, U.C. Berkeley Energy Inst. Blog (Mar. 21, 2022), https://energyathaas.wordpress.com/2022/03/21/crypto-mining-for-a-more-stable-grid/.

[49] Naureen S Malik, *Crypto Miners in Texas Need 'Approval to Energize' in New Grid Hurdle*, Bloomberg (Mar. 30, 2022), https://www.bloomberg.com/news/articles/2022-03-30/texas-crypto-miners-need-approval-to-energize-in-grid-hurdle.

[50] Standard energy efficiency requirements will not be sufficient. As the value of mining rewards has increased, more sophisticated mining equipment has developed. *See, e.g.*, Namcios, *News Intel Launches New Bitcoin Mining Chip, Blockscale*, Bitcoin Magazine (Apr. 4, 2022), https://bitcoinmagazine.com/business/intel-launches-new-bitcoin-mining-chip-blockscale. While ASICs are more powerful and energy efficient than the hardware previously used for cryptocurrency mining, the efficiency gains have not resulted in decreased overall energy consumption because of the substantially increased scale of mining. Neel Dhanesha, *The daunting task of making cryptocurrency climate-friendly*, Vox (Apr. 18, 2022) ("There hasn't been any time in the history of bitcoin where increasing machine efficiency led to less energy consumption," said Alex de Vries, founder of the website Digiconomist, which tracks the sustainability of cryptocurrencies."), https://www.vox.com/recode/23005493/cryptocurrency-bitcoin-climate-friendly.

[51] 17 C.F.R. § 210, 229, 232, 239, and 249 (2022), https://www.sec.gov/rules/proposed/2022/33-11042.pdf.

[52] Todd Phillips, *A Climate and Competition Agenda for the Commodity Futures Trading Commission*, CAP (Feb. 1, 2022), https://www.americanprogress.org/article/a-climate-and-competition-agenda-for-the-commodity-futures-trading-commission/.

[53] 7 U.S.C. § 2 (2015).

[54] Todd Phillips, *The SEC's Regulatory Role in the Digital Asset Markets*, CAP (Oct. 4, 2021), https://www.americanprogress.org/article/secs-regulatory-role-digital-asset-markets/.

[55] Kimberly Gedeon, *The most energy-efficient cryptocurrencies — Tesla's top picks to replace Bitcoin*, Laptop (May 31, 2021), https://www.laptopmag.com/best-picks/most-energy-efficient-cryptocurrencies-the-best-picks-for-teslas-new-coin.

Robert Altenburg
Senior Director for Energy and Climate
Citizens for Pennsylvania's Future
[redacted]

Alondra Nelson, Acting Director
Office of Science and Technology Policy
White House
[redacted]

May 2, 2022

RE: RFI Response: Climate Implications of Digital Assets

Dear Acting Director Nelson,

We, the undersigned organizations share an interest in protecting public health, the environment, and responding to the growing climate crisis. While we take no position on the use of digital currencies and blockchain technology in general, we view the outrageously high energy demand of mining Bitcoin and related Nakamoto-style proof-of-work cryptocurrencies as a significant threat to developing a sustainable energy economy and reaching the necessary climate goals. As such, we appreciate the opportunity to respond to Office of Science and Technology's request for information[1] and urge policymakers to explore all the avenues at their disposal to control the expansion of this wasteful process.

Issue #1, Protocols: *Proof-of-work consensus is incompatible with a sustainable energy economy.*

As of this writing, the Cambridge Bitcoin Energy Consumption Index[2] estimates the bitcoin network is consuming 15.6 GW. At that rate, the network will consume 416 MWh for each bitcoin that is created. That is approximately the same amount of electricity the average Pennsylvania household consumes in 40 years.

While we do not endorse any specific alternate technology or approach, we note that non-proof-of-work blockchain systems have been successfully operating for nearly ten years[3] and, in many cases, alternate systems offer more capabilities than the bitcoin blockchain while having far lower energy demand.

---

[1] OSTP RFI on the Energy and Climate Implications of Digital Assets, 87 Fed Reg 17105 (Mar. 25, 2022).
[2] Cambridge Bitcoin Energy Consumption Index (*available at: https://ccaf.io/cbeci/index).*
[3] Peercoin implemented a proof-of-stake system in 2012.

Issue #2 Hardware: *Proof-of-work cryptomining hardware cannot be considered energy efficient*

Policymakers must be aware of attempts by Bitcoin advocates to distract from criticism of Bitcoin's enormous energy demand with red herring arguments. One example raised at a recent Congressional hearing[4] was the claim that because the Application Specific Integrated Circuits (ASICs) used for cryptomining are highly optimized for hashing blocks of data, they are more efficient—or less energy intensive—than general-purpose computers used in conventional datacenters.

While an ASIC may be the least energy intensive tool available to calculate more than 100 trillion hashes in one second, that cannot be considered an efficient process if an alternate methodology exists that avoids the need to calculate trillions of hashes in the first place. In much the same way, using a single enormous mining truck may be the best way to move 400 tons of dirt, but if the same results can be achieved without moving dirt at all, the efficiency of the truck is illusory.

We also note that ASIC hardware has an extremely limited useful life before it becomes obsolete e-waste. Hardware that was introduced just two years is often impossible to operate profitably and even newer hardware may be replaced and discarded in favor of newer and more competitive equipment.

At a time when semiconductor shortages are contributing to higher consumer prices, this wasteful hardware cycle to proliferate is a particularly bad policy choice that disproportionately impacts low- and moderate-income families.

Issue #3 Resources: *Bitcoin is driving increased consumption in Pennsylvania*

Bitcoin operations are growing in Pennsylvania with the assistance of significant subsidies, lax regulation, and legislators who are not concerned with the energy and environmental impacts.

Waste coal

In July of 2021 a company by the name of Stronghold Digital Mining (Stronghold) filed an S-1 report with the Securities and Exchange Commission (SEC) disclosing plans to purchase three waste coal fired power plants and install 57,000 Application Specific Integrated Circuits (ASICs) dedicated to mining bitcoin. To date, Stronghold has purchased the 94-megawatt (MW) circulating fluidized bed (CFB) Scrubgrass power plant in Venango County and the 94 MW Panther Creek CFB facility in Carbon County and has plans to purchase a third facility bringing their total generating capacity to 300MW.[5] As of March 24, 2022, the company operated approximately 20,500 pieces of mining hardware and purchase agreements in place for an additional 29,400 miners.

---

[4] U.S. House Committee on Energy and Commerce Hearing, Cleaning Up Cryptocurrency: The Energy Impacts of Bitcoin, (Jan. 20, 2022).

[5] Stronghold Digital Mining, SEC Form 10-k, (filed Mar. 29, 2022).

Waste coal is a low-energy-value product that, before environmental restrictions were passed, was often dumped in piles near mining sites. Pennsylvania has approximately 840 such sites and operators such as Stronghold claim that burning it for energy is environmentally beneficial because it encourages the removal of these piles, and the waste ash can be used for fill and reclamation projects. Despite these claims, burning waste coal results in the emissions of significant amounts of air pollution including ozone precursors, fine particulates, acid gasses, heavy metals, and vast amounts of carbon pollution. The impacts of increased air pollution should not be ignored—particularly at these sites since the Scrubgrass plant is located within ten miles of a designated Environmental Justice area and the Panther Creek plant is within three miles of such an area.

Burning a low-energy-value fuel source also requires subsidies to be profitable and the state legislature has provided significant incentives to burn polluting waste coal. This includes $4/MWh from the Coal Refuse Reclamation tax credit and a claimed $16/MWh from the Tier II Alternative Energy Portfolio Standard Program. Altogether, Stronghold has claimed 60 percent of their generation costs will be covered by subsidies from taxpayers and ratepayers.[6]

Fracked gas

In January of 2022, inspectors from the Pennsylvania Department of Environmental Protection (DEP) found 30 methane-gas-fired generators with an estimated capacity of more than 10MW at the Hegarty A well operated by Big Dog Energy, LLC and located in Clearfield County, PA within two miles of a designated Environmental Justice area. These generators were installed without authorization from the DEP in violation of Pennsylvania regulations and the resulting energy was being used to mine bitcoin.

While the DEP issued a Notice of Violation (NOV) for this operation[7], it is unknown how many of Pennsylvania's many thousands of methane gas well are hosting similar mining projects. Big Dog Energy alone has 38 other active well permits across Pennsylvania.[8]

In addition to Big Dog Energy, there are media reports that another company, Pin Oak Energy, has purchased a midstream gathering system capable of 25,000 MMBtu/day. Given available ASIC mining hardware, that could represent fifteen to twenty thousand miners, and again, there are questions as to whether the required air quality permits have been obtained.[9]

Possibly related to this situation, a co-sponsorship memorandum has been circulated in the Pennsylvania Senate in which the sponsor expresses concern that "entrepreneurs of these emerging technologies leaving Pennsylvania for other states with less burdensome regulation" if

---

[6] Stronghold Digital Mining, SEC Form S-1, (filed Jul. 27, 2021).
[7] PA DEP, Notice of Violation to Big Dog Energy, LLC., (Jan. 7, 2022).
[8] PA DEP, eFacts information system (*available at: https://www.ahs.dep.pa.gov/eFACTSWeb/default.aspx/default.aspx*)
[9] B. Stockman, PA DEP Looking into Pin Oak Bitcoin Mine in Ridgeway Township, Ridgeway Record (Mar. 21, 2022) (*available at: https://www.ridgwayrecord.com/news/pa-dep-looking-into-pin-oak-bitcoin-mine-in-ridgway-township/article_5713036c-b136-11ec-bb37-2f666479782b.html).*

his bill does not pass.[10] This signals an attempt by the legislature to further weaken environmental protections.

Nuclear

In August of 2021, Talen Energy Corp. announced a joint venture with TeraWulf Inc. that would result in the construction of the 180MW Nautilus Cryptomine bitcoin mining facility adjacent to the Susquehanna nuclear power generating station in Columbia County, Pennsylvania.[11] It has since been reported that this facility will benefit from significant state subsidies in the form of Pennsylvania's datacenter tax exemption.[12]

While claims are made that this will use carbon-free nuclear generation, we reject any suggestion that this is environmentally neutral. In 2020, nuclear generation was responsible for more than 33 percent of Pennsylvania's energy generation and represented more than 92 percent of the carbon free energy generated. Diverting carbon free energy to wasteful Bitcoin mining virtually guarantees that demand will be backfilled with fossil resources.

Given Pennsylvania's grid mix, operation of 180MW operation could result in over one million tons of additional carbon pollution per year, in addition to thousands of tons of NOx and other dangerous air pollutants.

Issue #4: Economics: *Bitcoin mining operations are likely to raise consumer energy prices.*

It appears that most of the large Bitcoin mining operations in Pennsylvania are operating behind the meter and not drawing power from the wholesale power grid, but that does not mean these operations are not impacting the grid.

To the extent that miners are using electricity that would otherwise flow to the grid, that energy would, by definition, have been priced below PJM's market clearing price. By diverting that energy into wasteful Bitcoin mining, the energy markets will clear at a higher price. These increases in wholesale prices may ultimately be absorbed by consumers.

The claim that miners could provide a service to the grid as a source of interruptible load is highly suspect. Given current Bitcoin prices and network conditions, miners using competitive hardware can gross more than $200 per MWh. According to PJM's Market Monitor[13], average monthly wholesale prices in 2021 never exceeded $92/MWh and averaged considerably less. That suggests that situations where miners would voluntarily curtail their demand because of price concerns would be exceedingly rare. On the contrary, this makes it very likely that Bitcoin mining operations could be the marginal demand that sets an elevated price for the rest of the grid.

---

[10] Sen. Langerholc, Co-sponsorship Memorandum, Emerging Technologies Permitting Oversight, (Mar. 15, 2022)
[11] Press Release, *Talen Energy Corp. announces Bitcoin Mining Joint Venture with TeraWulf Inc.* (Aug. 3, 2021)
[12] Caruso, S., *Pa. passed a tax break for data centers. Now crypto-miners are taking advantage*, Penn-Capital Star, (Mar. 13, 2022).
[13] Monitoring Analytics, Components of PJM Price, 2021, (April 12, 2022) (*available at: https://www.monitoringanalytics.com/data/pjm_price.shtml).*

In addition to raising electricity prices, there are indications that diverting methane gas to bitcoin mining can be more profitable than selling the gas for other purposes such as residential heating. This would not only further raise consumer prices; it also may negatively impact reliability of our municipal gas systems.

Issue #5: Past or Ongoing Mitigation:

In Pennsylvania, we have seen no significant efforts at the state level to limit energy demand and pollution from Bitcoin mining operations. On the contrary, we often find miners benefiting from state subsidies that were designed for other purposes and may see new legislation specifically designed to incentivize wasteful mining.

Issue #6: Potential Energy or Climate Benefits: *We categorically reject the idea that wasting energy on Bitcoin mining operations is environmentally beneficial.*

Bitcoin mining and flared methane gas

A recent claim noted that using methane gas for mining Bitcoin is a "better" choice than flaring it, but that is a strawman argument. An even better choice is investing in energy efficiency, electrification, and clean renewable generation, so we avoid the emissions and risk associated with extracting the fossil fuels in the first place.

The next logical question is why is there such an excess of flared gas? The 2016 New Source Performance Standards (NSPS)[14] for oil and gas require that many wells utilize reduced emissions completions where gas is either captured and used for some productive purpose or reinjected. Those same standards will also often require low-bleed pneumatic controllers or other technology that further reduces the amount of potentially vented gas. Where flaring is allowed, this tends to be for a limited time and only for a limited number of wells.

Before claiming proof-of-work mining is a solution, we should first be sure the problem is well understood. That any remaining flared methane gas could be used for Bitcoin mining at all requires that the capture and use of the gas be technically feasible and that enough gas is available to make investment in capture economical. The question then is why is it not already being captured? This suggests that regulators are allowing oil and gas operators to opt-out capturing the gas for financial reasons. Such exemption forces the citizens to absorb the risk and damage from the polluting industry and acts as a subsidy for pollution. If polluting industries were, instead, required to internalize the costs of their waste, perhaps flaring would be less of a problem.

Bitcoin mining and clean energy

A similar strawman argument is to claim that mining Bitcoin could "absorb wasted clean energy." Again, this assumes that the only option is waste and Bitcoin mining is a viable alternative—neither is likely true.

[14] *See:* 40 CFR 60.5360 *et seq*. (*published:* 81 Fed. Reg. 35824 (Jun. 3, 2016))

In certain scenarios, energy markets have shown a “duck curve” where high solar generation has driven prices very low—sometimes even negative—for short periods in the mid-day period before ramping up sharply later in the day. This can be addressed in different ways, including increased investment in transmission allowing power to be wheeled to where there is demand, and increased storage allowing the excess energy to be used later.

It's unlikely Bitcoin will do anything to alleviate this issue. First, one of the reasons Bitcoin miners gravitate to more expensive fossil fuels rather than clean renewable generation is because 24/7 operations at high-capacity factors is more profitable. This is driven both by the nature of proof-of-work mining pools where increased hash rates directly translate to increased profits. (Other factors include the relatively short competitive life of ASIC hardware and the extreme market volatility.) It is highly unlikely that miners will invest a significant amount of money in mining hardware and let it sit idle until the energy grid “needs” their load.

It's far more likely that these mining operations will burn fossil fuels for energy to support their 24/7 operations and only curtail that generation and buy from the grid when price signals favor doing so. While there may be rare cases when this might keep grid prices from going negative, that will come at a significant cost. In normal operation, the marginal cost of the Bitcoin miner’s behind-the-meter generation will become a floor price for the market and have the effect of raising average wholesale prices for everyone while continuing polluting combustion.

Issue #7: Likely Future Developments:

As noted above, Pennsylvania is already seeing methane gas fired generators being installed directly at well sites. Our calculations indicate that these facilities could see significantly more revenue that would be obtained selling the gas on the wholesale market. Assuming such development is not prevented by regulators, this would be expected to raise wholesale prices for methane gas. As Pennsylvanian’s currently rely on gas for 53% of their electricity generation and a significant portion of their home heating, this could result in significant consumer impacts in addition to the added pollution. Considering methane is 86 times more potent a greenhouse gas than carbon dioxide over a 20-year period, any leakage from these operations would be particularly dangerous for our climate.

Burning waste coal to generate electricity for bitcoin mining is one of the worst choices available. According to EIA data[15], Pennsylvania’s waste-coal fired power plants had average CO2 emissions of over 2,760 pounds per megawatt-hour making them the second most carbon-intensive fuel behind residual fuel oil. This effect is compounded because facilities used to mine Bitcoin are operating at significantly higher capacity factors than plants suppling energy to the grid and Pennsylvania has nine other such facility where mining could expand.

Issue #8: Implications for U.S. Policy:

[15] US EIA, Emissions by Plant and Region, 2020 (*available at: https://www.eia.gov/electricity/data/emissions/)*

Between the Bitcoin mining operations announced by Stronghold Digital Mining and the carbon free nuclear generation that could be diverted from the grid for the TeraWulf operation, Pennsylvania could easily see more than three million tons of excess carbon pollution each year. In addition, we can expect to see more ozone precursors, fine particulates, heavy metals, and acid gasses—many of these being emitted in or near environmental justice areas. Since any new mining operations will likely make this situation worse, our focus must be on reducing these emissions and reaching net zero carbon by 2050.

Thank you,

Robert Altenburg,
Senior Director for Energy and Climate
Citizens for Pennsylvania's Future
(PennFuture)
[redacted]

Joseph Minott
Executive Director and Chief Counsel
Clean Air Counsel
[redacted]

The Rev. Mitchell C. Hescox
President/C.E.O.
The Evangelical Environmental Network
[redacted]

Devin McDougall
Mandy DeRoche
Nick Thorpe
Earthjustice
[redacted]

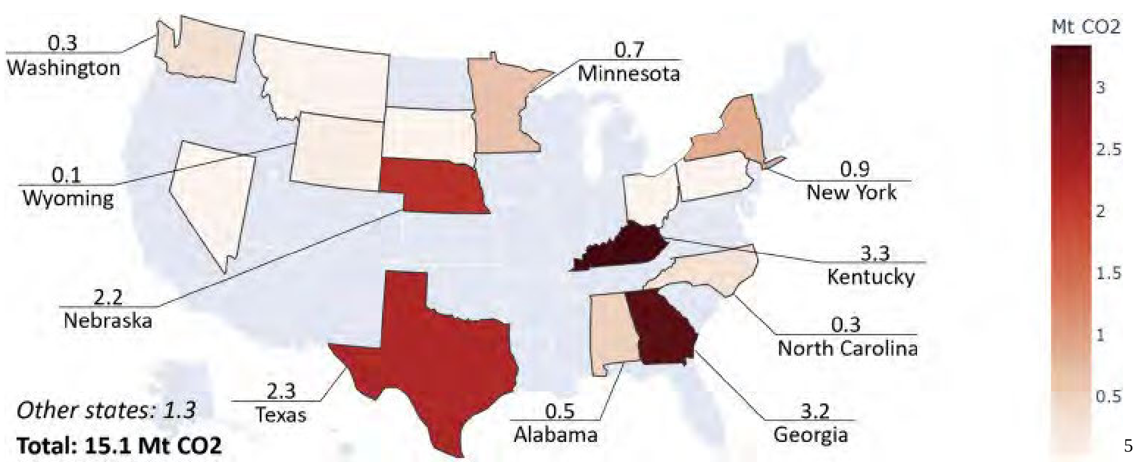
May 9, 2022

VIA ELECTRONIC SUBMISSION
Office of Science & Technology Policy
[redacted]

Re: Energy and Climate Implications of Digital Assets in Kentucky

Thank you for the opportunity to provide comments in response to the Request for Information ("RFI") regarding the Energy and Climate Implications of Digital Assets (87 Fed. Reg. 17105) from the Kentucky Conservation Committee, the Kentucky Resources Council, Appalachian Citizens' Law Center, Inc., Kentucky Equal Justice Center, Kentucky Interfaith Power and Light, Progress Kentucky, LLC, Nina and Mickey McCoy, and Earthjustice concerning the health and climate impacts posed by the enormous amount of energy that is powering proof-of-work cryptocurrency mining in Kentucky.

Kentucky is home to nearly 20% of the collective computing power of the country's proof-of-work cryptocurrency mining operations.[1] Kentucky produces more carbon dioxide pollution from cryptocurrency mining than any other U.S. state,[2] and has the second highest carbon intensity for crypto mining of any state.[3] As the map below shows, the State's carbon footprint from cryptocurrency mining is estimated at 3.3 megatons of carbon dioxide per year.[4]



[1] MacKenzie Sigalos, *New York and Texas are winning the war to attract bitcoin miners*, CNBC: Crypto Decoded (Oct. 9, 2021), https://www.cnbc.com/2021/10/09/war-to-attract-bitcoin-miners-pits-texas-against-new-york-kentucky.html (reporting that 18.7% of U.S.'s mining computing power in 2021 was located in Kentucky).

[2] Avi Asher-Schapiro, *Coal to crypto: The gold rush bringing bitcoin miners to Kentucky*, Thomson Reuters Foundation (Mar. 14, 2022), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate ("Coal to Crypto") (citing Alex de Vries *et al.*, *Revisiting Bitcoin's carbon footprint*, 6 Joule, 498, 500-01 (Feb. 25, 2022), https://www.sciencedirect.com/science/article/abs/pii/S2542435122000861?dgcid=author.

[3] Karin Rives, *Crypto mining industry's greening campaign raises new questions*, S&P Global (May 4, 2022), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/crypto-mining-industry-s-greening-campaign-raises-new-questions-69679254.

[4] Alex de Vries *et al.*, *Revisiting Bitcoin's carbon footprint*, 6 Joule, 498, Figure 3 at n.2.

[5] Estimated carbon footprint of the Bitcoin network in the United States, as of August 2021. *Id.*

While Kentucky residents must bear with the noise pollution, air pollution, water pollution, and increased electricity rates from cryptocurrency mining, the profits do not remain in Kentucky. As a recent article examining the impacts of cryptocurrency mining in Kentucky described, "[s]ome see echoes of what they say were the worst elements of the now largely defunct coal industry: out-of-state money, absentee owners, and huge fortunes made with little wealth trickling down to local communities."[6] Despite this, the Kentucky state government, in a race to the bottom, has offered enormous tax incentives to this new industry, which have been estimated to cost Kentucky taxpayers about $9 million a year in lost tax revenue, despite the few local jobs and the profits flowing out-of-state to increasingly centralized mining operations owners.[7] These tax incentives include "tax exemptions totaling 9 percent on electricity consumed at larger cryptocurrency mining operations, . . . sales-tax refunds on mining equipment, as well as potential incentives on income taxes and wage assessments."[8] The Kentucky Center for Economic Policy recently argued that incentivizing the industry so heavily is a poor use of government funds because among other reasons it creates little local work.[9] For example, the Blockware Mining operation in Paducah described below is estimated to provide just 10 full-time jobs in its initial phase.[10]

Lack of reliable and specific information on proof-of-work mining operations

Unfortunately, there is very little transparency in this developing industry, and many operations can operate as of right under existing laws, regulations, and permits with no additional oversight. For example, the Blockware Mining site described below has begun operating at Industrial Park West in Paducah, but a search of publicly available records through the websites of both the Kentucky Energy & Environment Cabinet and the U.S. EPA does not identify any environmental permits that have been applied for at that site.[11] Because existing laws, regulations, and/or permits mostly do not require that mining operations make this information available to any government agency or the public, it is notoriously difficult to discover how much a particular entity is mining at a location, how many miners it has running, how much energy it is using, or even an operation's fuel source. Without accurate information, it is nearly impossible for communities, local groups, and interested residents to understand the operations and how it will impact our communities. What little we do know seems troubling in terms of air pollution, energy use, and rate impacts on local residents.

---

[6] Asher-Schapiro, *Coal to crypto*.

[7] *Id. See also* Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market*, 4 Nat'l Bureau of Econ. Rsch., Working Paper No. 29396 (2021), https://www.nber.org/system/files/working_papers/w29396/w29396.pdf (the top 10% of cryptominers control 90% of mining and just 0.1% (about 50 miners) control close 50% of the mining).

[8] Bill Estep, *Kentucky's digital gold rush. What's behind the crypto mining boom in coal country?,* Lexington Herald Leader (Apr. 21, 2022), https://www.kentucky.com/news/state/kentucky/article259880855.html.

[9] Asher-Schapiro, *Coal to crypto*.

[10] *See* Order at 12, *In re: Elec. Tariff Filing of Big Rivers Elec. Corp. & Jackson Purchase Energy Corp.*, Case No. 2021-00282 (Ky. P.S.C. Oct. 14, 2021).

[11] *See, e.g.*, Ky. Dep't of Env't Prot., *Industrial Park W*, http://dep.gateway.ky.gov/eSearch/Search_AI_Detail.aspx?AgencyID=15885 (listing no licensed operators and no permits for the site); EPA: Enforcement & Compliance History Online, *Facility Search Results*, https://echo.epa.gov/facilities/facility-search/results (no listing for Blockware Mining site in Paducah, Ky.).

Proof-of-work mining operations generating their own power

One proof-of-work cryptocurrency mining operation owned by a company named Blockware Mining is located in Paducah, Kentucky. There are at least 8,000 ASIC miners as of June 2021 operating there and perhaps as many as 10,000 by 2023.[12] The company plans to add thousands of additional machines,[13] and it has stated that it "wants to power 100 megawatts of electricity to its site, an amount that could power tens of thousands of homes," which is in fact approximately the same amount as the peak electricity consumption of the town of Paducah in 2021.[14]

Different sources of information report that the operations in Paducah are powered by hydro, wind, nuclear, and/or coal and are also drawing electricity from the grid via the Big Rivers Electric Corporation.[15] For example, the Kentucky Public Service Commission recently approved a contract with Blockware Mining under an Economic Development Rate,[16] where the customer gets a 90% credit on their demand charge for incremental load above a certain minimum base level. For Blockware Mining, the credit will last until 2031 and is contingent on the company maintaining and adding to its load over time, giving Blockware Mining the incentive to keep growing through at least 2031 using electricity from a state grid that is 70% coal-based as of today.[17]

In addition, there is proof-of-work cryptocurrency mining at a reclaimed surface coal mine in Inez, Kentucky in Martin County. The company plans to build a waste-to-energy incinerator to burn and gasify municipal waste trucked in from outside the community.[18] Instead of that waste-to-energy incinerator powering 1,000 nearby homes, it will divert that power to the proof-of-work cryptocurrency mining operations on or adjacent to the site.[19]

There are also an unknown number of "gas to crypto" operations in Kentucky, in which methane gas generators powering mining rigs are hooked up directly to gas wells. A recent article recently demonstrated that some of these operations are truly off-the-map. The author visited a "small installation, miles from the nearest paved road, [that] draws methane gas from a long abandoned well that [the miner]

---

[12] Liam Niemeyer & Katie Myers, *A new kind of 'mining' has arrived in the Ohio Valley. What will crypto mean for the region?* (Apr. 25, 2022), https://ohiovalleyresource.org/2022/04/25/a-new-kind-of-mining-has-arrived-in-the-ohio-valley-what-will-crypto-mean-for-the-region/.

[13] Bill Estep, *Kentucky's digital gold rush. What's behind the crypto mining boom in coal country?*, Lexington Herald Leader (Apr. 21, 2022), https://www.kentucky.com/news/state/kentucky/article259880855.html.

[14] Liam Niemeyer & Katie Myers, *A new kind of 'mining' has arrived in the Ohio Valley. What will crypto mean for the region?* (Apr. 25, 2022), https://ohiovalleyresource.org/2022/04/25/a-new-kind-of-mining-has-arrived-in-the-ohio-valley-what-will-crypto-mean-for-the-region/.

[15] Cheyenne Ligon, *Blockware Raises $25M to Expand Bitcoin Mining Operations in Kentucky*, CoinDesk (June 30, 2021), https://www.coindesk.com/business/2021/06/30/blockware-raises-25m-to-expand-bitcoin-mining-operations-in-kentucky/; Asher-Schapiro, *Coal to crypto*; Blockware Mining, *Operations*, https://www.blockwaremining.io/mining (last visited May 5, 2022).

[16] Order at 21-23, *In re: Elec. Tariff Filing of Big Rivers Elec. Corp. & Jackson Purchase Energy Corp.*, Case No. 2021-00282 (Ky. P.S.C. Oct. 14, 2021).

[17] U.S. Energy Information Administration, *Kentucky: State Profile and Energy Estimates*, https://www.eia.gov/state/?sid=KY (last visited May 5, 2022); Asher-Schapiro, *Coal to crypto*.

[18] *See* Inez Power LLC, PowerPoint Presentation (July 9, 2019), https://apps.legislature.ky.gov/CommitteeDocuments/262/11966/Jul%209%202019%20Inez%20Power%20PowerPoint.pdf.

[19] Asher-Schapiro, *Coal to crypto*.

has fixed up with a generator and satellite internet . . . ."[20] One Kentucky company, Midstream Enterprises, advertises a "[t]urn-key crypto mining data array and generator tailored for natural gas producers."[21] The company also states that it hosts its own data centers "power[ed] . . . with our own natural gas wells."[22] Details about the company's operations (including their size, number of locations, emissions, etc.) do not appear to be publicly available, nor does the company appear to have applied for any environmental permits for these activities.[23] Midstream's Chief Operating Officer, Marshall Holbrook, claims that he is "3rd generation oil&gas" and was "one of the first (if not THE first) person to mine cryptocurrency in the US."[24] In a video on the company's website, Holbrook claims he has been mining Bitcoin off of natural gas for six years.[25] There are untold greenhouse gas emissions from these off-grid fracked-gas mining wells. Another concern is the resurrection of orphaned wells that were planned to be plugged or capped to prevent methane and carbon pollution, to crypto-mine instead.[26]

Proof-of-work mining operations that consume power from the grid

Most proof-of-work cryptocurrency mining operations in Kentucky do not generate their own power, but draw on the state's carbon-intensive grid.[27] In 2020, about 70% of Kentucky's power came from burning coal, according to government data.[28] Coal-powered electricity has numerous and severe health impacts from air and water pollution and is an enormous driver of greenhouse gas pollution.

One of the mining operations is run by Blockware Solutions (a different company than Blockware Mining) in Belfry, Kentucky, located at an abandoned coal-washing plant using up to 75 MW of electricity from the grid, more power than all the houses in Belfry combined, based on estimates from the

---

[20] *Id.*

[21] *See* midstream, *midstream's Post*, Linkedin, https://www.linkedin.com/posts/midstream-enterprises-inc%2E_midstream-bitcoin-miningbitcoin-activity-6845779138238930944-NmBd?utm_source=linkedin_share&utm_medium=member_desktop_web (last visited May 5, 2022); *see also* midstream, *solutions: Big Rig 2.0*, https://www.midstream.co/big-rig?hsLang=en-us (last visited May 5, 2022).

[22] midstream, *About us*, Linkedin, https://www.linkedin.com/company/midstream-enterprises-inc./about/ (last visited May 5, 2022).

[23] Based on searches done through http://dep.gateway.ky.gov/eSearch/Search_AI.aspx and https://echo.epa.gov/. Among other things, the "Big Rigs" operated by Midstream should be regulated as stationary sources under the Clean Air Act, to the extent any of their emissions exceed permitting thresholds – but it is unclear whether the company has sought any such permits (to the extent they are required) or the Kentucky Energy & Environment Cabinet has reviewed any of these operations to determine whether permits are required.

[24] midstream, *meet the team: marshall holbrook*, https://www.midstream.co/team (last visited May 5, 2022).

[25] *See* Video: midstream, *home: Why Partner With Us* at 00:48, https://www.midstream.co/ (last visited May 5, 2022).

[26] *See, e.g.*, Seth Tupper, *Orphaned South Dakota Gas Wells Could Soon Power Bitcoin Mining*, South Dakota Public Broadcasting (Feb. 24, 2021), https://listen.sdpb.org/business/2021-02-24/orphaned-south-dakota-gas-wells-could-soon-power-bitcoin-mining.

[27] Asher-Schapiro, *Coal to crypto*.

[28] U.S. Energy Information Administration, *Kentucky: State Profile and Energy Estimates*, https://www.eia.gov/state/?sid=KY (last visited May 5, 2022); Asher-Schapiro, *Coal to crypto*.

company.[29] The company recently reported that it has plans to expand further and have 24,000 mining machines running at the site by the end of 2022.[30]

Again, definitive data is hard to come by, but there also appear to be two proof-of-work cryptocurrency mining operations in Calvert City, Kentucky. One known as the Calvert Data Center is located at a former steel rolling mill and operated by Core Scientific, which will consume 125 MW of electricity from the grid to mine.[31] The second is a proof-of-work mining operation at a former steel plant operated by CC Metals & Alloys.[32] CC Metals & Alloys "is only one of around five major crypto mining operations in the region" but it is unclear the extent of the operations.[33] There are also at least two mining operations in Kentucky operated by Compass Mining but their fuel source and energy consumption is unknown.[34]

Proof-of-work mining operations strain the electrical grid and do not incentivize renewable energy

Proof-of-work cryptocurrency mining operations drawing energy from the grid are placing a mostly-unplanned-for load on already-strained grids across the country. Some experts have warned that there will be "risks to public power utilities unless they are sufficiently mitigated."[35]

In many states, the new additional loads on the grid - in the hundreds to thousands of MW - to mine proof-of-work cryptocurrency are causing concerns about grid reliability. In Texas recently, so many miners asked to be connected to the Electric Reliability Council of Texas Inc. ("ERCOT") system

---

[29] Asher-Schapiro, *Coal to crypto*; Aoyon Ashraf, *Blockware Solutions Builds 20MW Bitcoin Mining Data Center in Kentucky*, CoinDesk (Mar. 29, 2022), https://www.coindesk.com/tech/2022/03/29/blockware-solutions-builds-20mw-bitcoin-mining-data-center-in-kentucky/.

[30] Bill Estep, *Kentucky's digital gold rush. What's behind the crypto mining boom in coal country?*, Lexington Herald Leader (Apr. 21, 2022), https://www.kentucky.com/news/state/kentucky/article259880855.html.

[31] The Lake News, *Core Scientific opens Calvert data center*, The Paducah Sun (Nov. 27, 2019), https://www.paducahsun.com/news/kentucky/core-scientific-opens-calvert-data-center/article_c3cd355f-95d8-51ad-9f69-dd456931b1fe.html (it's unclear how much of this energy use is in Kentucky but "Core Scientific said the Calvert City facility 'extends the Core Scientific footprint to more than 250MW of capacity across five datacenters, with a further 400MW under LOI.'").

[32] Arnab Shome, *Ukrainian Oligarch Mining Bitcoins in a Closed Kentucky Steel Plant*, Finance Magnates (Dec. 14, 2020), https://www.financemagnates.com/cryptocurrency/news/ukrainian-oligarch-mining-bitcoins-in-a-closed-kentucky-steel-plant/ (noting that CC Metals & Alloys "is only one of around five major crypto mining operations in the region", and that "maintaining a data center mining cryptocurrencies does not need that many workers").

[33] *Id.*

[34] Compass Mining, *Kentucky 1*, https://compassmining.io/facilities/united-states/kentucky-1/-MIxYnkXEQ2zbrX8i4G- (last visited May 5, 2022); Compass Mining, *Kentucky 2*, https://compassmining.io/facilities/united-states/kentucky-2/-MVLjQAmUYPGtsdkhrnB (last visited May 5, 2022).

[35] Fitch Ratings, *Crypto Mining Poses Challenges to Public Power Utilities*, https://www.fitchratings.com/research/us-public-finance/crypto-mining-poses-challenges-to-public-power-utilities-24-01-2022 (Jan. 24, 2022) (finding that "[c]rypto mining operations typically bring in very little additional economic benefits in the form of jobs or ancillary business to a local economy").

that the grid operator instituted new processes to ensure the system can handle the enormous load.[36] ERCOT will now require new, large cryptocurrency miners to seek permission to connect to the state's power and will require utilities to submit studies on the impact of miners and other large users on the grid.[37] Texas also created a task force to create an interim plan until the full studies can be conducted in order to protect the grid from being overwhelmed.[38] This is on top of the well-recognized issues with the U.S. grid in this country that the Federal Energy Regulatory Commission ("FERC") is evaluating for significant upgrades.[39]

Some miners argue their operations are beneficial for the grid because they can shut down quickly via demand response programs. When that occurs, miners are paid for the ability to shut down even though they are "taking demand off the grid that they never would have put on the grid at those high prices anyway."[40] Moreover, this so-called "grid service" via demand response programs are not widely used in Kentucky. The Big Rivers utility, for example, has a "voluntary curtailment" rider, but it has not been used since 2010.[41] In Kentucky, power prices are consistently low enough that crypto miners are unlikely to have a sufficient incentive to shut down their operations during peak demand periods; the capital-intensive nature of their operations gives them a strong incentive to continue operating 24/7.

In addition, utilities are upgrading infrastructure not for local populations or to connect renewable energy to demand centers where it is most needed, but to serve mining operations. For example, the Kentucky Public Service Committee recently approved $12.7 million in transmission upgrades for Big Rivers to provide service to Blockware Mining in Paducah, the costs of which will be passed on to ratepayers.[42]

Moreover, contrary to many "greenwashed" claims, experts do not believe that proof-of-work mining will aid the transition to renewable electricity.[43] Cryptomining requires a steady source of power, so miners are seeking cheap sources of electricity generated in Kentucky by burning coal and fossil gas. Research shows that the use of renewable energy by miners has fallen in recent years, according to one

---

[36] Naureen Malik, *Crypto Miners in Texas Need 'Approval to Energize' in New Grid Hurdle*, Bloomberg (Mar. 30, 2022), https://www.bloomberg.com/news/articles/2022-03-30/texas-crypto-miners-need-approval-to-energize-in-grid-hurdle.

[37] *Id.*

[38] *Id.*

[39] Fed. Energy Regul. Comm'n, *FERC Issues Transmission NOPR Addressing Planning, Cost Allocation* (Apr. 21, 2022), https://www.ferc.gov/news-events/news/ferc-issues-transmission-nopr-addressing-planning-cost-allocation; *see also* Fed. Energy Regul. Comm'n, Building for the Future Through Electric Regional Transmission Planning and Cost Allocation and Generator Interconnection, 86 Fed. Reg. 40,266 (July 27, 2021).

[40] Severin Borenstein. *Crypto Mining for a More Stable Grid?*, Energy Institute At HAAS: Energy Institute Blog, (March 21, 2022), https://energyathaas.wordpress.com/2022/03/21/crypto-mining-for-a-more-stable-grid/.

[41] Big Rivers Elec. Corp., *2020 Integrated Resource Plan*, at 61-62, 86-87 (2020), https://psc.ky.gov/pscecf/2020-00299/roger.hickman%40bigrivers.com/09212020071904/Big_Rivers_2020_IRP_with_Appendices.pdf.

[42] Order, *In re: Elec. App'n of Big Rivers Elec. Corp. for a Certificate of Pub. Convenience & Necessity to Construct a 161 kV Transmission Line in McKracken Cnty., Ky.*, Case No. 2021-00275 (Ky. P.S.C. Jan. 14, 2022).

[43] *See, e.g.*, Neel Dhanesha, *The daunting task of making cryptocurrency climate-friendly*, Vox (Apr. 18, 2022), https://www.vox.com/recode/23005493/cryptocurrency-bitcoin-climate-friendly.

estimate.[44] There is also no way to ensure that operations that mine proof-of-work cryptocurrency will switch to clean energy. Unlike industries subject to pollution controls or energy efficiency standards, electricity use by miners and their climate pollution are not subject to state or federal limits and there is no reporting mechanism to keep miners accountable.

Rate impacts on local residents and businesses from proof-of-work mining operations

The enormous amount of energy that mining operations siphon from the grid leaves less electricity and more expensive electricity for the rest of Kentuckians.

Kentucky Power, a utility serving 165,000 consumers in 30 counties, has apparently been approached by "dozens of mining operations" to give preferential utility rates to proof-of-work miners.[45] Kentucky Power recently projected that about a half-dozen cryptocurrency operations were already up and running in its territory, with five additional operators working to open facilities.[46]

Yet ordinary Kentucky residents and businesses struggle with ever increasing energy burden from their bills. As Baylen Campbell**,** executive director for Appalachians for Appalachia, recently said, "[l]ocal energy infrastructure is being pushed to the limit. Meanwhile these miners are receiving benefits that local business owners, and everyday people, are not being extended as well."[47]

Several other localities have seen their local electricity prices rise when proof-of-work cryptocurrency miners move into town. For example, in Plattsburgh, New York, residents' electricity bills increased 30% when a mining boom came to town a few years ago.[48] A recent study found that Plattsburgh residents and small businesses paid $244 million more in higher electric bills due to crypto's arrival.[49] Similarly, in eastern Washington, the Chelan County Public Utility District was overwhelmed by demand for cheap hydropower from crypto miners, and had to institute two moratoriums on new mining operations and a new rate structure to discourage miners from setting up shop there and straining its grid.[50]

---

[44] Alex de Vries *et al.*, *Revisiting Bitcoin's carbon footprint*, 6 Joule, 498, Figure 3 (Feb. 25, 2022), https://www.sciencedirect.com/science/article/abs/pii/S2542435122000861?dgcid=author.

[45] Asher-Schapiro, *Coal to crypto*.

[46] Bill Estep, *Kentucky's digital gold rush. What's behind the crypto mining boom in coal country?*, Lexington Herald Leader (Apr. 21, 2022), https://www.kentucky.com/news/state/kentucky/article259880855.html.

[47] Asher-Schapiro, *Coal to crypto*.

[48] Laura Counts, *Power-hungry cryptominers push up electricity costs for locals*, Berkeley Hass (Aug. 3, 2021), https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-locals/; Mateo Benetton *et al.*, *When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy*, SSRN (May 14, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720.

[49] *Id.*

[50] Steve Wright, *Testimony before the Subcommittee on Oversight and Investigations, Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains* (Jan. 20, 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Wright_OI_2022.01.20.pdf.

Proof-of-work mining operations generate enormous amounts of electronic waste

Proof-of-work mining results in enormous amounts of electronic waste which can cause significant harm to the environmental and human health.[51] Bitcoin's proof-of-work mining generates approximately 31 metric kilotonnes of e-waste every year, which is comparable to the e-waste produced by the whole country of the Netherlands.[52] The mining devices used for proof-of-work quickly go obsolete, often lasting less than two years.[53] Experts predict the waste will only increase as proof-of-work mining infrastructure becomes more powerful and increases in scale.[54] Much of this waste is sent to low-income communities who bear the harms of this toxic waste.[55]

* * * * * * *

As this comment letter shows, Kentucky is home to some of the dirtiest proof-of-work cryptocurrency mining operations in the country. Locally, we can ill-afford additional air and water pollution in Kentucky and the planet can ill-afford even more greenhouse gas emissions in the middle of a climate crisis, especially where the Co-Chair of IPCC Working Group recently warned that:

> It's now or never, if we want to limit global warming to 1.5°C (2.7°F); without immediate and deep emissions reductions across all sectors, it will be impossible.[56]

---

[51] *Id.*; *see also*, Megan Avakian, *E-waste: An Emerging Health Risk*, Nat'l Inst. of Env't Health Scis. (Feb. 2014), https://www.niehs.nih.gov/research/programs/geh/geh_newsletter/2014/2/spotlight/ewaste_an_emerging_health_risk_.cfm; EPA, *Cleaning Up Electronic Waste (E-Waste):Understanding e-waste*, https://www.epa.gov/international-cooperation/cleaning-electronic-waste-e-waste (last visited May 5, 2022) ("Without proper standards and enforcement, improper practices may result in public health and environmental concerns, even in countries where processing facilities exist.").

[52] BBC, *Bitcoin mining producing tonnes of waste*, (Sep. 20, 2021), https://www.bbc.com/news/technology-58572385; Alex de Vries & Christian Stoll, *Bitcoin's Growing E-waste Problem*, 175 Res., Conservation & Recycling 105901 (Dec. 2021), https://www.sciencedirect.com/science/article/pii/S0921344921005103; *Bitcoin Electric Waste Monitor*, Digiconomist, https://digiconomist.net/Bitcoin-electronic-waste-monitor/ (last visited May 5, 2022).

[53] Joachim Klement, *Geo-Economics: The Interplay between Geopolitics, Economics, and Investments*, at 200 (2021), https://www.cfainstitute.org/-/media/documents/book/rf-publication/2021/geo-economics-full.pdf

[54] Mark Peplow, *Bitcoin Poses Major Electronic-Waste Problem*, Chem. & Eng'g News (Mar. 14, 2019), https://cen.acs.org/environment/sustainability/Bitcoin-poses-major-electronic-waste/97/i1.

[55] Peter Howson & Alex de Vries, *Preying on the poor? Opportunities and challenges for tackling the social and environmental threats of cryptocurrencies for vulnerable and low-income communities*, 48 Energy Rsch. & Soc. Sci. 102394 (Feb. 2022), https://doi.org/10.1016/j.erss.2021.102394.

[56] UN News, *UN Climate Report: It's 'Now Or Never' To Limit Global Warming To 1.5 Degrees*, United Nations: Africa Renewal (Apr. 4, 2022), https://www.un.org/africarenewal/magazine/april-2022/un-climate-report-it%E2%80%99s-%E2%80%98now-or-never%E2%80%99-limit-global-warming-15-degrees.

Thank you for the opportunity to provide comments on this urgent and timely issue.

Sincerely,

Lane Boldman
[redacted]

Ashley Wilmes
[redacted]

Mary Varson Cromer
[redacted]

Nina and Mickey McCoy
[redacted]

Elisa Owen
[redacted]

Ben Carter
[redacted]

Aaron Viles
[redacted]

Mandy DeRoche
Nick Thorpe
Earthjustice
[redacted]

Thomas Cmar
[redacted]

May 9, 2022

<u>**VIA ELECTRONIC SUBMISSION**</u>
Office of Science & Technology Policy
Eisenhower Executive Office Building
[redacted]

Re: The Energy and Climate Implications of Digital Assets in New York State

Thank you for the opportunity to provide comments on the Request for Information ("RFI") on the Energy and Climate Implications of Digital Assets. 87 Fed. Reg. 17,105 (Mar. 25, 2022). Please accept these state-specific comments for New York on behalf of the undersigned organizations.

We appreciate the Biden Administration's efforts to combat the climate crisis and advance environmental justice by cutting U.S. greenhouse gas pollution at least 50% by 2030 and having a net-zero emissions economy by 2050. However, as the RFI notes, these efforts will be imperiled by the climate, energy, and environmental challenges from digital assets that rely on proof-of-work consensus mechanisms. Tremendous amounts of fossil-fuel-powered energy in the U.S. following the ban on crypto-mining in China in September 2021 now threaten the achievement of climate and energy commitments.[1]

1. Proof-of-work Cryptocurrency or "Digital Asset" Mining Uses an Enormous Amount of Electricity.

Proof-of-work cryptocurrency mining consumes massive amounts of electricity.[2] Bitcoin's electricity consumption alone increased more than threefold between the beginning of 2019 and May 2021.[3] Estimates of Bitcoin's global energy use are approximately 152 tera-watt hour ("TWh").[4] In comparison, the entire state of New York used approximately 150 TWh in 2020.[5] Due to this enormous amount of electricity use, Bitcoin's annual global greenhouse gas emissions have been estimated by some at between roughly 60 to 100 million tons of carbon dioxide ("CO_2"), though this is most likely an underestimate given the exponential growth of mining in recent years.[6] Further, a recent congressional memo estimates that the annual emissions from Bitcoin and Ethereum are equal to roughly 15.5 million car tailpipes per year.[7] Although it is difficult to forecast emissions in coming years given the rapid growth of proof-of-work cryptocurrency mining in the United States after China's ban in September 2021, academics estimate that "cryptocurrency's energy usage will rise another 30% by the end of the decade—producing an additional 32.5 million metric tons of carbon dioxide a year."[8]

2. Climate and Energy Impacts from Proof-of-work Mining in New York State.

The climate and energy impacts of proof-of-work cryptocurrency mining in New York and throughout the United States are staggering and increasing every day.[9] Following China's ban on proof-of-work mining in September 2021, the U.S. is now the largest proof-of-work mining location in the world, accounting for more than one-third of the global market.[10] New York is home to approximately 20% of the country's proof-of-work cryptocurrency mining operations.[11]

As the map below shows, [12] there are many operating and proposed large-scale cryptocurrency mining operations in upstate New York.

As detailed below, New York is also at the frontline of several local fights against proof-of-work cryptocurrency mining operations that burn fossil fuels and which threaten local health, local ecosystems, local economies,[13] and prevent the State from meeting its statutory climate and clean energy goals. But this cannot be a town-by-town or even a state-by-state fight: the consequences of inaction and disparate action are too severe. An increased use of fossil-fueled electricity has terrible consequences for climate, for air and water pollution, and is unconscionable during a climate crisis.[14]

3. Lack of Reliable and Specific Information on Proof-of-work Mining Operations.

Unfortunately, there is very little transparency in this largely unregulated, energy-intensive wild-west industry. Many operations can operate as of right now under existing laws, regulations, and permits with no additional oversight. Mining operations can negotiate private contracts with merchant generators or utilities for discounted rates. Proof-of-work mining operations vary greatly in size and are often ever-expanding. Given the unregulated nature of crypto mining, it is notoriously difficult to determine how much energy a particular entity is using, what fuel source the mining operation relies on, or estimate how much a particular entity is mining in general. Without a standardized methodology to collect data to properly estimate energy consumption from cryptocurrency mining, estimates will continue to vary widely. Without accurate information, it is nearly impossible for communities, local groups, and interested residents to understand the impact a mining operation can have on the community. Despite what little we know about mining operations, what we do know for certain is that the expansion of crypto currency mining in the United States increases air and water pollution, strains the electrical grid, and increases electricity rates of local residents.

4. Proof-of-work Mining Increases the Operations of Fossil Fueled Power Plants.

Companies and private-equity firms have invested significantly in proof-of-work mining facilities in New York and throughout the U.S.[15] We frequently hear from the Bitcoin community about the merits of financial decentralization, but the reality does not seem to bear that utopian dream out.[16] Because of the immense amount of capital needed to purchase enough application-specific integrated circuit ("ASIC") miners[17] to competitively mine bitcoin, there are fewer miners today compared to even a few years ago.[18] In 2021, before China banned mining, a whitepaper published by the National Bureau of Economic

Research found that the top 10% of crypto miners control 90% of mining and just 0.1% (about 50 miners) control close to 50% of all mining—which directly translates to "ownership" of Bitcoin.[19] It has been surmised that the concentration of mining wealth is even more pronounced in the U.S. today.[20]

In New York, those entities are resurrecting and extending the life of old, inefficient, fossil-fueled power plants to mine proof-of-work cryptocurrency—translating to significant greenhouse gas emissions. Unfortunately, that increase in fossil-fueled electricity has dire consequences for the climate, air and water pollution, and communities that live in the shadow of fossil fuel plants. Two upstate New York power plants in particular tell a worrying story:

In North Tonawanda, New York, just outside Buffalo, is the fossil gas Fortistar North Tonawanda ("FNT") power plant where a new owner intends to convert the little-used 60 megawatt ("MW") gas turbine facility to mine proof-of-work cryptocurrency 24/7, 365 days per year. Over the past five years the FNT plant operated at 2–13% capacity factor emitting relatively small amounts of CO_2, nitrogen oxide ("NO_x"), and other harmful air pollutants.[21] If the plant operates every day at full capacity, the potential emissions from the facility will sharply increase to 339,068 tons of CO_2 per year—a nearly **3,000%** increase in its CO_2 emissions—while also significantly increasing emissions of NO_x, particulate matter, carbon monoxide, and volatile organic compounds.[22] This signficant increase in air pollution will spew into several nearby environmental justice areas.[23]

In addition, increased operation of the power plant significantly increases clean water intake and discharge of hot water. The FNT facility plans to use 500,000 gallons of water per day for cooling purposes, which will discharge to the local wastewater treatment plant. That will account for approximately 12% of the City of North Tonawanda's current total water usage.[24] This significant additional thermal discharge comes at a time when the city can least afford it. The North Tonawanda water treatment plant recently discovered that it needs $3 million in emergency repairs and $30 million for long term repairs.[25]

In another instance, on the western shores of Seneca Lake, amongst the productive vineyards and farms of the Finger Lakes, is the Greenidge Generating Station. Like FNT, in recent years Greenidge was operating infrequently[26] and is now operating 24/7/365 to mine cryptocurrency. In 2020, the Greenidge CFO stated "[w]ithout the crypto mining operation, we would not be running most of the time."[27] Indeed for six years, the plant did not operate at all.[28] The Greenidge facility emissions history tells the story:

Year	Days of Operation[29]	Approx. Annual Capacity Factor[30]	CO2 (tons/ year)	No. of Miners	Fuel source
2009	267	~34%	455,795	0	Coal
2010	358	~65%	599,105	0	Coal
2011[31]	77	~10%	113,357	0	Coal
2012	0	0%	0	0	*none*
2013	0	0%	0	0	*none*
2014	0	0%	0	0	*none*
2015	0	0%	0	0	*none*
2016	0	0%	0	0	*none*
2017	135	~17%	124,009	0	Gas
2018	147	~19%	119,304	0	Gas
2019[32]	48	~6%	39,406	0	Gas
2020	**343**	**~42%**	**228,303**	**6,900 miners[33]**	**Gas**
2021	353	~51%	278,846	15,300 miners[34]	Gas
2022	Every day	Increasing	91,530 (for 01/01–03/31/2022)[35]	32,500 miners[36]	Gas

The Greenidge plant also discharges hot water from the plant, but here the plant owners are permitted to discharge 134 million gallons of water daily into a nearby trout stream at temperatures of *up to 108 degrees Fahrenheit*.[37] This thermal pollution endangers the Keuka Outlet and Seneca Lake—impacting health and wildlife habitability, including but not limited to potential harmful algal blooms, migration and loss of biodiversity, oxygen depletion, direct thermal shock, and changes in dissolved oxygen.

As high-profile as they are, the conversion of Greenidge Generating Station and Fortistar North Tonawanda from low-capacity plants to 24 hours-a-day, 7 days-a-week, 365 days-a-year mining operations are just two examples of how a low-capacity power plant can ramp up operations to increase their profits at the expense of local air and water pollution and increasing greenhouse gas emissions that accelerate the impending climate crisis. Indeed, Senator Kirsten Gillibrand stated in her September 8, 2021 letter to the EPA that "the potential consequences of the plant's Bitcoin mining operations and the effect on local emissions and air quality" are significant and require full assessment.[38] Senator Schumer also recently "urged the Environmental Protection Agency (EPA) to exercise its oversight powers under the Title V Clean Air Act and Clean Water Act and closely review Greenidge Generation Plant's permit renewal application" because "[t]he EPA and NYSDEC regulate such plants to keep these negative impacts on our health and the environment to a minimum, while maximizing the public good" and "[t]his increase in emissions may bring profits to the plant's owners, but it does not provide the same pub[l]ic good to the surrounding community…."[39]

Notably, as New York and the U.S. transition to renewable energy resources, there will be an increasing number of fossil fuel power plants that operate less frequently. Evaluation of the New York Independent System Operator's ("NYISO") 2021 Load and Capacity Data spreadsheet identifies a potential 22,891 MW capacity from fossil fueled power plants operating at less than 30% capacity factor—all of which, under current lack of regulations, could be utilized for proof-of Work mining operations.[40] Indeed, a March 2021 opinion piece in the Albany Times Union,[41] penned the President and CEO of the Independent Power Producers of New York titled "There's a Role for Natural Gas in the Renewable Energy Future" foreshadowed such a turn, describing Greenidge's transition to crypto mining as a "model for innovation."

5. Proof-of-work Mining Places a Large New Load on the NYS Electric Grid.

At a recent NYS Environmental Conservation budget hearing, when asked about the potential impact of the escalating cryptocurrency mining activity in upstate NY on the state's energy grid, the NYS Energy Research and Development Authority ("NYSERDA") President Doreen Harris stated, "There could be a very significant impact on NY load resulting from cryptocurrency mining depending on the penetration of the resource."[42]

To our knowledge, there is no registry of proof-of-work mining facilities in New York State or anywhere in the U.S. Data on mining facilities in New York State in the below table are derived from various news stories, press releases, videos, Town Board minutes, etc. Based on the information we could locate, there are currently 13 proof-of-work mining facilities imposing at least a 576 MW load in New York State. Data on the number of mining rigs used at a given site was even harder to come by, but we were able to document approximately 88,000 mining rigs.[43] If these mining operations expand to the extent their literature suggests, by the fourth quarter of 2022, there could be up to 1,626 MW of proof-of-work mining operations in New York State.[44]

Table 1: Known Proof-of-work Mining Facilities Currently Operating in New York State

Mining Facility	MW	Electric Source	# Machines	Status
Coinmint NCDC Massena, Old Alcoa W	250 --> 435	NYPA, hydro	46,000 → 81,000	Operating @ 250; 185 request pending NYISO review
Greenidge LLC Coal → Gas power plant Seneca Lake, Dresden	25 – >100	Onsite Gas Generation Carbon offsets, 2MW solar proposed	17,300 →31,700	Operating @ 25MW, propose increase to 100MW. **Already 10x increase GHG emissions.** DEC air permit renewal pending 3/31/22
Fortistar (Digihost) Operating gas peaker plant N. Tonawanda	35 --> 55	Gas	9400	Proposal to convert pending PSC decision. DEC air permit renewal soon. Convert to RNG or Hydrogen? 14 containers @700 rigs each
Somerset, Lake Mariner Retired coal plant, Barker	0 - 250 --> 500	Hydro, grid mix		NYPA approved 90 MW hydro. Town approved; construction underway.
Cayuga, TeraWulf Retired coal plant Cayuga Lake, Lansing	0 --> 100	Hydro, grid mix		NYPA approved 2.5 MW hydro. Possible 100-200 MW solar? No active proposal w Town.
Wattum Niagara Falls area	5 –> 50	Hydro Grid mix		Operating 5MW now. Expand to 50MW in 2022.
Weitsman Owego	8 --> 115	Grid mix	2500 ->35,000	Operating 8 MW now. 100 more pending. Interconnection app?
Massena Containers	2 –> 20	Hydro Grid mix		Multiple. Town issued moratorium
Mechanicsville	4	Hydro		Operating.
US Bitcoin Niagara Falls	45	Hydro Grid mix	12,600	Operating. 18 containers@ old DuPont site in Niagara Falls x 700 rigs per container
Bit Digital / Blockfusion Niagara Falls	150	Hydro Grid mix		GM coal plant along Niagara River
Plattsburgh NCDC	10	Hydro Grid mix		
Digihost American Axle Buffalo	42	Hydro Grid Mix		
TOTAL	576 MW now 1336 – 1626 MW by Q4 2022		87,800 known	

To put the above cryptocurrency mining load in perspective, consider the following: For the year 2020, NYISO reports that NYS used 150,198 gigawatt hours ("GWh") electricity.[45] Thus, the 576 MW (5,046 GWh) load we have identified for active, known instances proof-of-work mining is 3.35% of NYS's 2020 energy use. If the proof-of-work mining expansion to 1,626 MW (14,244 GWh) by Q4 2022 occurs—this would be a whopping 9.5% of NYS's 2020 energy use.

6. Proof-of-work Cryptocurrency Mining Operations will Make it Harder to Achieve New York State Renewable Energy Goals.

Adding demand from proof-of-work cryptocurrency mining to the New York grid could increase capacity problems, especially downstate.[46] New York's Climate Leadership and Community Protection Act is one of the most ambitious climate laws in the country, committing the state to, among other things, 70% renewable electricity by 2030 as well as 40% reduction in greenhouse gas emissions.[47] In order to simultaneously meet these renewable energy targets while also rapidly electrifying the building and transportation sectors, the NYISO projects the need to install 15,000 MW new solar and 8,700 MW land-based wind by 2030.[48] This is a daunting task to accomplish in the next 8 years. The new solar farms will cover 90,000 acres, approximately 5 times the footprint of Manhattan; the wind farms will require erecting 2,200 turbines the size of the Statue of Liberty.[49] In addition, hundreds of miles of new transmission lines will need to be installed at a cost of tens of billions of dollars to convey this energy from upstate where the land is, to downstate where the load is.

Clearly allowing underutilized fossil fuel power plants to engage in proof-of-work mining of digital assets 24/7/365 would take NYS (and the country) in the wrong direction relative to meeting renewable energy and greenhouse gas reduction goals.

The difficulty of transitioning the added load from proof-of-work mining activities to renewable energy may not be as obvious, as one must understand that 100 MW energy drawn from the grid is not the same as installing 100 MW renewable resources. In New York State, solar has a capacity factor of approximately 14%,[50] meaning that one would need to install 100/0.14 = 714 MW solar to generate the equivalent of 100 MW grid power. Similarly, the capacity factor for wind in New York State at present is approximately 29%,[51] meaning that one would need to install 100/0.29 = 345 MW wind to produce 100 MW grid power. Applying these capacity factors to the current 576 MW proof-of-work cryptocurrency mining in New York State would mean adding an additional 4,144 MW (27%) solar to the 15,000 MW the NYISO indicated we need by 2030 and a whopping 11,614 MW (77% increase) to provide enough solar power to cover the 1,626 MW added proof-of-work mining load anticipated by Q4 of 2022. Alternatively, adding wind for 576 MW would entail adding 1,986 MW wind, at 4 MW per turbine, equal to adding another 496 turbines—a 23% increase over the 2,200 turbines already planned; to cover the 1,626 MW load anticipated by Q4 2022 would require an added 5607 MW wind, or 1,401 additional turbines by 2030—an increase of 64% over the NYISO planned build out. Studies are needed in order to understand what necessary additions would need to be made to the transmission system to provide interconnection and hosting to this added capacity.

As demonstrated by the forgoing calculations, satisfying the voracious appetite of proof-of-work mining with renewable energy while also meeting the state's ambitious renewable energy goals is simply not feasible. The inevitable result is that fossil-fueled power plants will need to continue operation in order to satisfy the added grid load from proof-of-work mining activities.

Further, as indicated in Table 1 above listing the current mining operations in the State, much of the current proof-of-work mining activity is taking place near Niagara Falls and the St. Lawrence River hydro plants. This means that the mining facilities are utilizing the State's only source of baseload renewable energy, while not providing any additive renewable and storage resources to the grid to compensate.

Regional Transmission Organizations, Independent System Operators, and utilities around the nation are beginning to understand the impacts caused by proof-of-work cryptocurrency to their mandates to provide just, reasonable, and reliable electricity to homes and local businesses. NYISO needs to also take note of the large amounts of load coming onto the system and plan accordingly. Recently, the Electric Reliability Council of Texas ("ERCOT"), responding to worries that a flood of requests from crypto miners would drive up electricity demand and could ultimately overwhelm the grid, announced it will be instituting additional processes and requirements for new large-scale crypto miners to connect to the state's power grid.[52] On March 25, 2022, ERCOT released a notice[53] instructing utilities to submit studies on the impact of miners and other large users tapping the grid before they can get "approval to energize."[54]

7. Proof-of-work Cryptocurrency Mining Operations Could Displace Renewables Away from Residential and Commercial Uses as well as Hard-To-Decarbonize Industries.

Across the country, the cryptocurrency mining industry has been arguing that proof-of-work cryptocurrency mining could "stabilize" the grid. Grid experts are dubious. For example, a recent analysis by UC-Berkeley's Energy Institute at Haas found that "[a]dding demand will just make a grid tighter and increase capacity problems." And then the "the mining companies get paid for taking demand off the grid that they never would have put on the grid at those high prices anyway."[55]

The enormous amount of energy used by proof-of-work cryptocurrency mining also threatens to undo climate action to date and potentially makes it impossible to tackle the climate crisis since it diverts renewable energy sources from people that need it.

Contrary to proof-of-work cryptocurrency mining proponents, mining is not a catalyst for growth in clean energy. Clean energy is already cost-effective, efficient, and decentralized in comparison to dirty fossil fuel plants, even without the presence of cryptocurrency mining.

And in actuality, cryptocurrency mining companies are predominantly utilizing fossil fuel generation,[56] to mine for cryptocurrency. And even where clean, renewable energy technologies like solar or wind are being used to mine, many operations do not have commitments for renewable-only power supply and instead continue to mine when the sun is not shining nor the wind blowing, using the grid or natural gas. Further, considering how volatile the cryptocurrency market is and the fact that cryptocurrency mining companies come and go, there are serious implications for what happens when a cryptocurrency mining facility leaves the area and the economics of the renewable energy project means that it is unable to properly compete in an open market and potentially becomes stranded.

Crypto miners also often assert that they can spur renewable energy growth. But renewable energy costs are already low, [57] its growth exponential, and it does not need crypto mining operations to prop it up. Even if cryptocurrency mining companies only used excess renewable energy that would otherwise be curtailed, there are serious implications with wasting energy at a time when we need to be placing that energy in energy storage technologies for dispatch at peak usage times.

Building and transportation electrification will further increase demand on the grid, and green hydrogen proposals would also require copious amounts of zero-emissions energy. [58] Simply put, there is not enough clean energy in New York State to meet all that demand while supporting the extensive demands of proof-of-work cryptocurrency mining.

8. Electricity Prices for Local Residents and Business Spike When Proof-of-work Mining Moves Into Town.

Several New York localities have seen their local electricity prices rise when proof-of-work cryptocurrency miners move into town.

For example, in Plattsburgh, New York, residents' electricity bills increased 30% when a mining boom came to town a few years ago.[59] As a result, the New York Municipal Power Agency ("NYMPA"), an association of 36 municipal power authorities, petitioned the NYS Public Service Commission to prevent high-density load customers, specifically cryptocurrency companies, from requesting disproportionately large amounts of power, in some cases amounting to up to 33% of municipal utility's total load.[60] Concerns about electric rates, noise complaints, and unsightly server setups ultimately led Massena to issue a moratorium on crypto operations while public hearings are conducted to consider their continued impact in the small town.[61] Cryptocurrency companies that require high quantities of power increase bulk power supply costs with little to no capital investment in the local community. A recent study found that Plattsburgh residents and small businesses paid $244 million more in higher electric bills due to crypto's arrival.[62] After NYMPA increased rates for supplemental electricity used by high-density load customers, large-scale cryptocurrency data centers were forced to move from Plattsburgh to Massena, which is not a NYMPA member, as their costs increased over $1 million more than the year prior when they were allowed to buy market-rate electricity.[63]

Other parts of the country have and continue to face the same issues. For example, in eastern Washington, the Chelan County Public Utility District was overwhelmed by demand for cheap hydropower from crypto miners, and had to institute two moratoriums on new mining operations and a new rate structure to discourage miners from placing further strains on their grid.[64] Many cryptocurrency miners left the area because of the rate changes,[65] and when miners leave an area, there is a recurring concern across the country that they might "leav[e] ratepayers to cover the costs of upgrades that may no longer be needed."[66] For example, a congressional memo cited to a cryptocurrency mining operation in Washington state that declared bankruptcy in 2018, leaving more than $700,000 in unpaid utility and electricity bills.[67]

For a fuller discussion of the economic and ratepayer impacts on local residents and municipalities, we refer to the comments being simultaneously submitted by Dr. Colin Read.[68]

9. Electronic Waste From Proof-of-work Cryptocurrency Mining.

Proof-of-work mining results in enormous amounts of electronic waste which can cause significant harm to environmental and human health.[69] Globally, proof-of-work mining generates approximately 31 metric kilotonnes of e-waste every year, which is comparable to the e-waste produced by the whole country of the Netherlands.[70] The mining devices used for proof-of-work quickly go obsolete, often lasting less than two years.[71] Experts predict the waste will only increase as proof-of-work mining infrastructure becomes more powerful and increases in scale.[72] Much of this waste is sent to low-income communities who bear the harms of this toxic waste.[73]

10. Conclusion.

As crypto continues to grow, the associated surge in energy consumption to maintain proof-of-work cryptocurrency mining threatens to make the clean energy transition and meeting federal and state-level climate and environmental justice goals much more difficult, if not impossible. While the impacts of large-scale cryptocurrency operations have been most felt in small towns by local residents bearing the brunt of local air and water pollution, as well as increased electricity costs, the consequences of allowing cryptocurrency mining operations to expand unmitigated are far too great to ignore.

This cannot be a town-by-town or even a state-by-state fight, but rather requires federal attention to address the ever-increasing public health and environmental threat that cryptocurrency mining poses. Without proper standards and the federal action, proof-of-work cryptocurrency mining will elongate the life of fossil fuels and divert renewable energy from where it's needed most to avert the worst of the climate crisis.

Thank you for the opportunity to provide comments concerning the impacts of proof-of-work cryptocurrency mining in New York State.

Respectfully submitted,

Joseph Campbell
Yvonne Taylor
Seneca Lake Guardian
[redacted]

Irene Weiser
Fossil Free Tompkins
[redacted]

Abi Buddington
Committee to Preserve the Finger Lakes
[redacted]

Bridge Rauch
The Clean Air Coalition of Western New York
[redacted]

Ellen Weininger
Grassroots Environmental Education
[redacted]

Kathryn Bartholomew
Bill Mattingly
Sierra Club Atlantic Chapter
[redacted]

Andra Leimanis
Alliance for a Green Economy
[redacted]

Gay Nicholson
Sustainable Tompkins, Inc.
[redacted]

Joseph Campbell
Gas Free Seneca
[redacted]

Eric Weltman
Food & Water Watch
[redacted]

Francesca Rheannon
Climate Reality Project Long Island Chapter

Doug Couchon
People for a Healthy Environment
[redacted]

Thomas Hirasuna
Climate Reality Project
Finger Lakes Greater Region NY Chapter

Mary Finneran
FrackBustersNY

Janet Harckham
Climate Reality Project Westchester NY Chapter

Dorian Fulvio
350NYC

Paul Kiesler

Regi Teasley

Climate Reality Project NYC Chapter

Denizens of the Biosphere

Lynn Saxton
Climate Reality Project Western NY Chapter

Eve Morgenstern
Climate Reality Project Hudson & Catskills Chapter

Fred Pfeiffer
The Solidarity Committee of the Capital District
[redacted]

Carol Baum
Syracuse Peace Council
[redacted]

Todd Ommen
Pace Environmental Litigation Clinic
[redacted]

Mandy DeRoche
Gilbert Zelaya
Nick Thorpe
Earthjustice
[redacted]

[1] Amy Qin & Ephrat Livni, *China Cracks Down Harder on Cryptocurrency With New Ban*, The New York Times (Sept. 24, 2021), https://www nytimes.com/2021/09/24/business/china-cryptocurrency-bitcoin.html. The ban in China also created a proof-of-work crypto mining boom in Kazakhstan, which lead to civil unrest as the new, unexpected load overwhelmed the needs of ordinary people and local businesses. *See, e.g.*, Gian M. Volpicelli, *As Kazakhstan Descends Into Chas, Crypto Miners Are at a Loss*, Wired (Jan. 12, 2022), https://www.wired.com/story/kazakhstan-cryptocurrency-mining-unrest-energy/; Ephrat Livni, *Kazakhstan's huge Bitcoin mining industry is upended by unrest*, The New York Times (Jan. 6, 2022), https://www.nytimes.com/2022/01/06/business/kazakhstan-bitcoin-mining.html; MacKenzie Sigalos, *Kazakhstan's deadly protests hit bitcoin, as the world's second-biggest mining hub shuts down*, CNBC (Jan. 7, 2022), https://www.cnbc.com/2022/01/06/kazakhstan-bitcoin-mining-shuts-down-amid-fatal-protests.html.

[2] Jon Huang et al., *Bitcoin Uses More Elec. Than Many Countries. How is that Possible?*, The New York Times (Sept. 3, 2021), https://www nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html.

[3] *Id.*; Brian Spegele & Caitlin Ostroff, *Bitcoin Miners Are Giving New Life to Old Fossil-Fuel Power Plants*, The Wall Street J. (May 21, 2021), https://www.wsj.com/articles/bitcoin-miners-are-giving-new-life-to-old-fossil-fuel-power-plants-11621594803.

[4] Bitcoin's network power demand is estimated to be in the range of 57.13 TWh to 343.75 TWh annually. *See* Univ. of Cambridge, Cambridge Bitcoin Elec. Consumption Index, https://ccaf.io/cbeci/index (last visited May 3, 2022).

[5] Statista, Leading states in elec. consumption in the United States in 2020 (2020), https://www.statista.com/statistics/560913/us-retail-electricity-consumption-by-major-state/; New York ISO ("NYISO"), *New York's Clean Energy Grid of the Future*, at 11–12 (2021), https://www.nyiso.com/documents/20142/2223020/2021-Power-Trends-Report.pdf/471a65f8-4f3a-59f9-4f8c-3d9f2754d7de.

[6] *See* Digiconomist, Bitcoin Energy Consumption Index (estimating Bitcoin's annual carbon footprint at 114.06 million metric tons of CO2, comparable to the carbon footprint of the Czech Republic), https://digiconomist.net/bitcoin-energy-consumption (last visited May 3, 2022); Forex Suggest, Global Impact of Crypto Trading (estimating that Bitcoin emits approximately 59 million metric tons of CO2 in 2020), https://forexsuggest.com/global-impact-of-crypto-trading/ (last visited May 3, 2022).

[7] Comm. on Energy and Com., Memorandum re: Hearing on 'Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains,' at 5 (Jan. 17, 2022), https://energycommerce house.gov/sites/democrats.energycommerce house.gov/files/documents/Briefing%20Memo_OI%20Hearing_2022.01.20.pdf.

[8] Lois Parshley, *How Bitcoin mining devastated this New York town*, MIT Tech. Review (Apr. 18, 2022), https://www.technologyreview.com/2022/04/18/1049331/bitcoin-cryptocurrency-cryptomining-new-york/.

[9] Renee Cho, *Bitcoin's Impacts on Climate and the Env't*, Colum. Climate Sch. (Sept. 20, 2021), https://news.climate.columbia.edu/2021/09/20/bitcoins-impacts-on-climate-and-the-environment/.

[10] *See, e.g.*, Joe Tidy, *US leads Bitcoin mining as China ban takes effect*, BBC (Oct. 13, 2021), https://www.bbc.com/news/technology-58896545; *see also* Letters from Senator Elizabeth Warren et al. to Cryptominers (Jan. 27, 2022) (explaining that the United States' share of global Bitcoin mining increased from 4% in August 2019 to 35% in July 2021), https://www.warren.senate.gov/imo/media/doc/2022.01.27%20Letters%20to%20Cryptominers.pdf.

[11] MacKenzie Sigalos, *New York and Texas are winning the war to attract bitcoin miners*, CNBC (Oct. 9, 2021), https://www.cnbc.com/2021/10/09/war-to-attract-bitcoin-miners-pits-texas-against-new-york-kentucky html.

[12] Provided by Fractracker Alliance.

[13] Marissa Solomon, *Gillibrand Commits LIVE ON AIR to Visit FLX & Meet w/Residents on Climate Killing Cryptomining @ Greenidge*, Seneca Lake Guardian (Apr. 27, 2022) (e.g., pointing to the $3 billion agritourism economy, employing approximately 60,000 people in the Finger Lakes), http://readme.readmedia.com/Gillibrand-Commits-LIVE-ON-AIR-to-Visit-FLX-Meet-w-Residents-on-Climate-Killing-Cryptomining-Greenidge/18521058.

[14] Africa Renewal, *UN climate report: It's 'now or never' to limit global warming to 1.5 degrees*, UN News (Apr. 4, 2022), https://www.un.org/africarenewal/magazine/april-2022/un-climate-report-it%E2%80%99s-%E2%80%98now-or-never%E2%80%99-limit-global-warming-15-degrees.

[15] *See, e.g.*, *supra* note 8.

[16] Khristopher J. Brooks, *Bitcoin has its own 1% who control outsized share of wealth*, CBS News (Dec. 21, 2021), https://www.cbsnews.com/news/bitcoin-cryptocurrency-wealth-one-percent/.

[17] Paul Kim, *ASIC mining: Computers built specifically for mining cryptocurrency*, Insider (Mar. 16, 2022), https://www.businessinsider.com/personal-finance/asic-mining.

[18] Kristina Zucchi, *Is Bitcoin Mining Still Profitable?*, Investopedia (Mar.12, 2022), https://www.investopedia.com/articles/forex/051115/bitcoin-mining-still-profitable.asp.

[19] Igor Makarov & Antoinette Schoar, Blockchain Analysis of the Bitcoin Market, National Bureau of Economic Research, at 4 (Oct. 2021), Working Paper 29396 (note: this analysis was for the time period before China banned mining), https://www.nber.org/system/files/working_papers/w29396/w29396.pdf; *see also* Emily Graffeo, *Bitcoin Is Still Concentrated in a Few Hands, Study Finds*, Time (Oct. 25, 2021), https://time.com/6110392/bitcoin-ownership/. It is believed that the concentration of mining and wealth is even more stark in the U.S. today.

[20] Paul Vigna, *Bitcoin's 'One Percent' Controls Lion's Share of the Cryptocurrency's Wealth*, The Wall Street Journal (Dec. 20, 2021), https://www.wsj.com/articles/bitcoins-one-percent-controls-lions-share-of-the-cryptocurrencys-wealth-11639996204; Laurence Fletcher, Hedge funds expect to hold 7% of assets in crypto within five years, Financial Times (June 15, 2021), https://www.ft.com/content/4f8044bf-8f0f-46b4-9fb7-6d0eba723017; Khristoper Brooks, *Bitcoin has its own 1% who control outsized share of wealth*, CBS News (Dec. 21, 2021), https://www.cbsnews.com/news/bitcoin-cryptocurrency-wealth-one-percent/; Gregory Zuckerman, *Mainstream Hedge Funds Pour Billions of Dollars Into Crypto*, The Wall Street Journal (Mar. 9, 2022), https://www.wsj.com/articles/mainstream-hedge-funds-pour-billions-of-dollars-into-crypto-11646808223.

[21] Env't Prot. Agency ("EPA"), *Power Sector Emissions Data*, https://www.epa.gov/airmarkets/power-sector-emissions-data; EPA, Air Markets Program Data (filtering by Customized Data Queries > 'All Programs' > 'Emissions', 'Unit Level' > 'Facility Attributes' > 'Daily,' > 'Facility ID and Name': 'Fortistar North Tonawanda Inc' > 'Select All' under Emissions Unit), https://ampd.epa.gov/ampd/ (last visited May 5, 2022).

[22] Digihost Tech., Inc., *Title V and Title IV Permits Renewal Application, Fortistar North Tonawanda Cogeneration Facility*, at 5–6, 30 (Apr. 21, 2021).

[23] N.Y. State Dep't of Env't Conservation, *Potential Environmental Justice Area (PEJA) Communities*, ArcGIS (filtering results to display: PEJA, 15000US360290091074; Census Block Group 15000US360290091074; Census Block Group 15000US360630232003; and Census Block Group 15000US360630232003), https://www.arcgis.com/home/webmap/viewer.html?url=https://services6.arcgis.com/DZHaqZm9cxOD4CWM/ArcGIS/rest/services/Potential_Environmental_Justice_Area__PEJA__Communities/FeatureServer&source=sd; *see also* EPA, *EJSCREEN: EPA's Environmental Justice Screening and Mapping Tool* (According to EPA's EJScreen, the area around the FNT plant has a disproportionately high ozone index when compared to the New York average), https://ejscreen.epa.gov/mapper/.

[24] Digihost, *Full Environmental Assessment Form*, at 5 (Aug. 12, 2021), https://www.northtonawanda.org/documents/legal%20notice/fortistar%20amended%20seqr_2.pdf (the City's current usage averages 4 million gallons per day).

[25] Thomas J. Prohaska, *North Tonawanda asks for $30 million in emergency aid to repair sewer plant*, The Buffalo News (Mar. 12, 2022), https://buffalonews.com/news/local/government-and-politics/north-tonawanda-asks-for-30-million-in-emergency-aid-to-repair-sewer-plant/article_91b32598-a145-11ec-b35d-7314fe498fd0.html.

[26] After only a few years of operating as an electric generating facility, the facility's owners realized that there was not enough demand for electricity to make operating the facility profitable. Greenidge's CFO stated that rather than close the power plant, they decided to convert the facility to a Bitcoin mining operation. John Christensen, *Power Plant to Add Data Center*, The Chronicle-Express (July 31, 2019), https://web.archive.org/web/20190731061907/https:/www.chronicle-express.com/news/20190731/power-plant-to-add-data-center#expand.

[27] *Digital Assets: Greenidge Gen, Once a Coal Plant, Is Now a Profitable Crypto Miner*, DailyAlts (Aug. 19, 2020) https://dailyalts.com/digital-assets-greenidge-gen-once-a-coal-plant-is-now-a-profitable-crypto-miner/.

[28] EPA, *Power Sector Emissions Data*, https://www.epa.gov/airmarkets/power-sector-emissions-data; https://ampd.epa.gov/ampd/ (filtering by Customized Data Queries > 'All Programs' > 'Emissions', 'Unit Level' > 'Facility Attributes' > 'Daily,' 'Select All' under Emissions Unit), (last visited May 4, 2022). These numbers do not include upstream emissions. For a full recitation of the facts and issues concerning the air permit at Greenidge, please see the Comments from Seneca Lake Guardian, The Comm. to Preserve the Finger Lakes, Fossil Free Tompkins, Sierra Club, and Earthjustice in Opposition to the Draft Title V Air Permit for Greenidge Generating Station, located at 590 Plant Road, Dresden, New York 14441 (Permit ID: 8-5736-00004/00017) (Nov. 19, 2021), https://earthjustice.org/sites/default/files/files/2021-11-19_slg-cpfl-fft-sc-ej-comments-to-dec.pdf.

[29] Days with less than three hours of operation were not included.

[30] The annual capacity factor is a percentage measurement of actual generation in relation to potential maximum generation on an annual basis. For example, a generator with a 1 MW capacity operating at full capacity for a year (8,760 hours) would produce 8,760 megawatt-hours of electricity. The generator's annual capacity factor would be 100%. New York ISO, *New York's Clean Energy Grid of the Future*, Glossary at 49 (2021), https://www.nyiso.com/documents/20142/2223020/2021-Power-Trends-Report.pdf/471a65f8-4f3a-59f9-4f8c-3d9f2754d7de.

[31] Based on its emissions, it appears that the power plant operated for the three months of 2011 before going offline.

[32] The year before Greenidge changed the operations at the plant to begin mining.

[33] Greenidge Generation Holdings Inc., Sec. & Exch. Comm'n Form S-1, at 2 (Oct. 5, 2021), https://sec.report/Document/0001193125-21-291578/.

[34] *Id*. at 13.

[35] Projected annualized CO2 emissions for 2022, if no more miners are installed. *Id*.

[36] *Id*. at 3.

[37] N.Y. State Dep't of Env't Conservation, Water Withdrawal Permit, DEC Permit No. 8-5736-00004/00015 (effective 09/11/2017), https://treichlerlawoffice.com/water/greenidge/WaterPermit_Final_2017-09-11_.pdf; Seneca Lake Guardian, *Facts Matter: Greenidge Bitcoin Mining Expansion* (Mar. 10, 2021), https://senecalakeguardian.org/Facts-Matter-Greenidge-Bitcoin-Mining.

[38] Letter from Sen. Kirsten Gillibrand to EPA on Greenidge Bitcoin Plant Title V Permit (Sept. 8, 2021), https://www.gillibrand.senate.gov/imo/media/doc/Gillibrand%20Letter%20to%20EPA%20on%20Greenidge%20Bitcoin%20Plant%20Title%20V%20Permit%20-%20Updated.pdf.

[39] Sen. Charles E. Schumer, *Schumer Calls on EPA to Review Air Permit For Greenidge Power Plant Cryptocurrency Mining Facility*, Press Release (Oct. 12, 2021), https://www.schumer.senate.gov/newsroom/press-releases/citing-environmental-concerns-schumer-calls-on-epa-to-review-air-permit-for-greenidge-power-plant-cryptocurrency-mining-facility-senator-reveals-emisions-from-plant-have-recently-increased-tenfold-and-with-ownership-planning-to-expand-virtual-mining-operation-pollution-from-mining-will-only-increase.

[40] Provided by Fossil Free Tompkins (citing NYISO, *2021 Load and Capacity Data*, at 80 (Apr. 2021), https://www.nyiso.com/documents/20142/2226333/2021-Gold-Book-Final-Public.pdf/b08606d7-db88-c04b-b260-ab35c300ed64).

[41] Gavin Donohue, *There's a role for natural gas in the renewable-energy future*, Times Union (Mar. 2, 2021), https://www.timesunion.com/opinion/article/There-s-a-role-for-natural-gas-in-the-15993563.php.

[42] Seneca Lake Guardian, *Gov Hochul + DEC Punt Decision on Greenidge Generation Air Permits Again* (Mar. 31, 2022), https://www.senecalakeguardian.org/index.php?tray=content&tid=1SLGtop4&cid=1SLG141.

[43] Table 1:13 Proof-Of-Work Mining Facilities Currently Operating In New York State. Provided by Fossil Free Tompkins.

[44] *See id.*

[45] NYISO, *Delivering the Grid of the Future How Mkts. Support Climate & Pol'y Goals*, at slide 9, https://www.nyiso.com/documents/20142/2225523/How-Markets-Support-Climate-and-Policy-Goals.pdf (last visited May 3, 2022).

[46] Severin Borenstein, *Crypto Mining for a More Stable Grid?*, Energy Inst. at HAAS (Mar. 21, 2022), https://energyathaas.wordpress.com/2022/03/21/crypto-mining-for-a-more-stable-grid/.

[47] S.B. 6599, 2019–2022 Reg. Sess. (N.Y. 2019).

[48] NYISO, *2019 Congestion Assessment and Res. Integration Study*, at 5–6 (July 24, 2020), https://www.nyiso.com/documents/20142/2226108/2019-CARIS-Phase1-Report-Final.pdf/bcf0ab1a-eac2-0cc3-a2d6-6f374309e961.

[49] Fossil Free Tompkins, Webinar to League of Women Voters, at 48:45 (Jan 13, 202, https://www.youtube.com/watch?v=qIuMqn2ISA4.

[50] NYISO, *Power Trends 2020: The Vision for a Greener Grid*, at 18 (2020), https://www.nyiso.com/documents/20142/2223020/2020-Power-Trends-Report.pdf/dd91ce25-11fe-a14f-52c8-f1a9bd9085c2.

[51] *Id.*

[52] Naureen S. Malik, *Texas Grid's Review of Crypto Miners Connection May Take Months*, Bloomberg (Apr. 4, 2022), https://www.bloomberg.com/news/articles/2022-04-04/texas-grid-s-review-of-crypto-miners-connection-may-take-months.

[53] Notice from Notice_Operations@lists.ercot.com, to Interconnecting Market Participants, Subject: W-A032522-01 Interim Large Load Interconnection Process (Mar. 25, 2022), https://www.ercot.com/services/comm/mkt_notices/detail?id=fc84b65f-72fe-4704-9974-b52974cdb81e.

[54] Bloomberg Wire, *Texas now requiring crypto miners to seek 'approval to energize' before plugging into grid*, Dallas Morning News (Mar. 30, 2022), https://www.dallasnews.com/business/energy/2022/03/30/texas-now-requiring-crypto-miners-to-seek-approval-to-energize-before-plugging-into-grid/; Husch Blackwell LLP, *ERCOT Now Requires Cryptocurrency Miners to Provide Info. on their Impact to the Texas Power Grid*, JDSupra (Apr. 6, 2022), https://www.jdsupra.com/legalnews/ercot-now-requires-cryptocurrency-6065651/.

[55] Severin Borenstein, *Crypto Mining for a More Stable Grid?*, Energy Inst. at HAAS (Mar. 21, 2022), https://energyathaas.wordpress.com/2022/03/21/crypto-mining-for-a-more-stable-grid/ (emphasis added).

[56] While proponents of proof-of-work cryptocurrencies claim that mining makes use of excess renewable generation, thereby reducing curtailment and helping to financially support renewable power development, miners have largely relied on baseload power supplied primarily by fossil fuels. Smart Energy International, *Cryptocurrency mining and renewable energy: Friend or foe?* (May 25, 2021), https://www.smart-energy.com/renewable-energy/cryptocurrency-mining-and-renewable-energy-friend-or-foe/.

[57] According to a 2020 report by the International Energy Agency, solar power now offers the "cheapest electricity in history" with technology cheaper than coal and gas in most major countries, and an estimated 43% increase in solar output expected by 2040. Simon Evans, *Solar is now 'cheapest electricity in history', confirms IEA*, CarbonBrief (Oct. 13, 2020), https://www.carbonbrief.org/solar-is-now-cheapest-electricity-in-history-confirms-iea. Utility-scale solar and wind power costs have dropped 90% and 71% respectively in the last 10 years, now costing less than gas, geothermal, coal, or nuclear. Ula Chrobak, *Solar power got cheap. So why aren't we using it more?*, Popular Science (Oct. 8, 2021), https://www.popsci.com/story/environment/cheap-renewable-energy-vs-fossil-fuels/.

[58] The limited clean renewable energy is also needed for the green hydrogen buildout as presently envisioned by the Biden administration. For clean hydrogen power generation, there cannot be grey or blue hydrogen, only hydrogen powered entirely by renewable energy. *See, e.g.*, Dep't of Energy, *DOE Seeks Public Input on New Hydrogen Hubs, Clean Hydrogen Manufacturing Programs to Decarbonize Industry, Transportation Sectors and Provide Healthier Air for All* (Feb. 15, 2022), https://www.energy.gov/articles/doe-establishes-bipartisan-infrastructure-laws-95-billion-clean-hydrogen-initiatives; *see also* Sasan Saadat & Sara Gersen, *Reclaiming Hydrogen for a Renewable Future: Distinguishing Oil & Gas Industry Spin from Zero-Emission Solutions*, at 24–26, Earthjustice (2021), https://earthjustice.org/sites/default/files/files/hydrogen_earthjustice.pdf (citing Jeffrey Goldmeer et al., Hydrogen as a Fuel for Gas Turbines at 3–4, Gen. Elec. (2021)), https://www.ge.com/content/dam/gepower-new/global/en_US/downloads/gas-new-site/future-of-energy/hydrogen-fuel-for-gas-turbines-gea34979.pdf.

[59] Patrick McGeehan, *Bitcoin Miners Flock to New York's Remote Corners, but Get Chilly Reception*, The New York Times (Sept. 19, 2018), https://www.nytimes.com/2018/09/19/nyregion/bitcoin-mining-new-york-electricity html.

[60] Paul Ciampoli, *Public power can charge cryptocurrency firms higher rates: N.Y. PS, American Public Power Association* (Mar. 16, 2018), https://www.publicpower.org/periodical/article/public-power-can-charge-cryptocurrency-firms-higher-rates-ny-psc.

[61] Keith Benman, *Massena seeks public's input on cryptocurrency mining*, 7 News WWNYTV(Feb. 15, 2022), https://www.wwnytv.com/2022/02/15/massena-seeks-publics-input-cryptocurrency-mining/.

[62] Laura Counts, *Power-hungry cryptominers push up electricity costs for locals*, BerkeleyHass (Aug. 3, 2021), https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-locals/; Mateo Benetton et al., *When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy*, SSRN (May 14, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720.

[63] McKenzie Delisle, *Mining operation moves out of city for winter*, Press-Republican (Nov. 11, 2019), https://www.pressrepublican.com/news/local_news/mining-operation-moves-out-of-city-for-winter/article_4c86c044-4e1e-5ad6-8e6d-0ad19b875e35.html.

[64] Steve Wright, *Testimony before the Subcommittee on Oversight and Investigations, Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains*, at 2 (Jan. 20, 2022), https://energycommerce house.gov/sites/democrats.energycommerce house.gov/files/documents/Witness%20Testimony_Wright_OI_2022.01.20.pdf.

[65] *Id*; Corbin Hiar, *Crypto mining gulps power. Can it help renewable energy?*, E&E News (Jan. 21, 2022), https://subscriber.politicopro.com/article/eenews/2022/01/21/crypto-mining-gulps-power-can-it-help-renewable-energy-285435.

[66] Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid.

[67] Comm. on Energy & Com., Memorandum re Hearing on Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains, at 9 (Jan. 17, 2022), https://energycommerce house.gov/sites/democrats.energycommerce house.gov/files/documents/Briefing%20Memo_OI%20Hearing_2022.01.20.pdf.

[68] State University of New York, Plattsburgh, Dr. Colin Read, Professor of Econ. & Finance, https://www.plattsburgh.edu/academics/schools/business-economics/economics-finance/faculty/read-colin.html (last visited May 4, 2022).

[69] *See* Megan Avakian, *E-waste: An Emerging Health Risk,* Nat'l Inst. of Env't Health Sci. (Feb. 2014), https://www.niehs nih.gov/research/programs/geh/geh_newsletter/2014/2/spotlight/ewaste_an_emerging_health_risk_.cfm; EPA, *Understanding e-waste* ("Without proper standards and enforcement, improper practices may result in public health and environmental concerns, even in countries where processing facilities exist."), https://www.epa.gov/international-cooperation/cleaning-electronic-waste-e-waste (last visited May 4, 2022).

[70] BBC, *Bitcoin mining producing tonnes of waste* (Sep. 20, 2021), https://www.bbc.com/news/technology-58572385; Alex de Vries & Christian Stoll, *Bitcoin's Growing E-waste Problem*, 175 Res., Conservation and Recycling 105901 (Dec. 2021), https://www.sciencedirect.com/science/article/pii/S0921344921005103; Digiconomist, *Bitcoin Electric Waste Monitor*, https://digiconomist net/Bitcoin-electronic-waste-monitor/ (last visited May 4, 2022).

[71] BBC, *Bitcoin Mining Produces Tons of Waste*, (Sep. 20, 2021), https://www.bbc.com/news/technology-58572385.

[72] Mark Peplow, *Bitcoin poses major electronic-waste problem*, Chem. & Eng'g News (Mar. 14, 2019), https://cen.acs.org/environment/sustainability/Bitcoin-poses-major-electronic-waste/97/i11.

[73] Peter Howson & Alex de Vries, *Preying on the poor? Opportunities and challenges for tackling the social and environmental threats of cryptocurrencies for vulnerable and low-income communities*, 84 Energy Research & Social Science 102394 (2022), https://www.sciencedirect.com/science/article/abs/pii/S2214629621004813.

May 9, 2022

Office of Science & Technology Policy
Eisenhower Executive Office Building
[redacted]

Submitted electronically via [redacted]

Re: The Energy and Climate Implications of Digital Assets in Texas

Thank you for the opportunity to provide comments on your Request for Information ("RFI") on the Energy and Climate Implications of Digital Assets. 87 Fed. Reg. 17,105 (Mar. 25, 2022). Please accept these state-specific comments on Texas on behalf of Chispa LCV, Chispa TX, Coastal Bend Group - Sierra Club Lone Star Chapter, Concerned Citizens of Cook County (Georgia), Earthjustice, Environmental Integrity Project, For the Greater Good, FracTracker Alliance, Ingleside on the Bay Coastal Watch Association, Move Past Plastic, Public Citizen, Texas Campaign for the Environment, and Turtle Island Restoration Network. While these comments are 12 pages in length, our footnotes represent five pages of the response, thus still meeting the 10-page limit.

We appreciate the Biden Administration's goals to combat the climate crisis and advance environmental justice by cutting U.S. greenhouse gas pollution by 50–52% below 2005 levels by 2030 and a net-zero emissions economy by 2050. However, as the RFI notes, these goals could be threatened by the climate, energy, and environmental challenges associated with digital assets, in particular proof-of-work cryptocurrencies like Bitcoin, Ethereum, and Dogecoin, among others.

The Scope of the Energy Demand from Proof-of-Work Cryptocurrency Mining in Texas

The impacts of proof-of-work cryptocurrencies are experienced most directly and acutely at the local level, particularly in a state like Texas where cryptomining operations rely on fossil fuel power plants and enable additional fossil fuel production at oil and gas wells by utilizing flared gas. These operations are also utilizing clean renewable energy generation that would otherwise be sent directly to the Texas grid, where it is needed for homes and local businesses.[1]

In addition, as described further below, the enormous load being placed on the Electric Reliability Council of Texas ("ERCOT") grid from proof-of-work mining will have significant impacts on electricity prices and on transmission and distribution infrastructure, which is already unstable—as evidenced most recent and tragically by the Texas Winter Storm in February 2021, in which at least 246 people lost their

[1] The limited clean renewable energy is also needed for the green hydrogen buildout presently being envisioned by the Biden Administration. For clean hydrogen power production, there cannot be grey or blue hydrogen, only hydrogen powered entirely by renewable energy. *See, e.g.*, U.S. Dept. of Energy, *DOE Establishes Bipartisan Infrastructure Law's $9.5 Billion Clean Hydrogen Initiatives* (Feb. 15, 2022), https://www.energy.gov/articles/doe-establishes-bipartisan-infrastructure-laws-95-billion-clean-hydrogen-initiatives; *see also* Sasan Saadat & Sara Gersen, *Reclaiming Hydrogen for a Renewable Future: Distinguishing Oil & Gas Industry Spin from Zero-Emission Solutions*, at 24–26, Earthjustice (2021) (citing Jeffrey Goldmeer et al., *Hydrogen as a Fuel for Gas Turbines*, at 3–4, Gen. Elec. (Sept. 2021), https://www.ge.com/content/dam/gepower-new/global/en_US/downloads/gas-new-site/future-of-energy/hydrogen-fuel-for-gas-turbines-gea34979.pdf), https://earthjustice.org/sites/default/files/files/hydrogen_earthjustice_2021.pdf.

lives,[2] and millions of households were without power in frigid and dire circumstances.[3] Proof-of-work cryptocurrency mining can cause local ratepayer impacts, raising rates for ordinary consumers of electricity, and, worse, potentially leaving ratepayers on the hook to pay for newly installed grid assets when miners pick up and leave. These challenges are not unique to Texas and are being experienced by communities across the United States.

Texas is emerging as the leading state for proof-of-work cryptocurrency mining, with the misguided support of Texas elected officials as well as financing and support from the oil and gas industry.[4] Further, Texas' deregulated power grid, with its abundance of inexpensive power sources and generally lax regulations across the board, have attracted an influx of cryptomining companies.[5]

As described further below, it is estimated that cryptomining operations will require as much as 6 gigawatts ("GW") of additional electricity over the next two years, the same amount as the city of Houston.[6] The amount of miners requesting interconnection is even more than that—17 GW—or as the interim head of described it: "that's about the equivalent of load of two-and-a-half New York Cities."[7] As of March 2022, the Texas Blockchain Council offered that the Lone Star State is home to seven large crypto mining companies and 20 smaller ones.[8] Just one proof-of-work cryptomining company, Greenidge Generation Holdings, will be responsible for 2 GW capacity in Texas alone, with undisclosed

---

[2] Erica Proffer, *Here is why death totals from Winter Storm Uri may vary*, KVUE (Feb. 15, 2022), https://www.kvue.com/article/weather/winter-storm/here-is-why-death-totals-from-winter-storm-uri-may-vary/269-f2bf277f-74d9-443b-ab2e-ff89f336f3ec.

[3] Texas Tribune Staff, *Texas power outages: Nearly half the state experiencing water disruptions as power grid operator says it's making progress*, Texas Tribune (Feb. 18, 2021), https://www.texastribune.org/2021/02/18/texas-winter-storm-power-outage-ercot/; *see also* Mandy Cai et al., *How Texas' power grid failed in 2021 – and who's responsible for preventing a repeat*, Texas Tribune (Feb. 15, 2022), https://www.texastribune.org/2022/02/15/texas-power-grid-winter-storm-2021/.

[4] *See, e.g.*, Kate Aronoff, *Because Oil Drilling Isn't Destructive Enough, ExxonMobil Is Getting Into Bitcoin Mining, Too*, NewRepublic (Mar. 30, 2022), https://newrepublic.com/article/165880/exxon-bitcoin-crypto-climate.

[5] MacKenzie Sigalos, *Bitcoin miners and oil and gas execs mingled at a secretive meetup in Houston – here's what they talked about*, CNBC (Sept. 4, 2021), https://www.cnbc.com/2021/09/04/bitcoin-miners-oil-and-gas-execs-talk-about-natural-gas-mining html; Zach Budryk, *Democrats press cryptomining companies on energy consumption*, The Hill (Jan. 27, 2022), https://thehill.com/policy/energy-environment/591714-eight-congressional-democrats-press-cryptomining-companies-on/.

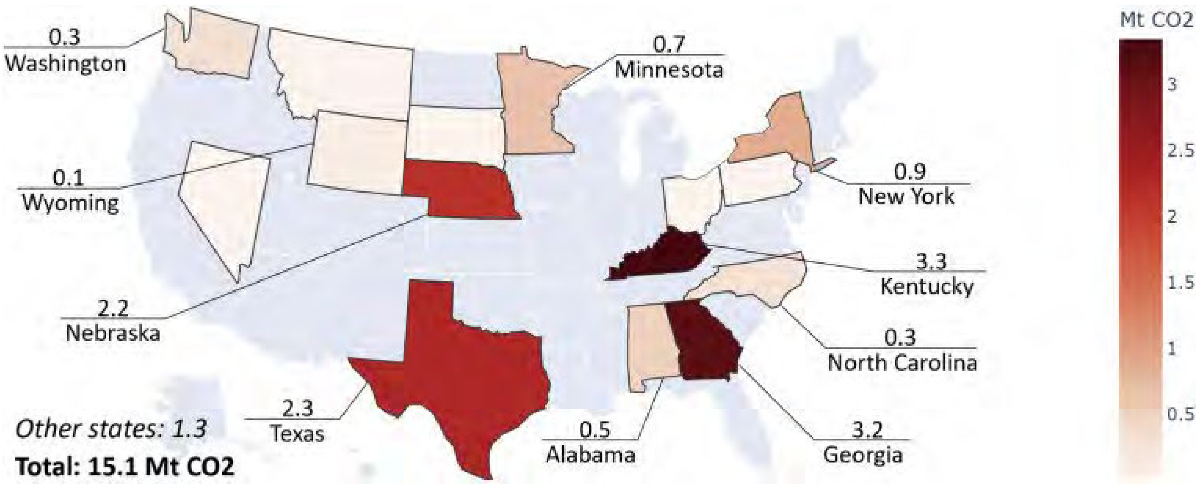
[6] MacKenzie Sigalos, *Bitcoin miners say they're helping to fix the broken Texas energy grid – and Ted Cruz agrees*, CNBC (Dec. 4, 2021), https://www.cnbc.com/2021/12/04/bitcoin-miners-say-theyre-fixing-texas-electric-grid-ted-cruz-agrees.html.

[7] Naureen S. Malik, *Crypto Miners' Elec. Use in Texas Would Equal Another Houston*, Bloomberg (Apr. 27, 2022), https://www.bloomberg.com/news/articles/2022-04-27/crypto-miners-in-texas-will-need-more-power-than-houston.

[8] Chandler France, *Texas bitcoin mining booms, but sustainability, grid concerns remain*, Beaumont Enter. (Mar. 3, 2022), https://www.beaumontenterprise.com/news/article/Bitcoin-mining-on-the-rise-in-Texas-with-27-16967837.php; David Yaffe-Bellany, *Bitcoin Miners Want to Recast Themselves as Eco-Friendly*, New York Times (Mar. 22, 2022), https://www nytimes.com/2022/03/22/technology/bitcoin-miners-environment-crypto.html.

fuel sources or locations.[9] Another publicly-traded proof-of-work cryptomining company, Riot Blockchain, has started the development of a large-scale 1 GW expansion project in Navarro County, TX—once online, Riot will account for 1.7 GW of energy, slightly behind Greenidge Generation.[10]

As of August 2021 (before China banned cryptomining), Texas was home to nearly 15% of the country's proof-of-work cryptocurrency mining operations, and that percentage has increased every day.[11] As the map below shows, the carbon footprint from cryptocurrency mining in Texas alone is estimated at 2.3 megatons of carbon dioxide per year:



[12]

---

[9] Abbie Bennett, *Bitcoin miner Greenidge enters deal for at least 2,000 MW of capacity in Texas*, S&P Global (Oct. 22, 2021) ("The company announced that it was entering an agreement for a development pipeline of at least 2,000 MW of capacity in Texas and another agreement with a company controlling 1,000 MW of power generation in the Electric Reliability Council of Texas Inc. market, according to a news release from the company."), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/bitcoin-miner-greenidge-enters-deal-for-at-least-2-000-mw-of-capacity-in-texas-67222563; Jamie Crawley, *Greenidge Generation to Expand into Texas, Acquire South Carolina Site*, CoinDesk (Oct. 22, 2021), https://www.coindesk.com/business/2021/10/22/greenidge-generation-holdings-to-expand-acquire-sites-in-texas-south-carolina/; Greenidge Generation, *Greenidge Generation Announces Comprehensive Expansion Plans*, at Ex. 99.1 (Oct. 21, 2021), https://www.sec.gov/Archives/edgar/data/1844971/000119312521304493/d221812dex991.htm.

[10] Aoyon Ashraf, *Riot Blockchain to Develop 1GW of Bitcoin Mining Capacity in Texas*, CoinDesk (Apr. 27, 2022), https://www.coindesk.com/business/2022/04/27/riot-blockchain-to-develop-1gw-of-bitcoin-mining-capacity-in-texas/.

[11] MacKenzie Sigalos, *New York and Texas are winning the war to attract bitcoin miners*, CNBC (Oct. 9, 2021), https://www.cnbc.com/2021/10/09/war-to-attract-bitcoin-miners-pits-texas-against-new-york-kentucky html; Avi Asher-Schapiro, *Coal to crypto: The gold rush bringing bitcoin miners to Kentucky*, Thomson Reuters Found. (Mar. 14, 2022) (citing Alex de Vries et al., *Revisiting Bitcoin's carbon footprint*, at Fig. 3, Joule (Feb. 25, 2022), https://www.sciencedirect.com/science/article/abs/pii/S2542435122000861?dgcid=author), https://longreads.trust.org/item/bitcoin-mining-US-coal-country-climate.

[12] Estimated carbon footprint of the Bitcoin network in the United States, as of August 2021. Alex de Vries et al., *Revisiting Bitcoin's carbon footprint*, at Fig. 3, Joule (Feb. 25, 2022), https://www.sciencedirect.com/science/article/abs/pii/S2542435122000861?dgcid=author.

Specific Comments

3. *Resources*

In Texas, there are three primary means by which proof-of-work cryptomining operations occur: (1) cryptomining companies deriving electricity from the grid; (2) cryptomining companies operating at or purchasing power directly from a power plant, often powered by fossil fuels; and (3) cryptomining companies hooking up a generator to underused oil and gas wells that would otherwise not be combusted, or otherwise be flared or vented. In all of these scenarios, these unregulated, energy-intensive, and energy wasteful proof-of-work cryptomining operations[13] serve essentially as a lucrative subsidy to continue fossil fuel extraction and generation—in direct opposition to the climate and environmental justice goals of the Biden Administration and what is needed to prevent the worst of the impacts from the climate crisis.

A. A Rapid Increase in Cryptomining Operations Threatens Texas' Already Strained and Struggling Grid and Everyday Texans' Livelihoods

Perhaps the biggest energy and climate impact of proof-of-work mining in Texas is the strain it puts on the grid, at a time when grid stability and reliability is front of mind for Texans, following the state-wide blackouts in February 2021.

As noted above, ERCOT estimates that proof-of-work cryptomining alone will account for 6 GWs of new demand over the next two years—with peak demand in 2022 7.7% higher than in 2021.[14] Another estimate by an analyst at Wood MacKenzie predicts that bitcoin could more than double demand growth in ERCOT's territory.[15]

Without the sudden increase in cryptomining in ERCOT, in 2018 (pre-cryptomining at a large scale in the U.S.), ERCOT already expected electricity consumption to increase more than 25% from 2018 to 2033.[16] ERCOT has an obligation to provide affordable, reliable, and sustainable electricity to more than 26 million Texas customers, representing 90% of Texas, and the massive amount of demand caused by cryptomining threatens Texas customers on a daily basis.[17]

During the Texas Winter Storm in February 2021, ERCOT instituted rolling blackouts to reduce demand as low temperatures forced power sources, in particular fossil gas, offline more than expected and caused millions of Texans to lose power for days. More than two out of three Texans, 69%, lost electricity at

---

[13] Proof-of-work cryptocurrency mining is often called proof-of-waste. Andrew Tayo, *Proof of work, or proof of waste?*, Hackernoon (Dec. 14, 2017), https://hackernoon.com/proof-of-work-or-proof-of-waste-9c1710b7f025.
[14] Naureen S. Malik, *Crypto Miners' Elec. Use in Texas Would Equal Another Houston*, Bloomberg (Apr. 27, 2022), https://www.bloomberg.com/news/articles/2022-04-27/crypto-miners-in-texas-will-need-more-power-than-houston; Michael Smith, *Texas governor eyes Bitcoin to fortify the elec. grid*, Bloomberg (Jan. 27, 2022), https://www.bloomberg.com/news/articles/2022-01-27/texas-governor-eyes-bitcoin-mining-to-fortify-the-electric-grid.
[15] MacKenzie Sigalos, *Bitcoin miners say they're helping to fix the broken Texas energy grid – and Ted Cruz agrees*, CNBC (Dec. 4, 2021), https://www.cnbc.com/2021/12/04/bitcoin-miners-say-theyre-fixing-texas-electric-grid-ted-cruz-agrees.html.
[16] ERCOT, *2018 Long-term System Assessment for the ERCOT Region* (Dec. 21, 2018), https://www.ercot.com/files/docs/2018/12/21/2018_LTSA_Report.pdf.
[17] *See, e.g.*, Matteo Benetton, *When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Econ.* (May 14, 2021) (noting that in NY as large crypto mining loads came onto the grid, residential and mid-size businesses had to pay significantly more for electricity), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720.

some point during Winter Storm Uri for an average of 42 hours.[18] In fact, ERCOT officials said that Texas was "seconds and minutes" away from catastrophic monthslong blackouts, thus necessitating rolling blackouts over the course of three consecutive days**.**[19] **Put frankly, the Texas grid is not prepared for another catastrophic event**, with or without several additional GW of energy-intensive and energy-wasteful proof-of-work cryptomining on top of new transportation electrification loads expected from additional electric vehicles, trucks, and buses in the coming decade and new renewable energy needed for truly green, clean hydrogen. Even heading into late 2021, an analysis by ERCOT found that four of the five extreme risk scenarios considered by ERCOT would leave the grid short of a significant amount of power, while recognizing that in an average year, "ERCOT anticipates that there will be sufficient installed generating capacity available to serve the system-wide forecasted peak demand."[20] Texans continue to worry: ERCOT issued a winter storm watch in early February 2022, causing uncertainty among everyday Texans.[21]

Because of this immense increase in load from proof-of-work cryptomining operations, ERCOT is instituting additional processes and requirements for new large-scale cryptominers to connect to the state's power grid.[22] On March 25, 2022, ERCOT released a notice[23] instructing utilities to submit studies on the impact of miners and other large users tapping the grid before they can get "approval to energize." ERCOT's new rule applies to both new projects and expansions as well as projects at the site of power generation and projects that do not have their own power generation: any project that will add 20 megawatts ("MW") of demand on the site of a generator within the next two years, and any project that will add 75 MW of demand without its own power generation on site within the next two years, will have to undergo a review process.[24]

Even at the local level, officials are sounding the alarm on grid instability that would be caused by cryptomining operations. For example, the City of Brenham's Planning and Zoning Committee said that the city's current power grid cannot sustain the amount of electricity required for large scale and commercial-like cryptomining set ups, thus necessitating the committee halting the approval of more

---

[18] Chris Stipes, *New Report Details Impact of Winter Storm Uri on Texans*, Univ. of Houston (Mar. 29, 2021), https://uh.edu/news-events/stories/2021/march-2021/03292021-hobby-winter-storm.php.

[19] Erin Douglas, *Texas was "seconds and minutes" away from catastrophic monthslong blackouts, officials say*, Texas Tribune (Feb. 18, 2021), https://www.texastribune.org/2021/02/18/texas-power-outages-ercot/; Kirstin Gibbs et al., *FERC/NERC Report on Winter Storm Uri Recommends Enhanced Cold Weather Preparation*, JDSupra (Sept. 28, 2021) ("The severity of the outages peaked from February 15–18, with the most severe and prolonged effects hitting ERCOT, which experienced three consecutive days of firm load shed—at one point up to 20,000 megawatts."), https://www.jdsupra.com/legalnews/ferc-nerc-report-on-winter-storm-uri-5140527/.

[20] Erin Douglas, *Texas grid vulnerable to blackouts during severe winter weather, even with new preparations, ERCOT estimates show*, Texas Tribune (Nov. 20, 2021), https://www.texastribune.org/2021/11/20/texas-grid-ercot-winter-estimates/; see also ERCOT, *Seasonal Assessment of Resource Adequacy for the ERCOT Region* (SARA) Winter 2021/2022 (Nov. 19, 2021), https://www.ercot.com/files/docs/2021/11/19/SARA_Winter2021-22.pdf.

[21] Mitchell Ferman, *A winter storm is heading to Texas. Here's what that means for the power grid*, Texas Tribune (Feb. 2, 2022), https://www.texastribune.org/2022/02/02/texas-winter-snow-storm-2022-power-grid/.

[22] Naureen S. Malik, *Texas Grid's Review of Crypto Miners Connection May Take Months*, Bloomberg (Apr. 4, 2022), https://www.bloomberg.com/news/articles/2022-04-04/texas-grid-s-review-of-crypto-miners-connection-may-take-months.

[23] ERCOT, *Market Notice re Interim Large Load Interconnection Process* (Mar. 25, 2022), https://www.ercot.com/services/comm/mkt_notices/detail?id=fc84b65f-72fe-4704-9974-b52974cdb81e.

[24] Bloomberg Wire, *Texas now requiring crypto miners to seek 'approval to energize' before plugging into grid*, Dallas Morning News (Mar. 30, 2022), https://www.dallasnews.com/business/energy/2022/03/30/texas-now-requiring-crypto-miners-to-seek-approval-to-energize-before-plugging-into-grid/; Chris Reeder & Miguel Suazo, *ERCOT Now Requires Cryptocurrency Miners to Provide Info. on their Impact to the Texas Power Grid*, JDSupra (Apr. 6, 2022), https://www.jdsupra.com/legalnews/ercot-now-requires-cryptocurrency-6065651/.

mining setups.[25] Further, electric cooperatives and utilities across the state are weighing requests from Bitcoin miners to connect to the grid, which would require millions of dollars in transmission upgrades and associated infrastructure. For example, the Rayburn County Electric Cooperative found that two of the crypto mines interested in connecting to the utility's service territory north and east of Dallas would each require as much as $20 million to fortify power lines and avoid blackouts and consume enough electricity to power as many as 60,000 Texas homes. As explained in Bloomberg, "[u]tilities like Rayburn have to provide service to miners if it's technically feasible to do so, but upgrades to the grid threaten to drive up bills for consumers already shouldering price shocks for almost everything."[26]

Despite this huge impact on the grid, the cryptomining industry has been arguing that proof-of-work cryptomining can "fortify" or "stabilize" the Texas grid. Grid experts are dubious. For example, a recent analysis by Professor Severin Borenstein of UC-Berkeley's Energy Institute at Haas found that "[a]dding demand will just make a grid tighter and increase capacity problems." In addition, it is patently unfair for miners to add enormous new loads on the grid and then seek to be paid, handsomely, to take that load off the grid during emergencies or peak times, at the expense of ratepayers.[27] As explained by Professor Severin Borenstein, "the crypto mining business model is based on buying electricity at wholesale prices or on a real-time variable price tariff. They would already have a strong incentive to cut back during grid emergencies without the additional payments from the demand response program, especially in Texas with its $5000/MWh wholesale price cap. **That means the mining companies get paid for taking demand off the grid that they never would have put on the grid at those high prices anyway**."[28]

---

[25] Morgan Riddell, *Brenham officials discuss cryptocurrency and their ability to sustain energy demands that come with it*, KBTX (Mar. 29, 2022), https://www kbtx.com/2022/03/29/brenham-officials-discuss-cryptocurrency-their-ability-sustain-energy-demands-that-come-with-it/.

[26] Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid.

[27] *See, e.g.*, MacKenzie Sigalos, *Bitcoin miners say they're helping to fix the broken Texas energy grid – and Ted Cruz agrees*, CNBC (Dec. 4, 2021) ("Miners commit to buying a certain amount of power, and either use it for mining if the grid doesn't need it, or sell it back at a profit if the grid demands it."), https://www.cnbc.com/2021/12/04/bitcoin-miners-say-theyre-fixing-texas-electric-grid-ted-cruz-agrees.html; Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022) ("Upgrades to the power system will be needed because the grid 'can't handle all of this new load,' said Evan Caron, a former power trader in Austin who invests in energy technology. New investments in the transmission system are typically shared among Ercot's consumers and show up in their utility bills."), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid; Chris Tomlinson, *Crypto could raise Texas elec. prices if not planned well*, Houston Chronicle (Apr. 15, 2022) ("Crypto-miners often brag they can shut down in five seconds if the grid needs the power, but rising cryptocurrency values make voluntarily 'saving the grid' less attractive. Miners are enrolling in ERCOT programs where they are paid to shut down, creating an additional cost."), https://www.houstonchronicle.com/business/columnists/tomlinson/article/Crypto-could-raise-Texas-electricity-prices-if-17081552.php; Sabrina Toppa, *In Texas, an Influx of Crypto Miners May Mean Higher Elec. Bills for Consumers*, The Street (Mar. 16, 2022) (explaining that "upgrades to the local electricity grid may soon involve an increase in electricity fees for consumers across the Lone Star state"), https://www.thestreet.com/crypto/news/in-texas-the-influx-of-crypto-miners-may-mean-higher-electricity-bills; Karin Rives, *Crypto mining industry's greening campaign raises new questions*, S&P Global (May 4, 2022) ("[C]oncerns are growing that the industry could be using too much of the state's wind capacity and could drive up power prices for homes and businesses."), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/crypto-mining-industry-s-greening-campaign-raises-new-questions-69679254; *see also* Ariana Garcia, *Can Texas' Power Grid Withstand Cryptocurrency Mining?*, Governing (Nov. 2, 2021), https://www.governing.com/next/can-texas-power-grid-withstand-cryptocurrency-mining.

[28] Severin Borenstein, *Crypto Mining for a More Stable Grid?*, Energy Inst. at Haas (Mar. 21, 2022) (emphasis added), https://energyathaas.wordpress.com/2022/03/21/crypto-mining-for-a-more-stable-grid/.

A primary takeaway of his analysis is that paying cryptomining for demand response is likely to encourage even more cryptomining. And the industry points to outlier events like they are the norm, which they are not. For example, Bloomberg recently reported that Texas' largest Bitcoin miner, Riot Blockchain, voluntarily began to reduce power to Bitcoin mining rigs at its Whinstone facility, which typically uses enough electricity to power about 60,000 homes.[29] Using ratepayer money, ERCOT pays miners when they are asked to shut down or curtail power use, bankrolling an energy-intensive industry. During the summer of 2021, ERCOT asked residents to reduce their electricity usage for almost a week due to "tight" power grid operations.[30]

B. Proof-of-work Cryptomining Companies Use Energy from Fossil Fuel Power Plants

There is also a number of fossil fuel plants directly contracting with cryptomining companies, often with discounted prices, generating a massive amount of money for these companies at the expense of local communities who directly face the toxic air and water pollution associated with fossil-fueled power generation.

Most recently, Bootstrap Energy received approval by the City of Corpus Christi in April 2022 to expand its Industrial District Agreement[31] to install a $1.1 billion cryptomining operation.[32] Phase 1 of the project includes a partnership with Bootstrap and Compute North, a cryptomining data center provider, which

---

[29] Michael Smith, *Biggest Texas Bitcoin Miner Shuts Down Ahead of Cold Blast*, Bloomberg (Feb. 2, 2022), https://www.bloomberg.com/news/articles/2022-02-02/biggest-bitcoin-miner-in-texas-will-shut-for-cold-blast-if-asked.

[30] Erin Douglas & Mitchell Ferman, *Is Texas headed toward another blackout? Did the Legislature fix the power grid? Here are answers to your questions about the grid*, Texas Tribune (June 15, 2021), https://www.texastribune.org/2021/06/15/texas-power-grid-ercot/.

[31] City of Corpus Christi, Ordinance No. 22-0485 (Apr. 12, 2022), https://corpuschristi.legistar.com/ViewReport.ashx?M=R&N=Master&GID=212&ID=5532494&GUID=F51C6F1B-FD1A-4FF1-BC6D-D42FF12EC5B9&Extra=WithText&Title=Legislation+Details+(With+Text); Alecia Ormsby, *Bitcoin generator coming to Corpus Christi*, Corpus Christi Business News (Apr. 20, 2022), https://www.ccbiznews.com/bitcoin-generator-moving-to-corpus-christi.

[32] To the extent that hydrogen is being proposed to be a new fuel source at these natural gas plants, the gas-hydrogen blend creates additional harmful local pollution with modest CO_2 reductions, absent significant advances in emission control technology. For example, a 10 percent hydrogen blend, which is all the current Proposed Project could accomplish without major modifications, would only result in 3 percent CO_2 emissions savings. *See* Jeffrey Goldmeer, *Power to Gas: Hydrogen for Power Generation*, Gen. Elec. (Feb. 2019), https://www.ge.com/content/dam/gepower/global/en_US/documents/fuel-flexibility/GEA33861%20Power%20to%20Gas%20-%20Hydrogen%20for%20Power%20Generation.pdf. Even 100 percent hydrogen has greenhouse gas emissions, particularly when the gas leaks, as it is prone to do. Justin Mikulka, *Decoding the Hype Behind the Nat. Gas Industry's Hydrogen Push*, Desmog Blog (Jan. 14, 2021) (citing Zahreddine Hafsi et al., *Hydrogen Embrittlement of Steel Pipelines During Transients*, 13 Procedia Structural Integrity 210 (2018)), https://www.desmog.com/2021/01/14/decoding-hype-behind-natural-gas-industry-hydrogen-push/. Unburned, leaked hydrogen is a potent GHG, "100 times more potent than CO_2 emissions over a 10-year period (for equal emissions annually during this time)." *Id.* (citing Zahreddine Hafsi et al., *Hydrogen embrittlement of steel pipelines during transients*, 13 Procedia Structural Integrity 210 (2018)). Local air quality and local public health outcomes will worsen with hydrogen combustion. For example, a study conducted by General Electric on its combustion turbines found that a 50/50 mixture of hydrogen and fossil gas (by volume) increased concentrations of NO_x in gas exhaust by 35 percent. Jeffrey Goldmeer et al., *Hydrogen as a Fuel for Gas Turbines*, at 5, Gen. Elec. (Sept. 2021), https://www.ge.com/content/dam/gepower-new/global/en_US/downloads/gas-new-site/future-of-energy/hydrogen-fuel-for-gas-turbines-gea34979.pdf. NO_x does significant damage to the respiratory system over time. In areas affected by smog resulting from NO_x emissions, symptoms including coughing, increased rates of asthma, and comorbidities with other respiratory illness develop. Resp. of Clean Energy Group to DOE Hydrogen Program Req. for Information #DE-FOA-0002529, at 3 (July 7, 2021), https://www.cleanegroup.org/wp-content/uploads/CEG-Response-to-DOE-Hydrogen-RFI.pdf.

will build, own, and operate approximately 150 containers, which collectively require 300 MW to mine bitcoin.[33] Already, Bootstrap has contracted with AEP Texas for 600 MW.[34] In addition to the massive amount of electricity that this project will require, the City of Corpus Christi is forgoing $7 million annually in sales tax and franchise fees, equating to $70,501,509 over ten years.[35]

For example, Cipher Mining, a publicly traded company, announced a 200 MW power purchase contract in October 2021 with Vistra, most likely at Vistra's 1,054 MW Odessa gas-fired plant.[36] There are countless other examples of announcements by cryptomining companies signing power purchase agreements with energy providers that generate electricity from fossil fuel production at rates significantly lower than available to Texas residents.

C. Cryptomining Operations are Incentivizing Additional Extraction and Combustion of Fossil Fuels

Many cryptomining companies are utilizing electricity generated from combusting gas at well pads that otherwise could be used for more societally beneficial uses, especially as fossil gas prices continue to rise,[37] putting households and business' bottom lines in jeopardy. This further incentivizes the practice of flaring gas, rather than capturing as much gas as possible—directly placing harmful and toxic air pollution into local communities and adding climate-warming pollution into the atmosphere. Examples of this in Texas and throughout the west abound.[38]

[33] Bootstrap Energy, Project Corpus Christi Energy Park, at slide 9 (Mar. 25, 2022), https://corpuschristi.legistar.com/View.ashx?M=F&ID=10675758&GUID=10B47135-9684-416F-A8C0-D46E8AA2B5AE.

[34] City of Corpus Christi, Agenda Memorandum from Ian Vasey and Andrea Gardner to Peter Zanoni re Disannexation and Amendment Industrial District #2 Boundaries, at 2 (Mar. 3, 2022), https://corpuschristi.legistar.com/View.ashx?M=F&ID=10666001&GUID=E7BE68AC-B0F7-4198-B758-739D20E1814D.

[35] Bootstrap Energy, Project Corpus Christi Energy Park, at slides 22–24 (Mar. 25, 2022), https://corpuschristi.legistar.com/View.ashx?M=F&ID=10675758&GUID=10B47135-9684-416F-A8C0-D46E8AA2B5AE; *see also* City of Corpus Christi, Agenda Memorandum from Ian Vasey and Andrea Gardner to Peter Zanoni re Disannexation and Amendment Industrial District #2 Boundaries, at 2 (Mar. 3, 2022) ("However, staff's financial analysis concludes the City will forego $70,501,509 over a ten-year period if the same development were constructed and operated outside of an Industrial District Agreement in the city limits.").

[36] Eliza Gkristi, *Cipher Mining Scraps Plan to Buy Bitfury Rigs, Sticks With Bitmain, MicroBT*, CoinDesk (Mar. 4, 2022), https://www.coindesk.com/business/2022/03/04/cipher-mining-scraps-plan-to-buy-bitfury-rigs-sticks-with-bitmain-microbt/; *see also* Cipher Mining, S-4 Registration Statement, at Exh. 10-26, Purchase and Sale Agreement, U.S. Securities & Exchange Commission, (June 28, 2021), https://www.sec.gov/Archives/edgar/data/0001819989/000119312521224426/d127963ds4a.htm. While the name of Vistra's power plant is redacted, the "1,054 megawatt natural gas fired electric generating facility" is most likely Vistra's Odessa gas plant.

[37] Patti Domm, *Nat. gas prices are rising and could be the most expensive in 13 years this winter*, CNBC (Sept. 9, 2021), https://www.cnbc.com/2021/09/09/natural-gas-prices-are-rising-and-could-be-the-most-expensive-in-13-years-this-winter html.

[38] Audrey Carleton, Inside a Bitcoin Mine at a Nat. Gas Well in Texas, Vice (Mar. 17, 2022), https://www.vice.com/en/article/m7v49n/inside-a-bitcoin-mine-at-a-natural-gas-well-in-texas; MacKenzie Sigalos, *These 23-year-old Texans made $4 million last year mining bitcoin off flare gas from oil drilling*, CNBC (Feb. 12, 2022), https://www.cnbc.com/2022/02/12/23-year-old-texans-made-4-million-mining-bitcoin-off-flared-natural-gas.html; *see also* Seth Tupper, *Orphaned South Dakota Gas Wells Could Soon Power Bitcoin Mining*, South Dakota Pub. Broadcasting (Feb. 24, 2021), https://listen.sdpb.org/business/2021-02-24/orphaned-south-dakota-gas-wells-could-soon-power-bitcoin-mining.

Some cryptomining companies claim that they are a beneficial end-user of gas that would otherwise be flared or vented directly into the atmosphere.[39] In reality, these operations are further enabling oil and gas extraction at a time when we need to be rapidly decreasing our oil and gas consumption, per multiple reports by international organizations like the Intergovernmental Panel on Climate Change ("IPCC")[40] and International Energy Agency ("IEA") in order to meet the real and existential challenge of the climate crisis.[41] Oil and gas companies should be incentivized to capture and pipe as much of the oil and gas they extract as possible, ensuring that said oil and gas does not leak or spill while in transit,[42] which directly aligns with the U.S. Environmental Protection Agency's ("EPA") recently released proposed rule to ensure the capture of gas for beneficial use rather than flaring.[43] As the Biden Administration offered upon the launch of the Global Methane Pledge, "[r]apidly reducing methane emissions is complementary

---

[39] *See, e.g.*, Sergio Chapa, *Cryptocurrency mining company eyes flared gas in Permian Basin*, Houston Chronicle (June 23, 2020) (EZ Blockchain installs mobile computer rigs in Texas's oil and gas fields, powering their mining operations with natural gas that would otherwise be flared.), https://www.houstonchronicle.com/business/energy/article/Cryptocurrency-mining-company-eyes-flared-gas-in-15359750.php; Crusoe Energy, *Understanding the Problem Crusoe Solves* (Sept. 23, 2021), https://www.crusoeenergy.com/blog/3MyNTKiT6wqsEWKhP0BeY/understanding-the-problem-crusoe-solves.

[40] IPCC Newsroom, *The evidence is clear: the time for action is now. We can halve emissions by 2030.* (Apr. 4, 2022) (quoting IPCC Working Group III Co-Chair Jim Skea, "It's now or never, if we want to limit global warming to 1.5°C (2.7°F)…Without immediate and deep emissions reductions across all sectors, it will be impossible."), https://www.ipcc.ch/2022/04/04/ipcc-ar6-wgiii-pressrelease/; Damian Carrington, *It's over for fossil fuels: IPCC spells out what's needed to avert climate disaster*, The Guardian (Apr. 4, 2022) (quoting UN Secretary General, António Guterres, "Increasing fossil fuel production will only make matters worse…It is time to stop burning our planet, and start investing in the abundant renewable energy all around us."), https://www.theguardian.com/environment/2022/apr/04/its-over-for-fossil-fuels-ipcc-spells-out-whats-needed-to-avert-climate-disaster; Lina Tran & Joseph Winters, *'We are at a crossroads': New IPCC report says it's fossil fuels or our future*, Grist (Apr. 4, 2022), https://grist.org/science/we-are-at-a-crossroads-new-ipcc-report-says-its-fossil-fuels-or-our-future/.

[41] IEA, *Net Zero by 2050: A Roadmap for the Global Energy Sector* (May 2021) ("A rapid shift away from fossil fuels. Net zero means huge declines in the use of coal, oil and gas. This requires steps such as halting sales of new internal combustion engine passenger cars by 2035, and phasing out all unabated coal and oil power plants by 2040.") (scroll down on linked page), https://www.iea.org/reports/net-zero-by-2050; Fiona Harvey, *No new oil, gas or coal development if world is to reach net zero by 2050, says world energy body*, The Guardian (May 18, 2021), https://www.theguardian.com/environment/2021/may/18/no-new-investment-in-fossil-fuels-demands-top-energy-economist.

[42] *See, e.g.*, Dan Charles, *A satellite finds massive methane leaks from gas pipelines*, NPR (Feb. 3, 2022) (citing a paper that found over the course of two years, during 2019 and 2020, there were more than 1,800 large bursts of methane, often releasing several tons of methane per hour), https://www.npr.org/2022/02/03/1077392791/a-satellite-finds-massive-methane-leaks-from-gas-pipelines; Morgan McFall-Johnsen, *Views from space reveal huge methane leaks in the US and Asia. They could be easy spots to cut emissions and save money*, Business Insider (Feb. 3, 2022), https://www.businessinsider.com/space-imagery-reveals-methane-pouring-from-the-us-russia-daily-2022-2; Leah Burrows, *Leaky natural gas pipelines are tip of the iceberg*, Harvard Gazette (Oct. 26, 2021) (citing research by the Harvard John A. Paulson School of Engineering and Applied Sciences that found "[m]ethane emissions from the distribution and use of natural gas across U.S. cities are 2 to 10 times higher than recent estimates from the Environmental Protection Agency"), https://news harvard.edu/gazette/story/2021/10/urban-areas-across-u-s-are-undercounting-greenhouse-gas-emissions/.

[43] EPA, Standards of Performance for New, Reconstructed, and Modified Sources and Emissions Guidelines for Existing Sources: Oil and Natural Gas Sector Climate Review, 86 Fed. Reg. 63110, 63116 (Nov. 15, 2021) ("The EPA is also seeking input on ways to ensure that captured associated gas is collected for a useful purpose rather than flared."), https://www federalregister.gov/documents/2021/11/15/2021-24202/standards-of-performance-for-new-reconstructed-and-modified-sources-and-emissions-guidelines-for; *see also* EPA, *U.S. to Sharply Cut Methane Pollution that Threatens the Climate and Public Health* (Nov. 2, 2021) ("Key features of the proposed rule include…standards to eliminate venting of associated gas, and require capture and sale of gas where a sales line is available, at new and existing oil wells."), https://www.epa.gov/newsreleases/us-sharply-cut-methane-pollution-threatens-climate-and-public-health.

to action on carbon dioxide and other greenhouse gases, and is regarded as the single most effective strategy to reduce global warming in the near term and keep the goal of limiting warming to 1.5 degrees Celsius within reach."[44] Instead, cryptomining operations take the economics of flared gas in the *opposite* direction, by further rewarding and subsidizing an industry that already receives subsidies from taxpayers while harming local communities and the planet.[45]

4. *Economics*

Energy-intensive proof-of-work mining companies often point to two primary arguments as to why they benefit Texas economically. First, they claim that the lucrative crypto industry can increase renewable energy development. In actuality, cryptomining companies are predominantly utilizing fossil fuel generation, and often times resurrecting and elongating the lifespan of dirty fossil fuel power plants, to mine for cryptocurrency. And even where clean, renewable energy technologies like solar or wind are being used to mine, many operations do not have commitments for renewable-only power supply and instead continue to mine when the sun is not shining nor the wind blowing, using the grid or natural gas, since these operations are 24/7/365. Further, considering how volatile the cryptocurrency market is and the fact that cryptomining companies come and go, there are serious implications for what happens when a cryptomining rig leaves the area and the economics of the renewable energy project means that it is unable to properly compete in an open market and potentially becomes stranded. In places like New York,[46] ratepayers have had to pick up the bill, and this is becoming a concern in Texas as more and more cryptomining operations attempt to plug into the grid.[47]

Regardless of cryptocurrency operations that supposedly promise increased renewable energy deployment, renewable energy is already low-cost in Texas and throughout the U.S. Texas led the country in new renewable energy capacity in 2021, boasting 7,352 MWs of new wind, solar, and energy storage.[48]

---

[44] The White House, *Joint US-EU Press Release on the Global Methane Pledge* (Sept. 18, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/18/joint-us-eu-press-release-on-the-global-methane-pledge/.

[45] Justine Calma, *Why fossil fuel companies see green in Bitcoin mining projects*, The Verge (May 4, 2022) (quoting Professor Paasha Mahdavi of University of California, Santa Barbara, "This is basically a way to monetize flaring. It's not a way to stop flaring."), https://theverge.com/2022/5/4/23055761/exxonmobil-cryptomining-bitcoin-methane-gas.

[46] For a fuller discussion of the economic and ratepayer impacts on local residents and municipalities in New York, we refer to the comments being simultaneously submitted by Dr. Colin Read. *See* State Univ. of New York, Plattsburgh, Dr. Colin Read, Professor of Econ. & Finance, https://www.plattsburgh.edu/academics/schools/business-economics/economics-finance/faculty/read-colin.html (last visited May 4, 2022).

[47] Naureen S. Malik & Michael Smith, *Crypto Mania in Texas Risks New Costs and Strains on Shaky Grid*, Bloomberg (Mar. 15, 2022), https://www.bloomberg.com/news/articles/2022-03-15/crypto-mania-in-texas-risks-new-costs-and-strains-on-shaky-grid ("Given the crypto industry's notorious volatility, there's also the chance that miners will close up shop, leaving ratepayers to cover the costs of upgrades that may no longer be needed."); see also Fitch Ratings, Crypto Mining Poses Challenges to Public Power Utilities (Jan. 24, 2022), https://www.fitchratings.com/research/us-public-finance/crypto-mining-poses-challenges-to-public-power-utilities-24-01-2022 ("The first two of these three options pose the greatest risk to the utility should the crypto mining operation shut down, as utilities could be left with stranded assets and costs that then must be recovered.").

[48] American Clean Power Ass'n, *U.S. surpasses 200 gigawatts of total clean power capacity, but the pace of deployment has slowed according to ACP 4Q report* (Feb. 15, 2022), https://cleanpower.org/news/u-s-surpasses-200-gigawatts-of-total-clean-power-capacity-but-the-pace-of-deployment-has-slowed-according-to-acp-4q-report/; Dan Gearino, *Inside Clean Energy: Texas Is the Country's Clean Energy Leader, Almost in Spite of Itself*, Inside Climate News (Feb. 17, 2022), https://insideclimatenews.org/news/17022022/inside-clean-energy-texas-clean-energy-leader/.

In 2020, wind and solar accounted for 25.2% of power generation, growing steadily from 7.8% in 2010.[49] Even if cryptomining companies only used excess renewable energy that would otherwise be curtailed, there are serious implications with wasting energy at a time when we need to be placing that energy in energy storage technologies for dispatch at peak usage times by deploying more energy efficiency technologies. While the interim CEO of ERCOT, Brad Jones, described himself as "pro bitcoin," it is worth noting that was specifically in the context only of excess solar and wind, in which cryptominers would actually get paid to use power if the price per megawatt hour goes negative.[50]

The second argument for proof-of-work crypto's purported economic value is a claim that because miners are able to ramp up and down cryptomining operations when the grid may be strained, they can safeguard the grid's reliability. However, if the curtailment of crypto electric usage comes through demand response and load reduction programs, as discussed above, in addition to already receiving massive amounts of money through mining cryptocurrencies like Bitcoin and then incentives from local and state governments, ratepayers are then on the hook for paying cryptomining companies through demand response programs, an unjustified double subsidy.

A. Subsidies from taxpayers to small amount of wealthy miners

Because of the immense amount of capital needed to purchase enough ASIC miners[51] to mine bitcoin, there are actually very few miners today compared to even a few years ago. In 2021, a whitepaper published by the National Bureau of Economic Research found that the top 10% of cryptominers control 90% of mining and just 0.1% (about 50 miners) control close 50% of the mining—which directly translates to ownership of Bitcoin.[52]

And miners combusting fossil fuels seek even more handouts from taxpayers. The industry is lobbying state lawmakers to introduce legislation that would eliminate the taxes on sales of stranded gas, which is currently set at 7.5% of market value for fossil gas in Texas.[53] While the cryptocurrency industry will have to wait until the 2023 Texas legislative session to pass more crypto-friendly legislation like North Dakota, Wyoming, and Kentucky, the Texas Legislature already passed House Bill 4474 to recognize

---

[49] Garrett Golding, *Surging Renewable Energy in Texas Prompts Electricity Generation Adequacy Questions*, Federal Reserve Bank of Dallas (Aug. 17, 2021) (percentages calculated using chart data for Figure 1) (citing data from ERCOT), https://www.dallasfed.org/research/economics/2021/0817.
[50] MacKenzie Sigalos, *Bitcoin miners say they're helping to fix the broken Texas energy grid – and Ted Cruz agrees*, CNBC (Dec. 4, 2021), https://www.cnbc.com/2021/12/04/bitcoin-miners-say-theyre-fixing-texas-electric-grid-ted-cruz-agrees.html.
[51] Paul Kim, *ASIC mining: Computers built specifically for mining cryptocurrency*, Insider (Mar. 16, 2022), https://www.businessinsider.com/personal-finance/asic-mining.
[52] Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market*, at 22–23, Nat'l Bureau of Econ. Rsch., Working Paper 29396 (Oct. 2021) (note: this analysis was for the time period before China banned mining), https://www.nber.org/system/files/working_papers/w29396/w29396.pdf. It is believed that the concentration of mining and wealth is even more stark in the U.S. today.
[53] Bloomberg, *Texas bitcoin miners sketch a future of cozying up to gas wells*, E&E News (Apr. 1, 2022), https://subscriber.politicopro.com/article/eenews/2022/04/01/texas-bitcoin-miners-sketch-a-future-of-cozying-up-to-gas-wells-00022124; *see also* Texas Railroad Commission, *Texas Severance Tax Incentives*, https://www.rrc.texas.gov/oil-and-gas/publications-and-notices/texas-severance-tax-incentives (last visited May 5, 2022); Shelly Hagan & Michael Smith, *Texas Bitcoin miners seek tax break for using trapped well gas*, World Oil (Mar. 31, 2022), https://www.worldoil.com/news/2022/3/31/texas-bitcoin-miners-seek-tax-break-for-using-trapped-well-gas/.

cryptocurrency in the state's Uniform Commercial Code as well as enacted House Bill 1576 to establish a 16-member working group on blockchain matters.[54]

Conclusion

Texas is ground-zero for where proof-of-work cryptomining operations are located—the externalities of which are being placed on everyday Texans who are still concerned about grid stability, reliability, and affordability after the lethal Texas Winter Storm in February 2021 that took the lives of 246 people and left millions of households without power in frigid and dire circumstances. The massive amount of energy unnecessarily required by proof-of-work cryptomining, which operates intentionally as an energy-wasteful industry, threatens the United States' ability to meet the Biden Administration's goal of enabling a swift and equitable transition away from a fossil fuel economy through deployment of zero-emissions, renewable energy to power our grid, transportation, and buildings. As more and more communities face the public health, noise, ratepayer, environmental, energy, and climate impacts associated with energy-intensive, energy-wasteful proof-of-work cryptocurrency, the Biden Administration must take a holistic approach to ensuring that this industry does not exacerbate social inequities and environmental injustice—and is held accountable for the destructive actions it continues to take at the expense of communities. Unfortunately, the states with the most cryptomining operations, like Texas, also have the weakest state environmental laws and energy regulations, and lax enforcement. The federal government should explore options at its disposal to ensure that proof-of-work cryptocurrency does not continue to threaten the Biden Administration's climate, environmental, and energy goals.

Thank you for the opportunity to submit these comments and for your attention to this issue. Sincerely,

Chispa LCV

Chispa TX

Coastal Bend Group - Sierra Club Lone Star Chapter

Concerned Citizens of Cook County (Georgia)

Earthjustice

Environmental Integrity Project

For the Greater Good

FracTracker Alliance

Ingleside on the Bay Coastal Watch Association

Move Past Plastic

Public Citizen

Texas Campaign for the Environment

Turtle Island Restoration Network

---

[54] James Pollard, *Texas Republicans want to make the state the center of the cryptocurrency universe*, The Texas Tribune (Oct. 28, 2021), https://www.texastribune.org/2021/10/28/texas-republicans-blockchain-bitcoin/.

May 9, 2022

Office of Science & Technology Policy
Eisenhower Executive Office Building
[redacted]
Submitted electronically via [redacted]

Re: Request for Information on the Energy and Climate Implications of Digital Assets in Montana

Thank you for the opportunity to provide comments on your Request for Information ("RFI") on the Energy and Climate Implications of Digital Assets (87 Fed. Reg. 17105). Please accept these state-specific comments for Montana on behalf of the Montana Environmental Information Center, Montana Conservation Voters Education Fund, Climate Smart Missoula, the Montana Chapter of the Sierra Club, Moms Clean Air Force, Park County Environmental Counsel, Montana Health Professionals for a Healthy Climate, and Earthjustice.

General Comments

We appreciate the Biden Administration's goals to combat the climate crisis and advance environmental justice by cutting U.S. greenhouse gas pollution by 50-52% by 2030 and having a net-zero emissions economy by 2050. However, as the RFI notes, these goals could be threatened by the climate, energy, and environmental challenges associated with digital assets, in particular proof-of-work cryptocurrencies such as Bitcoin.

Proof-of-work cryptocurrencies pose a threat to the Biden Administration's climate, clean energy, and environmental justice goals. Those impacts are experienced most directly and acutely at the local level, in particular in a state such as Montana where cryptomining operations have resurrected fossil fuel power plants, enabled fossil fuel production at oil and gas well pads by utilizing flared gas as opposed to enabling capturing for beneficial use, and threatened decarbonization goals by mining Bitcoin through renewable energy generation that would otherwise be injected directly into the grid. Further, proof-of-work cryptocurrency mining can have local ratepayer impacts, potentially leaving ratepayers on the hook when corporate cryptomining companies pick up and leave, in addition to straining the grid from being able to keep the lights on, which in Montana poses a unique problem considering the rural nature of the state's major utility's service territory. To illuminate the impacts currently being experienced by communities at the local level, these comments focus on the climate and energy impacts of proof-of-work cryptocurrency in Montana.

These challenges are not unique to Montana; communities and the environment are being threatened across the United States.

Specific Comments

3. *Resources*

Montana is home to some of the dirtiest and most polluting proof-of-work cryptocurrency mining operations in the country, including mining using energy directly from a coal plant, utilizing electricity from a grid that relies heavily on dirty coal generation, and incentivizing additional oil & gas extraction (a process that is environmentally destructive and climate harming) by mining using fracked methane gas, rather than capturing the gas for more beneficial uses for Montana households and businesses.

Hardin Coal Plant

There are several examples of proof-of-work cryptomining operations resurrecting and elongating the lifespans of toxic fossil fuel power plants across the country, and Montana is home to one of the most well-documented facilities. The Hardin Generating Station, a 115-megawatt ("MW") coal-fired power plant just north of the Crow Indian Reservation in Big Horn County, Montana, found new life supplying power to Marathon Digital Holdings, a publicly-traded cryptomining company. Before its newfound existence to mine Bitcoin, the plant operated only infrequently between 2017 and 2021 and had been slated to close permanently in 2018.[1] However, in late 2020, Marathon announced a partnership with the plant's operator, Beowulf Energy, to utilize roughly 37 MW of power from the plant to mine Bitcoin around the clock.

Before cryptomining operations ramped up at Hardin, an analysis by Montana Environmental Information Center found that the plant generated power for just 75 days on average from 2017 through 2020, though in 2021, the plant operated on 323 days.[2] Since the last half of 2021, the plant has been operating at or near full capacity, 24 hours a day, and its emissions of NOx, SO_2, and CO_2 have increased accordingly—as demonstrated in the table below.[3]

As the table below shows, according to the U.S. Environmental Protection Agency's Clean Air Markets Program Data, because of the ramp up at the Hardin Generation Station to mine Bitcoin in 2021 compared to the prior year, nitrogen oxides ("NOx") emissions increased **842%**, sulfur dioxide ("SO_2") emissions increased **508%**, and carbon dioxide ("CO_2") emissions increased **850%**.

Hardin Generating Station Operational and Emissions Data from 2017 to 2021[4]

Year	**Operating Time,** hours per year	**CO_2,** short tons per year	**NOx,** tons per year	**SO_2,** tons per year
2017	1,379	169,936	66	72
2018	2,011	227,407	93	109
2019	1,930	231,132	78	115
2020	828	79,516	26	50
2021	**7,449**	**755,670**	**245**	**304**

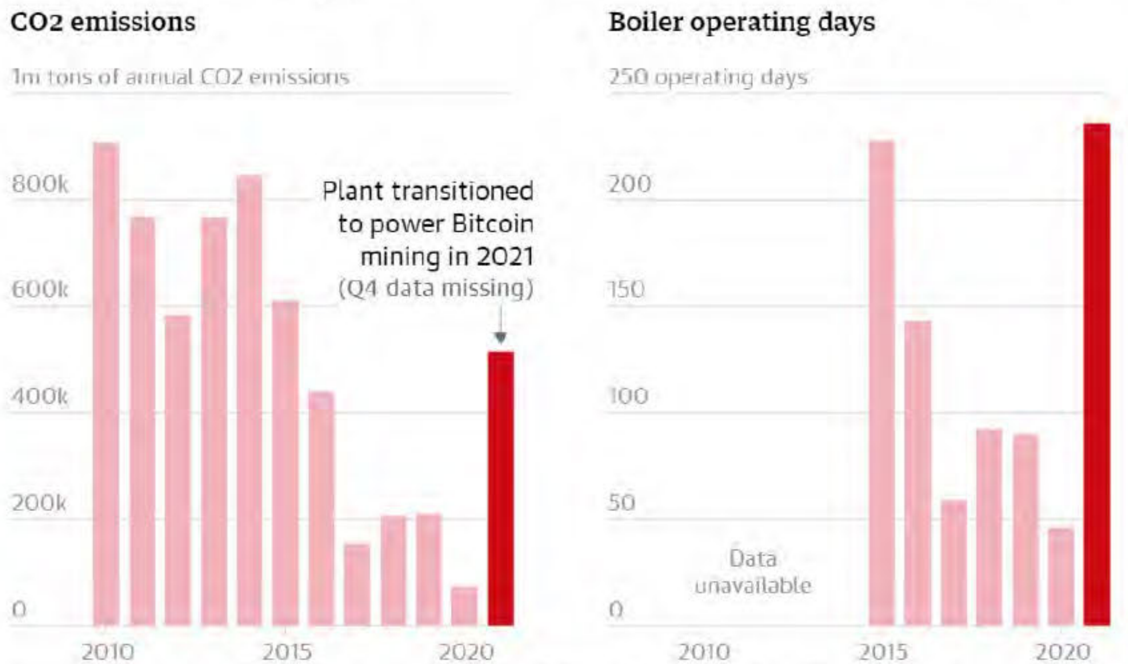
[1] Alex Alley, Bitcoin miner Marathon signs for coal-fired electricity in Montana, Data Center Dynamics (Oct. 16, 2020), https://www.datacenterdynamics.com/en/news/bitcoin-miner-marathon-signs-coal-fired-electricity-montana/.

[2] Data compiled from Heorot quarterly air monitoring reports filed with the Montana Department of Environmental Quality.

[3] Montana Environmental Information Center et al., Comments on Montana's Proposed Regional Haze State Implementation Plan for the 2nd Implementation Period (Mar. 21, 2022), https://protectnps.org/wp-content/uploads/2022/03/Combined-MT-Regional-Haze-R2-Comment-Letter-Exhibits-2022-3-21_reduced-file-size.pdf; see also Victoria R. Stamper, Review and Comments on Reasonable Progress Four-Factor Analyses for Sulfur Dioxide and Nitrogen Oxide Pollution Controls Evaluated as Part of the Montana Regional Haze Plan for the Second Implementation Period, at 47–48 (Mar. 2022) (Exhibit A).

[4] Data from EPA's Air Markets Program Database, https://ampd.epa.gov/ampd/; see also Montana Environmental Information Center et al., Comments on Montana's Proposed Regional Haze State Implementation Plan for the 2nd Implementation Period (Mar. 21, 2022), https://protectnps.org/wp-content/uploads/2022/03/Combined-MT-Regional-Haze-R2-Comment-Letter-Exhibits-2022-3-21_reduced-file-size.pdf.

Shown differently, when the Hardin plant re-powered to mine Bitcoin, harmful local air pollution and greenhouse gas emissions spiked.[5]



Guardian graphic. Sources: Emissions from EPA, boiler activity compiled by the Montana Environmental Information Center from reports submitted to the Montana Department of Environmental Quality.

To demonstrate how crucial coal-fired generation at the Hardin plant was for Marathon's business viability, when the plant went offline in November 2021 for upgrades and maintenance, Marathon offered that this substantially reduced the company's ability to produce Bitcoin. For example, Marathon's total network hash rate (i.e., the number of Bitcoin produced in a given month) fell from 417.7 in October 2021 to 196 in November 2021, demonstrating a difference of 221.7 Bitcoin in just one month—before climbing to 484.5 in December 2021.[6] Once the Hardin plant re-opened in December with fully completed miner installations, Marathon announced that it produced approximately 34 Bitcoin on December 1, 2021 alone[7]—equivalent to $1,945,786 at the time, considering that Bitcoin was valued at $57,229.83 at the close of December 1, 2021.[8]

Perhaps succumbing to public, community, and investor pressure and the prospect of complying with proposed new SEC rules regarding climate change disclosures, in early April 2022, Marathon Digital announced that it would transition its operation at Hardin to other locations to reduce its pollution by the

---

[5] Oliver Milman, Bitcoin miners revived a dying coal plant – then CO2 emissions soared, The Guardian (Feb. 18, 2022), https://www.theguardian.com/technology/2022/feb/18/bitcoin-miners-revive-fossil-fuel-plant-co2-emissions-soared.

[6] Marathon Digital Holdings Announces Bitcoin Production and Mining Operation Updates for December 2021 (Jan. 3, 2022), https://ir.marathondh.com/news-events/press-releases/detail/1273/marathon-digital-holdings-announces-bitcoin-production-and.

[7] Marathon Digital Holdings Announces Bitcoin Production and Mining Operation Updates for November 2021 (Dec. 3, 2021), https://ir marathondh.com/news-events/press-releases/detail/1269/marathon-digital-holdings-announces-bitcoin-production-and.

[8] Yahoo Finance, Bitcoin USD (BTC-USD) Historical Prices, https://finance.yahoo.com/quote/BTC-USD/history/.

end of 2022.[9] Even with this announcement, Marathon's own CEO Fred Thiel stated that the company is leaving the Big Horn Data Hub and millions of dollars' worth of infrastructure intact, "so another miner can come in right behind us with a minimal delay and then com[e] up to speed[.]"[10] Thus, another cryptomining company can swiftly and easily utilize the infrastructure built at Hardin by Marathon. In fact, prior to Marathon operating at the plant, there was an attempt in 2019 by Big Horn Data Hub to utilize power from Hardin to mine Bitcoin. Although Marathon recently announced it plans to stop operating at Hardin, the infrastructure exists for a non-publicly traded mining company, of which there are many, to move in. That concern could be soon realized as the Hardin plant's owner is currently in discussions with potential tenants that are interested in moving into the Big Horn Data Hub.[11]

Notwithstanding the uncertain future of the Hardin plant after the recent announcement by Marathon Digital, the plant's operation in 2021 led to a massive uptick in emissions of harmful pollutants, including coal ash or coal combustion residuals ("CCR") —a solid waste byproduct of burning coal. Because of the historic and continued coal-dependent energy system in the American economy, CCR remains one of the largest waste streams in the U.S. Today, coal-fired power plants in the U.S. generate roughly 100 million tons of CCR every year.[12] While some (generally around half) of this is ash is reused in various ways each year, much of it has historically been dumped in landfills and water-filled pits (impoundments or "ash ponds") on site or near coal fired power plants.[13] Billions of tons of CCR currently sits in landfills and ponds across the U.S. with heavy-metal laden waste spanning hundreds of acres.[14] Recent industry data demonstrate that 92% of CCR ponds are polluting the underlying groundwater to levels that exceed federal drinking water standards.[15] CCR contaminates groundwater with carcinogens, neurotoxins, developmental toxins and other dangerous chemicals including arsenic, boron, lithium, chromium, cobalt, lead, lithium, manganese, molybdenum, radium, mercury, and cadmium. This groundwater can flow to drinking water wells or pollute nearby surface water.

In addition to issues related to coal ash because of coal-fired generation, power plants that engage in cryptocurrency mining present a unique problem to the regional haze program. As outlined in March 2022 comments by conservation organizations to the Montana Department of Environmental Quality on its proposed regional haze state implementation plan ("SIP"), since the proposed SIP relies on past

---

[9] Tom Lutey, Crypto miner plans to exit Hardin coal-fired power plant, Billings Gazette (Apr. 6, 2022), https://billingsgazette.com/news/crypto-miner-plans-to-exit-hardin-coal-fired-power-plant/article_cd2ca444-929a-511d-913d-903fbc570498.html.

[10] Kayla Desroches, As crypto company departs Hardin, what's next for the communities it leaves behind?, Yellowstone Public Radio (Apr. 28. 2022), https://www.ypradio.org/energy/2022-04-28/as-crypto-company-departs-hardin-whats-next-for-the-communities-it-leaves-behind; Marathon Digital Holdings, Our Facilities, https://marathondh.com/our-facilities/.

[11] Kayla Desroches, As crypto company departs Hardin, what's next for the communities it leaves behind?, Yellowstone Public Radio (Apr. 28. 2022), https://www.ypradio.org/energy/2022-04-28/as-crypto-company-departs-hardin-whats-next-for-the-communities-it-leaves-behind.

[12] U.S. EPA, Coal Ash (Coal Combustion Residuals, or CCR), https://www.epa.gov/coalash; see also Associated Press, EPA Moves to Crack Down on Dangerous Coal Ash Storage Ponds, U.S. News (Jan. 11, 2022), https://www.usnews.com/news/business/articles/2022-01-11/epa-moves-to-crack-down-on-dangerous-coal-ash-storage-ponds.

[13] Ross K. Taggart et al., Trends in the Rare Earth Element Content of U.S.-Based Coal Combustion Fly Ashes, 50 ENVIRON. SCI. TECHNOL. 5919–5926 (2016), https://pubs.acs.org/doi/abs/10.1021/acs.est.6b00085.

[14] See Earthjustice, Mapping the Coal Ash Contamination (July 29, 2021), https://earthjustice.org/features/coal-ash-contaminated-sites-map.

[15] Environmental Integrity Project & Earthjustice, Coal's Poisonous Legacy: Groundwater Contaminated by Coal Ash Across the U.S. (Mar. 2, 2019, rev. July 11, 2019), https://environmentalintegrity.org/reports/coals-poisonous-legacy/.

reductions from power plant retirements and pollution controls to support its proposal, the state fails to recognize potentially drastic future emissions increases associated with growing electricity demand in Montana from, among other things, data-processing centers used for cryptocurrency mining. Thus, the March 2022 comments by conservation organizations offered that the proposed SIP must require emissions reductions both from power plants that may supply electricity for cryptocurrency mining operations and from other sources as necessary to ensure that increases do not thwart Montana's progress toward the national visibility goal.[16]

The negative environmental and health impacts resulting from CCR and regional haze caused by cryptocurrency operations at Hardin disproportionately harm nearby communities. Hardin is located on the border of the Crow Indian Reservation, posing direct harm to that community's airshed, groundwater, and health. Cryptocurrency operations imperil the Biden Administration's efforts to achieve its environmental justice commitments, and most importantly, the costs of that failure will be borne disproportionately by communities that continue to live in Hardin's polluting pall.

Colstrip Coal Plant

Further, considering that Hardin was on the brink of closing for years, and the fact that Colstrip power plant has been teetering in terms of its future in a climate-constrained world, there has been some speculation that Colstrip could have a similar fate as Hardin: an uneconomic coal-fired power plant resurrecting for the sole purpose of generating electricity to produce Bitcoin. In fact, one of Colstrip's co-owners, Talen Energy, is part-owner of the Nautilus Cryptomine at Pennsylvania's Susquehanna nuclear facility, a joint venture with TeraWulf Inc.—an affiliate of Beowulf Energy, owner of the Hardin Generating Station.[17] Additionally, it was reported in 2018 that Talen Energy contracted with a Bitcoin mining operation for 64 MW of power from the Colstrip plant, presumably also increasing that facility's operating time and emissions.[18] Already, CryptoWatt Mining of Butte, Montana has a power purchase agreement with Portland General Electric, which supplies electricity from Colstrip.[19] Furthermore, Colstrip is located near the Northern Cheyenne Reservation, a designated "Class I" airshed.[20] Like

---

[16] Montana Environmental Information Center et al., Comments on Montana's Proposed Regional Haze State Implementation Plan for the 2nd Implementation Period, at 73 (Mar. 21, 2022), https://protectnps.org/wp-content/uploads/2022/03/Combined-MT-Regional-Haze-R2-Comment-Letter-Exhibits-2022-3-21_reduced-file-size.pdf; see also Victoria R. Stamper, Review and Comments on Reasonable Progress Four-Factor Analyses for Sulfur Dioxide and Nitrogen Oxide Pollution Controls Evaluated as Part of the Montana Regional Haze Plan for the Second Implementation Period (Mar. 2022) (Exhibit A).

[17] See Dan Swinhoe, Cryptomining firm TeraWulf join's Talen's nuclear-powered facility in Pennsylvania, Data Center Dynamics (July 20, 2021), https://www.datacenterdynamics.com/en/news/cryptomining-firm-terawulf-joins-talens-nuclear-powered-facility-in-pennsylvania/; Beowulf, Our Projects, https://www.beowulfed.com/projects/.

[18] Montana Right Now, Daines: Colstrip closures could hurt Montana's Bitcoin mining business (Aug. 22, 2018), https://www.montanarightnow.com/news/daines-colstrip-closures-could-hurt-montanas-bitcoin-mining-business/article_ebf1b10e-1f16-5d30-b861-3df262c1bf73 html.

[19] Tom Lutey, Crypto miner plans to exit Hardin coal-fired power plant, Billings Gazette (Apr. 6, 2022), https://billingsgazette.com/news/crypto-miner-plans-to-exit-hardin-coal-fired-power-plant/article_cd2ca444-929a-511d-913d-903fbc570498.html.

[20] Section 164 of the Clean Air Act provides that federally recognized Tribes may petition to have land within the exterior boundaries of reservations be redesignated as a Class I area. Under the Clean Air Act, all areas in the United States are categorized into one of three area classifications: Class I, Class II, and Class III. Class I increments are the most protective because they allow the least amount of air quality degradation. In 1977, the Northern Cheyenne Tribe voluntarily and successfully petitioned the U.S. Environmental Protection Agency to redesignate its reservation as a Class I area, which requires more stringent limits on sulfur dioxide and airborne particulate pollutants (two major pollutants resulting from coal-fired electrical generating facilities) within the exterior boundaries of the Northern Cheyenne Reservation.

Hardin, the multitude of harms resulting from cryptocurrency mining operations at Colstrip will disproportionately impact already vulnerable and overburdened communities, posing serious environmental justice concerns.

Coal-fired power plant owners and operators such as Talen Energy and Beowulf Energy recognize that their product is becoming less desirable to public utilities trending towards decarbonization targets.[21] As carbon intensive electricity is squeezed from highly regulated power markets, these coal plant operators are developing competency in on-site cryptomining because it allows their electricity to be consumed "behind-the-meter" instead of on the grid. Public utilities can still meet clean energy targets while coal plants continue to operate if the coal power does not count in evaluations of the public's energy mix. The ability of coal plants to remain operational by embracing cryptomines when they become uneconomic for public power undermines clean power programs and decarbonization efforts.

Fracked gas

In addition to resurrecting a coal plant, Montana is one of many states where cryptomining companies have popped up to mine Bitcoin using gas at fracking well pads. Many of these operations are unknown and mobile, and therefore hard to quantify. For example, Crusoe Energy, a Colorado-based cryptomining company, recently received an Air Quality Permit from the Montana Department of Environmental Quality at the Altuve Pad, located at Section 35, Township 26 North, Range 59 East, Richland County, Montana.[22] According to the final permit, issued March 25, 2022, Crusoe plans to install and operate ten 2,500 brake horsepower fossil gas-fired generator engines (Waukesha 9394 GSI engines) on-site at the Altuve Pad. In totality, these 10 fossil gas-fired generators will spew 1.5 grams per brake horsepower-hour of NOx, 3 grams per brake horsepower-hour of carbon monoxide ("CO"), and 0.1 grams per brake horsepower-hour of volatile organic compounds ("VOC")—equivalent to 36.21 tons of NOx per year, 72.42 tons of CO per year, and 2.41 tons of VOC per year. The environmental assessment accompanying the final air permit found that the operations will have "[m]inor impacts to air quality . . . due to the facility emitting air pollutants." Crusoe also received numerous other air permits, including: Kai Pad (permit 5265), Doris Pad (permit 5264), Altuve Pad (permit 5268), Sundance Kid Pad (permit 5266), Eagle 4-9 CTB (permit 5243), Crusoe Energy System (permit 5262), Crusoe Energy Systems, Inc. (permit 5256), Crusoe Energy Systems (permit 5255), Mayson Phoenix CTB (permit 5223), RKT Carda CTB (permit 5252), and Taylor LW 14-23 CTB, Fletch 5-8 CTB (permit 5234).[23]

Even if Crusoe will utilize some well gas that would otherwise be flared to the atmosphere, such operations serve as a subsidy to an extractive industry that should otherwise be capturing the flared gas for beneficial use or ramping down production at a time when landmark reports by the IPCC and IEA argue that we need to swiftly reduce fossil fuel production to combat the climate crisis. While Crusoe Energy's Altuve Pad operation is just one of many, as of October 2021, the company operates 44 data centers in Montana, North Dakota, Wyoming, and Colorado—with more to come in Texas and New Mexico.[24]

---

[21] NorthWestern Energy, Our Net Zero Vision (n.d.), https://www northwesternenergy.com/clean-energy/net-zero-by-2050#
[22] Montana Department on Environmental Quality, Air Quality |Crusoe Energy Systems, Inc. – Altuve Pad| Public Comment Period Ends March 7, 2022, https://deq mt.gov/News/publiccomment-folder/news-article161.
[23] Montana Department of Environmental Quality, Air and Permitting Operating Assistance, https://deq.mt.gov/air/assistance.
[24] Bitcoin miners help US oil producers cut flaring, Argus Media (Oct. 8, 2021), https://www.argusmedia.com/en/news/2261931-bitcoin-miners-help-us-oil-producers-cut-flaring.

4. *Economics*

These 24/7/365 operations do not come without community impacts and consequences. In fact, in 2017, a company named Project Spokane moved into an old lumber mill in Bonner, Montana—causing an uproar in the community for the loud buzzing noise from the air cooling and large fans to keep the computers from overheating.[25] The same company, Project Spokane, was sued in a Montana federal court in May 2020 by Energy Keepers Inc., a Tribal-owned power company, for not paying its $3.7 million bill to power its cryptomining operations.[26] As noted before, environmental justice concerns are central to the discussion about the environmental effects of cryptocurrency operations in Montana. Hardin borders the Crow Indian Reservation, and Colstrip is located near the Northern Cheyenne Reservation. Both coal-fired power plants are overburdened communities that will be disproportionately impacted by cryptocurrency operations. President Biden made a commitment to consider and advance environmental justice. President Biden's new Executive Order on climate change and environmental justice, amending the 1994 Order, provides that:

> It is the policy of [this] Administration to organize and deploy the full capacity of its agencies to combat the climate crisis to implement a Government-wide approach that reduces climate pollution in every sector of the economy; … protects public health … delivers environmental justice …[and that] … [s]uccessfully meeting these challenges will require the Federal Government to pursue such a coordinated approach from planning to implementation, coupled with substantive engagement by stakeholders, including State, local, and Tribal governments.[27]

Executive Order 12898 also requires the analysis of disproportionately high and adverse human health effects and environmental effects on overburdened and vulnerable communities.[28] Environmental effects include ecological, cultural, human health, economic, or social impacts on minority communities, low-income communities, or Indian tribes.[29] Cryptocurrency operations in Montana have significant negative environmental effects, and these effects threaten to undermine the Biden Administration's commitments to deliver environmental justice that is necessary for achieving equitable solutions to air and water pollution.

And current and planned data-processing centers in Butte, Broadview, Hardin, and Polson may demand up to 500 MW of Montana's electricity generation in the coming years.[30] In 2021, coal-fired power plants provided 43% of Montana's in-state electricity.[31]

---

[25] Mark Jaffe et al., Colorado's curious case of a crypto mine that no one is really sure exists, The Colorado Sun (Mar. 6, 2022), https://coloradosun.com/2022/03/06/olathe-solar-panels-secret-crypto-mine/.
[26] Morgan Conley, Tribal Power Co. Says Cryptocurrency Miner Owes $3.7M, Law360 (May 28, 2020), https://www.law360.com/articles/1277581/tribal-power-co-says-cryptocurrency-miner-owes-3-7m.
[27] Exec. Order No. 14008, 86 Fed. Reg. 7619 (Jan. 27, 2021).
[28] Exec. Order No. 12898, § 1-101, 59 Fed. Reg. 7629 (Feb. 16, 1994), as amended by Exec. Order No. 12948, 60 Fed. Reg. 6381 (Feb. 1, 1995).
[29] *Id.*
[30] David McCumber, Dirt and power, Rick Tabish's data center, slag plans hit high gear, Montana Standard (Mar. 31, 2019), https://mtstandard.com/news/local/dirt-and-power-rick-tabishs-data-center-slag-plans-hit-high-gear/article_9c6e72b9-1499-516f-8cfd-20ab30463f96.html.
[31] U.S. Energy Information Administration, Montana State Profile (Mar. 17, 2022), https://www.eia.gov/state/?sid=MT.

Considering that Montana's grid relies heavily on coal—and the state needs to rapidly decarbonize through the deployment of renewable energy—proof-of-work cryptomining not only leads to further dependence on coal-fired generation, but could also strain the grid's ability to adequately support existing load and potentially raise rates for local electricity consumers, especially considering how substantial the state's rural customer base is. In other rural areas, in places such as upstate New York,[32] Idaho Power's service territory,[33] and eastern Washington,[34] proof-of-work cryptominers have gobbled up inexpensive electricity, in particular hydropower, and in some cases, left ratepayers on the hook for their bills. We are worried about this also happening in Montana, which similarly relies significantly on hydropower to meet existing load throughout the state.

Butte

Butte is a prime example of the magnitude of electricity demand that cryptocurrency mining operations can place on small utility jurisdictions. Atlas Power, a cryptocurrency mining operation located in Butte, consumed approximately 75 MW to power its mining operation, as of January 2022.[35] Before operations began, the entire city of Butte consumed approximately 48 MW.[36] The increased demand is comparable to Montana's installed capacity of solar power (117 MW) statewide at the end of 2020, according to the Solar Energy Industries Association.[37] Further, while not in Montana, Atlas Power has plans to develop 700 MW of cryptomining capacity in North Dakota. The electricity consumption of North Dakota's largest city, Fargo, uses approximately 240 MW.

[32] See, e.g., Mateo Benetton et al., When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy, SSRN (May 14, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3779720; Laura Counts, Power-hungry cryptominers push up electricity costs for locals, Berkeley Hass (Aug. 3, 2021), https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-locals/.

[33] In November 2021, Idaho Power filed a petition with the Idaho Public Utilities Committee to create a separate class of "Speculative High-Density Load Customers," since the utility has received at least 17 seperate inquiries totaling 1,950 MW that could threaten the utility's ability to meet its existing load, in which it hit a record peak demand in June 2021 at 3,751 MW. See Case No. IPC-E-21-27, Application of Idaho Power Company for Authority to Establish a New Schedule to Serve Speculative High-Density Load Customers (Nov. 4, 2021), https://puc.idaho.gov/Case/Details/6774.

[34] Steve Wright, former CEO of Chelan County Public Utility District and Bonneville Power Administration, offered testimony to the U.S. House Subcommittee on Oversight and Investigatons that the utility he formerly ran, Chelan County Public Utility District, was overwhelmed by demand for cheap hydropower from crypto miners, and had to institute two moratoriums on new mining operations and a new rate structure to discourage miners from chasing short-term gains, which was upheld by the federal district court in Eastern Washington. See Steve Wright, Testimony before the Subcommittee on Oversight and Investigations, Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains (Jan. 20, 2022), https://energycommerce house.gov/sites/democrats.energycommerce house.gov/files/documents/Witness%20Testimony_Wright_OI_2022.01.20.pdf.

[35] Adam Willis, Large-scale crypto mining data center planned for western North Dakota oil patch, InForum (Jan. 26, 2022), https://www.inforum.com/business/large-scale-crypto-mining-data-center-planned-for-western-north-dakota-oil-patch.

[36] Rob Starner, There's Bitcoin Gold in Them Thar Hills, Site Selection Magazine (July 2018), https://siteselection.com/investor-watch/cryptocurrency-miners-reveal-the-site-selection-process-that-led-them-to-montana.cfm.

[37] Molly Taft, This Solar Crypto Mine Plan Is Stranger Than Fiction, Gizmodo (May 27, 2021), https://gizmodo.com/this-solar-crypto-mine-plan-is-stranger-than-fiction-1846966085.

Conclusion

Thank you for the opportunity to provide comments on this urgent and timely issue. Proof-of-work cryptocurrencies pose significant threats to the climate, clean energy, and environmental justice commitments of the Biden Administration, and the Administration should consider all tools in its toolbox to ensure that communities do not experience toxic air and water pollution at the behest of proof-of-work cryptominers who become rich as they pollute our neighborhoods.

As this comment letter shows, Montana is home to some of the dirtiest and most-polluting proof-of-work cryptocurrency mining operations in the country. Locally, we cannot afford additional air and water pollution, Nor can the planet afford more greenhouse gas emissions in the middle of a climate crisis, especially where the Co-Chair of IPCC Working Group III C recently warned that:

> It's now or never, if we want to limit global warming to 1.5°C (2.7°F); without immediate and deep emissions reductions across all sectors, it will be impossible.[38]

This cannot be a town-by-town or state-by-state fight. The federal government must mitigate the externalities this new industry places on local people, local environments, and our energy systems that should serve real people.

Thank you again for the opportunity to provide comments on this urgent and timely issue.

Sincerely,

Anne Hedges
Ian Lund
Montana Environmental Information Center
[redacted]

Jenny Harbine
Emily Qiu
Nick Thorpe
Mandy DeRoche
Earthjustice
[redacted]

Amy Cilimburg
Climate Smart Missoula
[redacted]

Michelle Uberuaga
Moms Clean Air Force
[redacted]

Caitlin Piserchia
Montana Chapter of the Sierra Club
[redacted]

Michelle Uberuaga
Park County Environmental Council
[redacted]

Whitney Tawney
Montana Conservation Voters Education Fund
[redacted]

Lori Byron
Montana Health Professionals for a Healthy Climate
[redacted]

[38] UN News, UN Climate Report: It's 'Now Or Never' To Limit Global Warming To 1.5 Degrees, Apr. 4, 2022, https://www.un.org/africarenewal/magazine/april-2022/un-climate-report-it%E2%80%99s-%E2%80%98now-or-never%E2%80%99-limit-global-warming-15-degrees.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Electronic Frontier Foundation (EFF)

COMMENTS OF THE
ELECTRONIC FRONTIER FOUNDATION
REGARDING DIGITAL ASSETS RESEARCH AND DEVELOPMENT

88 Fed. Reg. 5043

Submitted on March 3, 2023 to the
White House Office of Science and Technology Policy

The Electronic Frontier Foundation (EFF) submits the following comments in response to the White House Office of Science and Technology Policy (OSTP) request for information regarding digital assets research and development.

EFF is a non-profit organization that has worked for over 30 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With more than 30,000 contributing members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

EFF is encouraged to see the White House taking interest in the future of digital assets. These technologies have the potential, if used properly, to increase individuals' privacy while facilitating online commerce and research in this area could push forward the domain of advanced cryptography in ways that could radically change the landscape of online services that we all use every day. The White House and OSTP have the opportunity to guide this future today.

I. Coders' Rights

Fulfilling OSTP's goal of encouraging this important research requires at the very least ensuring that researchers and software developers do not face legal jeopardy for legitimate research. The Treasury Department's Office of Foreign Assets Control (OFAC) in August of 2022 placed the Tornado Cash smart contract on their sanctions list, sending shock waves through the digital assets community. OFAC's actions, taken without consultation with the community or input regarding questions such as what jurisdiction they have, what entities may be sanctioned, and what liability can attach to people who write code that ends up in a sanctioned smart contract, was extremely concerning.

Courts have consistently held that computer code is protected speech under the First Amendment. In particular, legal regimes that target the publication of speech and knowledge (in the form of code or other information), bear a heavy burden to establish that they are consistent with the First Amendment. A regulation that punishes researchers and software developers who are not responsible for harmful or illegal activity is very likely to fall afoul of these constitutional protections.

In addition, targeting developers in this way is a strategy guaranteed to discourage people from developing the very technologies and services in which OSTP is seeking to boost research and development. The chilling effect of seeing other digital assets developers placed on sanctions lists and even put at risk of arrest can not be overstated.

The White House should make it clear that writing code by itself cannot give rise to liability, it is only the actions taken with code that can create legal liability.

II. Non-Blockchain Ledgers

As OSTP suggests in the Request For Information, digital assets are not confined to blockchain-based solutions, and, in reality, blockchains may not end up being the ideal backing technology for keeping track of digital assets. Blockchains suffer from a number of issues that make them unsuitable to acting as the backing technology for a digital asset.

First, and most importantly, blockchains inherently place every transaction into a public ledger and require that ledger to be distributed to every other participant. Aside from the purely logistical problems that this poses, particularly as the size of the blockchain grows over time, this fact poses massive privacy problems. While transactions are usually pseudonymous on blockchain ledgers, eventually money needs to be used if it is to be valuable and that use enables tracing of coins to individuals with a modicum of investigation. There are blockchain systems that use anonymity technologies to blur the participants in the exchange, there are also countermeasures.

Secondly, the proof-of-work method of securing a blockchain against double spending, which Bitcoin uses and Ethereum used until very recently, uses electricity far in excess of what is reasonable for a transfer of value system and exacerbates an already-dire climate change situation. The proof-of-stake system that Ethereum now uses is a great improvement in terms of electricity use, but is still young and needs further research into its long term stability and its actual efficiency benefits. The White House should encourage research into newer exchange systems with lower energy costs, especially ones that take less energy than the traditional payment systems such as cheques or credit/debit cards.

Finally, as the cybersecurity research organization Trail of Bits showed in a report from June of 2022 entitled “Are Blockchains Decentralized,” blockchains tend not to live up to their largest claimed benefit: that of decentralization. According to Trail of Bits, at the time of publication of the report even just a handful of entities held enough control to disrupt the Bitcoin and Ethereum blockchains.

The White House should avoid assuming that blockchain is inevitably the solution for digital assets, and encourage research and development into other alternatives.

III. Privacy

One of the largest points of contention that will inevitably arise surrounding any digital asset system is that of financial privacy. We have already witnessed the opening salvos of this fight in the actions taken by OFAC against Tornado Cash. The administration should lay out a firm expectation at the outset of any process leading to the creation of digital assets that the financial privacy of ordinary Americans is fundamental.

Financial data can reveal enormous amounts of information, including medical status, religious or political affiliation, and sexuality. Charitable donations can obviously reveal a lot about a person, but even everyday purchases, particularly when taken in aggregate, are capable of painting a detailed picture of a person’s likes, dislikes, habits, and income. These pieces of information should not be the business of any private bank, credit card issuer, or government agency.

Financial privacy also enables and protects people’s constitutional free speech rights to support unpopular political and social campaigns and organizations without fear of reprisal. In an era of extreme political polarization, the demonization of marginalized groups, and movements to intimidate people away from accessing healthcare such as abortions, it is essential to preserve this freedom. Similarly, the US dollar is used around the world in places where giving money to certain charities or religious institutions could be dangerous. Giving those people financial privacy through the use of digital assets could improve human rights under repressive regimes everywhere.

Finally, building in financial privacy has the welcome side effect of ensuring that an asset can be used to buy anything and everything that is not illegal. For many years the major payment processors have acted as morality police, unilaterally deciding what they would and would not allow their systems to be used to purchase. Pre-internet this was perhaps more of an annoyance, as cash could always be used as a fall back. Since commerce has moved online, however, and credit and debit cards have become essential to transactions, these unelected intermediaries have become the unreviewable arbiters of what can and cannot be sold. Any digital asset contemplated by the White House should expand the options that purchasers have. Private transaction processors should not be empowered to force their restrictive preferences on the populace.

If the White House decides to undermine this privacy for the purpose of combating money laundering, the focus should be on large denomination transfers of value. Routine transactions of small denominations, as nearly all people make on a daily basis, should remain private under all circumstances. Some proposals, such as Senator Lynch's ECASH bill, directly address these issues. By calling for non-blockchain, direct-cash payments of under $10,000, it looks directly at the real issues that need proposals, test deployments, and infrastructure.

IV. Conclusion

EFF is encouraged by the White House's interest in digital assets, and we hope the administration will pay particular attention to making sure that any system created ensures privacy for everyday Americans and that researchers and developers working to advance the state of the art in digital assets are not burdened by legal liabilities for their work.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

EMTECH SOLUTIONS INC.

To:

Office of Science and Technology Policy

From:

EMTECH SOLUTIONS INC.
(U.S. Corporation, Technology Provider)

Subject:

Notice of Request for Information – Digital Assets Research and Development

Date:

March 3, 2023

Introduction

We are pleased to provide comments to the Office of Science and Technology Policy regarding the Federal Government's efforts to thoroughly evaluate and potentially incorporate a central bank digital currency (CBDC) in the United States. The proliferation and use of digital assets in mainstream society is still in its nascency, but market signals suggest there are long-term benefits to adopting or integrating digital currency into the fabric of the United States' monetary ecosystem.

In this RFI, we will first share our perspective on the "Goals, Sectors, or Applications Where Digital Assets Might Introduce Risk or Harm" and secondarily share our perspective on "R&D That Should Be Prioritized for Digital Assets." We chose to provide comments on these two points because we believe they are interrelated. Moreover, the coordination of R&D to solve these problems requires a thorough understanding of both topics.

Goals, Sectors, or Applications Where Digital Assets Might Introduce Risk or Harm

The introduction and implementation of digital transactions into the United States financial ecosystem started in the early 1950s with the invention of the credit card. For example, Diners Club introduced the first credit card in 1951,[1] which was followed by BankAmericard in 1958[2] and American Express in 1958.[3] Mastercard entered the market in 1966[4] and BankAmericard split off to become Visa in 1976.[5] Discover joined the credit card network in 1986.[6] Given the novelty of this new invention, naysayers balked at the thought of using anything other than cash, checks, or travelers checks. Today, nearly all of society uses some form of digital payment platform or system for some or all of their financial activities. A few popular payment platforms include, but are not limited to Venmo, Cashapp, Paypal, Apple Pay, Google Pay, and many others.

One of the features of these platforms is the ability to receive, send, and store value with very few interactions with a bank. As these platforms have grown in popularity they serve as proof points that individuals are willing and able to transact in a cashless and digital manner within digital ecosystems that they trust. This trust has been built slowly over time as more and more users join these platforms and users maintain the ability to easily convert their digital currency into cash.

One of the biggest challenges to the integration and mass adoption of a potential CBDC is getting society to trust it. Unfortunately, trust isn't solely developed by way of functionality; it is also developed by the degree of freedom users receive from utilizing the service. As it pertains to using cash, many people use

---

[1] https://www.dinersclubus.com/home/about/dinersclub/story

[2] https://www.washingtonpost.com/archive/lifestyle/magazine/1994/11/04/the-day-the-credit-card-was-born/d42da27b-0437-4a67-b753-bf9b440ad6dc/

[3] https://www.britannica.com/topic/American-Express-Company

[4] https://brand.mastercard.com/brandcenter/more-about-our-brands/brand-history.html

[5] https://www.forbes.com/advisor/credit-cards/history-of-credit-cards/

[6] https://www.investopedia.com/terms/d/discover-card.asp

it because it’s widely accepted, discrete, and they know that it’s backed by the full faith and credit of the United States Government. At EMTECH, our experience has shown that despite how much the public states it wants less interference from the Federal Government in their financial matters, these same individuals would not fully trust the financial system in America without the government’s involvement. The paradoxical nature of this relationship will likely never change. However, it's important to understand this dynamic to develop a central bank digital currency that, similar to cash, is accessible, easy to use, reliable, and trustworthy.

Building trust is difficult when companies who purport to be frontrunners in the digital asset industry cheat and defraud users out of their hard-earned dollars. To make matters worse, these types of fraudulent activities can severely damage a company's reputation and erode customer trust. Recent examples like FTX and Celcius have done little to bolster trust in digital assets. The FTX fraud was particularly egregious because it involved the company's own token, and it was done on its own exchange. This type of behavior risks undermining trust in the world of digital assets and presented another reason why a CBDC must be designed for trust to successfully be a riskless digital asset.

R&D that Should be Prioritized for Digital Assets

While there are several places one could start to focus R&D efforts, we suggest focusing on the two following areas:

1. R&D efforts to address the technical infrastructure changes that should be made to streamline the regulation, creation, and trusted adoption of a U.S. CBDC.
2. Consumer financial behavioral studies to better understand how consumers currently view digital assets, the pros and cons of using them, and how open consumers might be to using a digital currency that is backed by the federal government. In fact, it is also vital to understand the role that newer service providers play working with consumers and traditional financial institutions or systems to deliver trusted innovative goods and services that accelerate the adoption of CBDCs.

In respect to the first point, EMTECH has created an innovative technology platform that helps central banks and regulators deploy actionable digital tools to modernize their regulatory environment and adopt future-proof technical infrastructure. This will enable them to better adapt to the introduction of digital assets, including CBDC and monitor the risks of new digital assets and products being brought to market.

As societies around the world evolve and become accustomed to alternative finance tools, services, and digital currencies, institutions must be able to provide the systems, regulatory frameworks, and technological infrastructure for them to function well. EMTECH is one of the first companies to develop an innovative and scalable solution that equips central banks, banks, and other financial institutions with the tools they need to reduce the friction and complexity of this evolving banking paradigm. EMTECH’s solutions are built for a central bank to allow the U.S. CBDC to be safely distributed via a broad set of service providers that can close access gaps; improve the distribution of government funds; lower the cost for the U.S. Government to ensure disadvantaged communities are not left behind; and have built-in consumer protection and compliance frameworks.

The creation and implementation of a U.S. CBDC could facilitate financial adoption by segments of the U.S. population that have historically lacked access to or trust in traditional banking services, such as low-income families, displaced veterans, and minorities.

If the U.S. CBDC is built natively as digital token that is recorded on public distributed ledger technologies (DLT). it could help invoke public trust because of the transparent, immutable, accessible, and easily transferable nature of such technologies. Moreover, this is possible while preserving user data privacy, user choice of provider, transaction transparency and clear rules for Anti-Money Laundering. Coupled with expanding access to CBDC infrastructure for new financial services providers, the U.S. could achieve decentralized, yet safe, resilient, and inclusive access to the U.S. Dollar.

As stated in the E.O. 14067, "the United States should ensure that safeguards are in place and promote the responsible development of digital assets to protect consumers, investors, and businesses; maintain privacy; and shield against arbitrary or unlawful surveillance, which can contribute to human rights abuses."

At EMTECH, we are prepared to assist the Federal Government in any capacity that we can to move the United States closer to a trusted digital currency environment. The creation of a U.S. CBDC represents a once-in-a-lifetime opportunity for the United States to revolutionize its payment infrastructure. This will position the U.S. as a leader in this global effort to digitize, track, and expand access to financial services.

Respectfully,

EMTECH SOLUTIONS INC.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Fidelio Tata

From:	Fidelio Tata
To:	DARD-FTAC-RFI
Subject:	RFI Response: Digital Assets R&D Agenda
Date:	Wednesday, February 8, 2023 8:15:46 AM

RFI Response: Digital Assets R&D Agenda
Topic #4: R&D that should be prioritized for digital assets

Emerging areas that could enable new opportunities to leverage digital assets, particularly U.S. CBDC features that make U.S. CBDC more competitive internationally.

We are witnessing the creation of a new class of financial market products in the form of Central Bank Digital Currencies. While those instruments are still at an embryonic stage and their final form and shape is still unknown, it is already obvious that they are extremely flexible instruments due to their potential digital features. This paper adds to the extensive and rapidly growing literature by proposing a new type of Central Bank Digital Currency with an embedded time-limitation design feature based on a validity interval within which time-period the digital currency is an effective claim against the central bank. We call this interval Central Bank Digital Currency. Focusing on four use cases, we analyze the merits of the proposed interval design feature. We find that there are several potential applications in the context of liquidity management, lending, monetary policy of central banks and derivative transactions. It can be argued that interval CBDC have several potential advantages, including the reduction of counterparty credit risk, enabling remuneration, and enlarging the monetary and fiscal toolkit.

Link to paper: https://doi.org/10.1016/j.ribaf.2023.101898

Prof. Fidelio Tata
International School of Management
[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Fluency Technologies Inc.

Fluency Technologies Inc.
(CBDC Technology Provider)
NYC, U.S.

RFI Response: Digital Assets R&D Agenda

1. Goals, sectors, or applications that could be improved with digital assets and related technologies: Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered. This includes explanations of the current limitations in how those goals, sectors, and applications are currently advanced with limited use of digital assets and related technologies, and how increased or better use of digital assets could provide a specific advantage over existing approaches in advancing these objectives. Where relevant, respondents are encouraged to justify how digital assets provide unique value for advancing that goal, sector, or application compared to the use of traditional databases or other technologies (e.g., as outlined in National Institute of Standards and Technology Internal Report 8202, Figure 6).

CBDC Purposes

Central banks play an essential role in the economy as the institutions that manage the currency, monetary policy and stability of various countries. They provide the means and security guarantees required for a payment system to exist while ensuring inclusion, adoption and availability of those systems to citizens. As technological advances have made significant progress over the years, they introduced a variety of new topics and solutions that could be included within the financial system.

From an innovation and adoption perspective, the multiple years of technology experimentation in commercial, cryptocurrency and alternative finance have achieved an excellent level of maturity. As the key technical challenges to the new technology kept being solved, those markets grew steadily over the years. It is critical that Central Banks also evolve to continue to play their role and that Central Bank money adapt to take advantage of new opportunities. Today is one of the moments where technology offers the banking industry enormous possibilities to comply with their obligations and introduce brand new offerings, thereby improving the society and economy of their nations. Distributed Ledger Technology (DLT) has emerged as one of the transformational technologies of the last decade and its introduction is gathering significant interest around the world. DLT allows for highly transparent, secure, tamper-proof transactions between parties, and creates trust even when the parties have no reason to trust each other. DLT technology opens new, not previously thought of, solutions which can stand as the foundation for creating CBDC systems for Central Banks.

We strongly believe that the introduction of Central Bank Digital Currency (CBDC) will make a significant positive change to both developed and developing countries and their citizens including;

- Improving the availability and usability of Central Bank money
- Supporting a resilient and fault-tolerant payment system ecosystem
- Encouraging financial inclusion of underbanked and unbanked people
- Reducing the cost of processing cash and digital payments
- Enabling automation of payment systems inside operational processes of emerging industries
- Enabling innovation and optimisation for banking products
- Increasing revenue and tax collection for governments
- Reducing the cost and improving the efficiency of cross-border payments

Purposes for releasing CBDC

National central banks and international financial institutions have been exploring the pros and cons of central bank digital currency available to the public over the last few years. The idea of a Central Bank issuing digital currency available to the public is not new but gained traction thanks to digitisation, the internet, competition in the form of decentralized and alternative finance and other aspects. The needs and risks associated with issuing a CBDC to the public vary and are somewhat connected to the technical solutions and considerations of those solutions.

An array of arguments have been made for CBDC issuance. The main purposes can be regrouped into the following sections:

- The decline in the use of cash suggests the need to provide the public with another form of legal tender money
- The growing dependence of the economy on electronic payment systems
- Advances in new technologies concentrating the payment system landscape
- A need to accelerate the transmission of monetary policies, compliance and regulations

The decline in cash

The relevance of cash as a means of payment is diminishing. Businesses and households have increasingly turned to cashless payment methods such as debit and credit cards and e-wallets, at points of sale. Cash is generally incompatible with digital economies and as households purchase more goods and services online over time, demand for cash as a means of payment will decline further. A digital dollar is a way to provide the general public with legal tender money, as the replacement for more traditional cash. CBDC could substitute this role by providing public access to central bank money.

Growing Economy Dependence on Electronic Payments

Economic dependence on electronic payments rises as ubiquitous services such as ride-hailing, online shopping, food delivery and many other new types of businesses seamlessly integrate electronic payments into their interfaces, creating better user experiences for retail users. The trend of abandoning cash in favour of digital payments accelerated even further because of the COVID-19 pandemic. An increased percentage of purchases made digitally is being observed across all relevant industries.

Advances in Technology

The advances in technology have made significant progress over the years. From an innovation and adoption perspective, the technology used previously only in decentralised or alternative finance has advanced to a good level of maturity, with key technical challenges already resolved. Further process automation could be undertaken by converting those technologies into a potential CBDC design capable of high availability and accessibility of trusted data, including the use of Distributed Ledger Technologies (DLT). Such new innovation could be used for risk management, fraud detection and to enhance decision-making for the purposes of enforcing consensus between system modules. Internet of Things (IoT) devices could also provide an added dimension of data for conditional payments and programmability cases.

Enhancing Monetary Policies

The effect of CBDC on the transmission mechanism of monetary policies depends on the issuance model of CBDC. While some issuance models would have virtually no effect on the transmission and conduct of monetary policy, others would have important implications. Those implications mostly relate to the following aspects of designing CBDC:

- the existence or nonexistence of interest rates,
- the minimal and maximal amount of CBDC per person,
- convertibility into other forms of central bank money etc.

Various combinations of those three aspects define alternative models of CBDC issuance.

Enhancing Cross-Border Payments

CBDCs could facilitate faster and more efficient cross-border payments. As cross-border payments are more complex than domestic payments, CBDCs would help ease international payments by offering cheaper transaction and storage costs, and more transparent and resilient payment solutions. CBDCs could also increase safety in payment infrastructures, enhance systemic efficiency and offer increased protection against money-laundering processes.

CBDC Opportunities

Evolving Payment Landscape

Over the last decade, the payment landscape has significantly evolved with the rise in digital payments. New market roles have emerged on the back of this trend and so also new market players who are changing the dynamics of the payment industry by offering a redefined value proposition to customers. In the midst of this disruption, a whole new subsection of digital solutions has emerged: cryptocurrencies, stablecoins, alternative finance, decentralized finance and others which are focused on the payments value chain, as well as payments facilitators, payment providers, networks creating new payments propositions, and payments technology suppliers.

At the same time, economic dependence on electronic payments is on the rise as ubiquitous services such as ride-hailing, online shopping, food delivery and many other new types of businesses seamlessly integrate electronic payments into their interfaces, creating better user experiences for retail users. Fundamentally, payments are becoming more instant, frictionless and embedded within customer journeys – hence invisible. Payment providers continue to drive transformation, but incumbent intermediaries also have a major role to play in shaping the future outlook of the sector to better serve their customers and guide them into the next payments era.

The shift from the use of cash to digital payments signifies a headline objective for the Central Banks towards fostering the development of a digital economy. The introduction of CBDCs is another drive by the banks to reduce cash usage but holistically address other fundamental economic and policy objectives. Fundamentally CBDCs would allow banks and payment service providers to innovate and take advantage of all the new possibilities in order to provide a better quality of services to banked users as well as to provide financial services to the unbanked and underbanked.

Besides the payment drive, the policy measures that have facilitated and enabled the rise in digital payments and the overall resilient and innovation-centric initiatives include:

- Cashless policies
- Financial Inclusion policies
- Identity framework for banks and government services
- Establishment of interoperable domestic and cross-border payment infrastructure
- Enabling payment automation for businesses
- Supporting standardization initiatives
- Strengthening and reducing the time-to-market of monetary policies

The introduction of CBDCs potentially allows banks to focus and efficiently implement those policies or continue to support them, while at the same time:

- making it easier and safer to use internet payment services
- better protecting consumers against fraud, abuse, and payment problems
- promoting innovative mobile and internet payment services
- strengthening consumer rights
- strengthening the role of the Central Banks authority

Opportunities to support monetary and financial stability

Monetary and financial stability are fundamental to any payment system at its core. We strongly advocate for a greater level of stability, resilience and fault-tolerance to the payment systems built around CBDCs and allow practical implementation of cash-less policies and initiatives. Beyond this, maintaining monetary and financial stability is a prime objective and a driving factor towards a financially inclusive economy which is a key factor for the company's vision.

We see the potential in CBDC systems to enable overall economic growth by providing the following improvements over more traditional payment systems:

- Support for the inclusion of banked, unbanked and underbanked citizens
- Increase the resilience and fault-tolerance of the payment system
- Standardization and simplification of monetary flows, both domestic and cross-border
- Reduction of costs related to processing payments
- Introduction of means for providing automation in business and distribution of welfare to the citizens
- Strengthening of monetary policies and compliance applications

Those improvements are possible to be achieved by taking an innovative approach to modelling financial systems using distributed ledger technology. We have researched and actively continues to research solutions allowing the implementation of such systems, believing in their potential and possibility of providing the greater good to society.

2. Goals, sectors, or applications where digital assets introduces risks or harms: Information about goals, sectors, or applications where digital assets might introduce risks or harms, and examples of where risks or harms are already being manifested. This includes explanations of direct or indirect impacts on users of digital assets, communities or sectors in which digital assets might circulate or be integrated into services, and non-users (e.g., communities, environment) that may be exposed to risks or harms of digital assets (e.g., ransomware attacks, higher electricity costs, pollution). Where relevant, respondents are encouraged to justify how digital assets are introducing new risks or harms in advancing the underlying goal, sector, or application compared to the use of traditional databases or other technologies.

<u>CBDC Risks</u>

Managing Risks

The potential financial stability-related risks through the introduction of CBDCs arise primarily from a significant substitution away from private money, whereas central bank cash-to-CBDC substitution is generally regarded as having no implication for financial stability. CBDCs (like other forms of digital money) could lead to higher volatility in bank deposits and/or a significant, long-term reduction in the volume of customer bank deposits. This could, under certain circumstances, affect bank profitability, lending and the overall provision of financial services. Customer bank deposit-related funding is at the heart of the commercial banking business of maturity transformation and intermediation services. Any material loss in customer deposit funding would require banks to consider additional initiatives to maintain regulatory ratios and risk-adjusted profitability.

The transfer risks come mainly from the fact that in the banking system, two types of money exist - Central Bank money which is risk-free and commercial bank money which represents a claim on Central Bank money. Therefore the risks emerge as those two types of money exist in imbalance with each other which can happen if commercial banks' reserves become too low or too high.

When excess reserves are small, the decline in banks' reserves following an increase in the demand for cash or CBDC by the public leads to tighter money market conditions and higher short-term interest rates. To prevent a tightening of monetary conditions, the central bank needs to accommodate this demand with a corresponding increase in banks' reserves. This accommodation implies an expansion of the Central Bank's balance sheet and, thereby, a transfer of risk to the Central Bank.

When excess reserves are large, the decline in banks' reserves does not immediately lead to tighter money market conditions and higher short-term interest rates. Thus, the central bank does not have to accommodate the demand for cash or CBDC by nonbanks to maintain its monetary policy stance. However, because banks' excess reserves decline, the central bank loses its ability to reduce its balance sheet and its associated risk in case this becomes necessary.

Transfer risks can be minimized by developing correct design choices regarding remuneration, quantity ceiling and the degree of convertibility at par.

Remuneration

The first option to limit the transfer risk is the possibility of making CBDC more expensive to hold than cash would limit its demand. In normal times, a moderately negative interest rate might limit the demand for CBDC and, thereby, the risk transfer. During crises, interest in CBDC would probably need to be lowered sharply, which would yield uncertain results because even a very negative annual interest entails only small costs over a short period.

Quantity Ceiling

Another way to address this issue is to set a maximum amount of CBDC per capita. A quantity ceiling can be strictly enforced so that any surplus above an individual threshold is automatically transferred into another account at a commercial bank or another technical method of locking funds. Alternatively, a strict limit on the number of holdings could be implemented.

Limited convertibility

The other popular approach limiting transfer risk is limited convertibility which assumes that CBDCs and reserves are distinct and in a situation of financial instability they will not be convertible to each other. Additionally, there would not be guaranteed on-demand convertibility of bank deposits into CBDC at commercial banks, which would stop the potential outflow of bank deposits into CBDC if needed.

We believe that mechanisms for managing previously mentioned risks should be provided within CBDC out-of-the-box within provided technology and support means to securely handle them. The potential CBDC solution should look into how to achieve remuneration, quantity ceiling, limited convertibility and/or any other measures of managing transfer risks. The research should prioritize solutions that are not hard coded inside the platform, but rather can be configured freely by the authorities so all those mechanisms can be adjusted on-demand as time progresses.

Cryptocurrency & Stablecoin Risks

A number of recent events have demonstrated how volatile and unstable both cryptocurrencies and stablecoins are. The collapse of the likes of FTX and TerraUSA proved these approaches are flawed and can send a currency's value to zero and wipe out billions of dollars of wealth.

To avoid the risks associated with both cryptocurrency and stablecoins, the obvious solution is the creation of a central bank digital currency (CBDC), with the elimination of alternative digital assets. It's the route China is following. China launched the digital yuan after banning cryptocurrencies in September 2021.

Cryptocurrency Risks

There is no central bank or exchange which mediates transactions, so most transactions are irreversible. Since there is no centralized party or government which enforces its value the value of the coin is purely determined by the value which peer investors place on it. If the investing community were to lose interest in a particular cryptocurrency because of a security incident, the units of that currency could become worthless overnight.

Some of the risks associated with cryptocurrency include;

Volatility - It is common for cryptocurrencies to double in value in a matter of months. It is also common for cryptocurrencies to halve in value within the same period of time. Cryptocurrencies are seen as a store of value for speculators. Investors who are looking for a stable source of value for their investments continue to steer clear of the cryptocurrency markets.

Tax - Since cryptocurrencies are relatively new, there is still a lack of clarity about how the gains from these investments need to be taxed. Since the rules are not completely clear. Most countries in the world do not have tax gains from cryptocurrencies mentioned in their tax code. Even though this mention has not been explicitly done, investors are supposed to mention the income and pay taxes on them. Since governments do not have a strong mechanism to determine the exact income from cryptocurrencies, some investors have tried to avoid paying taxes on them. This has landed them in trouble with the tax authorities. In many cases, investors genuinely wanted to pay their dues. However, due to the confusion about the exact nature of tax that needs to be applied to cryptocurrencies, they have been unable to do so. Hence, paying taxes on cryptocurrencies is also a complex task that requires significant transaction costs.

Legal - The problem with cryptocurrencies is that they are completely anonymous. As a result, they are widely used by crime syndicates and other people indulging in unlawful activities. Since cryptocurrencies are not regulated by the government, criminals find this to be the best way to launder their money. As such, many countries have made issuing and accepting cryptocurrencies an illegal activity.

Data Loss - The money invested in cryptocurrencies is held in digital wallets which are protected by digital passwords. If the owner deletes these passwords and is not able to recover them on their own, there is a big possibility that the money locked in the digital wallet may become inaccessible.

Data Theft - Hackers can hack into individual accounts by using techniques such as phishing and social engineering. This means that instead of hacking into the system, they actually trick the investor and obtain the password voluntarily. Data theft is common among cryptocurrency investors. In 2020, the estimated value of data theft related to cryptocurrencies was around $2 billion. Since there is no centralized authority that facilitates cryptocurrency-based transactions, data thefts are common. Some fintech companies are trying to provide security solutions. However, those solutions will have to be implemented at the individual level and will have to be paid for individually.

Stablecoin Risks

Tether provides an example of how a stablecoin can go wrong. Fiat-backed stablecoins are centralized, meaning they are run by a single entity. This requires trust that this entity is actually backing up its stablecoins with real fiat. To solve this trust problem, stablecoins could adopt approaches like providing regular audits from third parties to bolster transparency.

Fiat-backed stablecoins are also constrained by all of the regulations that come with fiat currency, compromising the efficiency of the conversion process and the potential efficacy of the digital asset. For example, Facebook’s Libra currency promised a stablecoin backed by a basket of global fiat currencies, thus broadening the coin’s appeal and utility. However, it received so much regulatory blowback that the project’s management dropped its multi-currency aim, distanced itself from Facebook, and rebranded altogether. The network is still struggling to get regulators to sanction its own stablecoin.

Stablecoins may also have less liquidity than regular cryptocurrencies. This is especially true for commodity-backed stablecoins - if you ever wanted to get your real bars of gold, for example, it could take months. Moreover, there’s always the risk that the underlying asset crashes in value.

Crypto-backed stablecoins also come with their own set of issues. Being pegged to other cryptocurrencies makes them much more vulnerable to price instability in comparison to fiat or commodity-backed stablecoins, which means if that crypto takes a deep nosedive, the stablecoin ultimately will as well.

Another risk of crypto-collateralized stablecoins is that they're difficult to understand, which introduces a much higher risk for people holding them to face unexpected events.

4. R&D that should be prioritized for digital assets: Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present. This includes topics for technical research, topics for research in the social sciences and across disciplinary boundaries, and opportunities for hardware and software development. This also includes information about emerging areas that could enable new opportunities to leverage digital assets, as well as information about technical limitations of digital assets and the associated business models and governance arrangements they often rely upon. Respondents are encouraged to, where relevant, describe how the discussed R&D topic could be useful in helping a potential U.S. CBDC system align with the Policy Objectives for a U.S. CBDC System. Respondents are also encouraged to share how the discussed R&D topic could help advance U.S. competitiveness and leadership in the world.

CBDC Continuous Research Process

Business Areas of Interest

Our own research leads us to a better understanding of the areas that a CBDC system needs to cover. The most important areas to be considered by adopting CBDC systems are:

- CBDC Issuance, Distribution and Lifecycle Management
- Programmability around payments including Smart Contracts
- Digital Innovation and Automation of payments
- Privacy and offline capability
- Support for compliance, AML and custom regulations
- Upgradeability of the CBDC platform
- Cross-CBDC and cross-border payments and custom messages

We believe that none of the currently existing public or enterprise platforms outside of our solution is capable of fully implementing CBDC systems as per directives already published by major central banks and international financial organizations. The potential CBDC system has to be designed and implemented from scratch and we see a strong case for using DLT technology for the purpose. The research about proposed solutions should not focus on purely technical perspectives but collaborate across technical and business propositions to be able to propose specialized solutions optimized for CBDCs provision and nothing else.

Technical Areas of Interest

In order to define and design the best-suited architecture and infrastructure for the CBDC platform, first the strengths and weaknesses of possible solutions need to be thoroughly analyzed. This analysis has to be made while making the right choice between a variety of mutually compatible and incompatible solutions. The decision process requires also keeping in mind the current state of digital banking technology, the innovations being introduced on that topic by foreign countries, and the innovations being made in related markets. The important part of the process is to take a particular look into the shortcomings of the enterprise platforms used in CBDC pilots and understand threats presented by CeFi, DeFi and cryptocurrency markets. The business design principles and related issues needed to explore can be divided into two groups:

- Foundational issues that covered monetary and financial stability; legal and governance frameworks; data privacy; competition fairness; operational resilience and cybersecurity; illicit finance counter-acting; and energy and environment.
- Opportunities issues, which cover digital economy and innovation; financial inclusion; payments inside the public sector; cross-border functionality; and international development.

The technical areas of interest are:

- Permissioning and administration over the CBDC network
- Fault tolerance and resiliency
- Data availability, data replication, latency and coverage of the network
- Traceability of assets, support for AML and other illegal activities detection systems
- Performance, throughput and finalization time of transactions
- Inclusivity - i.e. introduction of offline payments, support for people with disabilities, simplicity of end-user facing flows, cleanliness of UX etc
- Programmability - definition of conditions that could be attached to transactions and rules and constraints connected to monetary policies, compliance and regulations
- Upgradeability and maintenance of the platform
- Innovation by creating support for complex scripting through smart contracts
- Privacy and system trust - limited visibility of transactions, trust levels, confidential and indisputable settlements
- Interoperability - interoperability with other CBDCs and the current digital banking system
- Cross-border and cross-CBDCs features

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Gary C.

From:	Gary C
To:	DARD-FTAC-RFI
Subject:	RFI Response: Digital Assets R&D Agenda
Date:	Sunday, January 29, 2023 2:53:29 AM

There are a lot of innovations in digital assets that will have a worldwide impact. For many in Venezuela and Argentina, among massive inflation, they are holding assets in stable coins since getting physical US fiat is difficult.

Furthermore, defi exchanges are completely transparent since the code can be inspected by the public. Compared to wall street, where dark pools and off-exchange transactions occur, crypto applications offer more transparency since everything is recorded on the ledger and the code is viewable by the public. Goldman Sachs, JP Morgan, and all of the major investment banks would never publicly share their code or algorithm, creating a non transparent banking system.

As more things become digital and digital universes, such as VR and gaming, become more mainstream, the significance of digital assets will grow. If the United States decides not to act on this opportunity, then some other nation will. Currently, the US holds the largest percentage of mining operations and has a huge influence on the price/direction of digital assets. I think maintaining that influence will be significant in continuing to have a competitive edge in technological advances.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Gauntlet

Gauntlet is a risk management platform that uses quantitative analysis to inform on-chain protocol management.

Q5: *Opportunities to advance responsible innovation in the broader digital assets ecosystem*

As a risk management firm, Gauntlet has extensively researched the unique market risks associated with digital assets and decentralized finance. We propose various lines of research that could contribute to a better understanding of risk and responsible development in the broader ecosystem:

1. Research to support the cross-disciplinary learning of risk best practices in the digital assets ecosystem and traditional financial markets. Gauntlet has worked with traditional institutions, like Moody's Analytics, to build new frameworks for assessing risk. Further research in this area could help develop a better understanding of emerging risks and potential opportunities in both the traditional and digital assets ecosystems.

   Past research in this area:
   Block by Block: Assessing Risk in Decentralized Finance

2. Research to better understand trading venues in the digital assets ecosystem. Gauntlet has studied novel trading mechanisms like Automated Market Makers (AMMs) and worked to quantify their behavior under various market conditions. Further research in this area could support the development of more efficient and robust trading solutions for digital assets.

   Past research in this area:
   When does the tail wag the dog? Curvature and market making
   Optimal Fees for Geometric Mean Market Makers
   Improved Price Oracles: Constant Function Market Makers

3. Research to better understand lending mechanics in the digital assets ecosystem. The growth of lending protocols that allow users to borrow digital assets has led to the emergence of novel money markets existing entirely on a blockchain. Gauntlet has studied the risks and opportunities presented by existing and proposed lending mechanisms. Further research in this area could help better understand existing risks and guide the responsible development of improved solutions.

   Past research in this area:
   An analysis of the financial risk to participants in the Aave protocol
   An Analysis of the Market Risk to Participants in the Compound Protocol

    When do dynamic DeFi rate curves reduce capital efficiency

4. Research to better understand the risks and opportunities of derivatives built on blockchain mechanics. Gauntlet has studied the emergence of derivative trading products, such as perpetual futures, in the digital assets ecosystem. Derivatives are a recent innovation that presents significant new risks and opportunities to the broader ecosystem going forward. Further research could help better understand emerging risks and guide responsible development practices.

    Past research in this area:
    A primer on perpetuals

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Global Blockchain Business Council (GBBC)

March 3, 2023

SENT VIA EMAIL: DARD-FTAC-RFI@nitrd.gov

To whom it may concern,

Re: RFI Response: Digital Assets R&D Agenda

About

Global Blockchain Business Council (GBBC) is the largest and leading industry association for the blockchain technology and digital assets community. Launched in Davos in 2017, GBBC is a Swiss-based non-profit, with more than 500 institutional members, and 231 Ambassadors across 109 jurisdictions and disciplines. The organization is dedicated to furthering adoption of blockchain technology by convening regulators, business leaders, and global changemakers to foster collaboration and advance dialogue to create more secure, equitable, and functional societies.

1. Goals, sectors, or applications that could be improved with digital assets and related technologies

1a. Goals: Importance of Ecosystem

While there exist a wide range of applications where digital assets[1] and blockchain technology can bring promising solutions (i.e., through cost effectiveness, transparency, and accountability across all industries), it is important to first note that this is a collaborative technology whose growth also depends heavily on robust networks of engaged participants. Because decentralization enables an unprecedented degree of peer-to-peer interactions, and also allows individuals to drive governance, the value of blockchain-enabled solutions will also rely on the strength of the ecosystems around them.

This is not a new concept; it can be applicable to Metcalfe's Law, where the value of a network grows exponentially with the growth of the user base. This has been proven with early telecommunications networks, where the value of a phone is not based only on the solution of enabling calls but also by the number of users who adopt it. Ecosystems are not easy to build and require buy-in from a wide range of stakeholders – hence the importance of functions like partnerships, business development, and formalized bodies to foster meaningful collaborations.

GBBC has grown a robust ecosystem to support the adoption of blockchain and digital assets space, bringing together a wide range of stakeholders from large corporations, startups, academia, and government with a focus on education, partnership and advocacy. GBBC's community of builders and pioneers are deeply involved in the most promising solutions, propagating the rise of a new generation of decentralized business models that rely heavily on communities of users and large-scale, collaborative initiatives. The global community is in the early innings of this growing multi-trillion-dollar industry, with many innovative developments underway.

[1] Throughout this paper, all references to digital assets refer to those supported by blockchain technology.

An resulting example of such collaboration, GBBC's Global Standards Mapping Initiative (GSMI) has compiled a research-based repository of resources and recommendations for the blockchain ecosystem which has dealt with precisely this question stated in section 1, namely to bring light to areas being improved by digital assets and blockchain technology. In the sections below, this RFI response aims to highlight GBBC's existing research content, as well as that of its members, to illustrate this point This industry is not short on data, nor research. It does need more analysis and synthesis of raw data to form and develop both macro and micro trends as well as development of standards and best practices that exist in more mature industries.

1b. Sectors: Blockchain and Digital Assets Landscape:

Blockchain technology and digital assets are breaking silos and progressing substantive solutions to move our world in a positive direction and meet the most pressing challenges of our time, while facilitating corporate responsibility. For instance, these tools are improving the lives of refugees with the World Food Program's Building Blocks program managing refugee camp operations in Jordan on blockchain technology, and redefining the way we produce and consume art with non-fungible tokens (NFTs), allowing artists to raise fund for specific causes such as Proof of Art's carbon neutral collection produced by Afghan women artists to fund local education and other refugee needs. This technology is also allowing communities to reimagine electrical grids, and reshape our capacity to combat climate change.

The blockchain and digital assets landscape is made up of products, services, platforms, and infrastructure that are collectively shaping applications across sectors. GSMI has produced a global mapping of this landscape, with more than 2,000 key stakeholders and their interactions illustrated below:

It is fundamental that blockchain ledgers record quality data. Once this is assured, analytics using AI algorithms can be applied to track and trace the activity recorded on the blockchain, drawing patterns to make informed decisions about the transactions occurring on the blockchain with respect to those transactions. This has proven highly effective in detecting illicit activities such as hacks and money laundering. Another facet of data takes the form of off-chain information through news, social media, and metrics providers, through which users become informed of new developments, decide to participate in them, and can engage with each other in ways that drive community and growth.

Infrastructure providers – particularly exchanges, wallets, and custodians – provide the means to acquire, hold, and exchange tokens on the blockchain. Blockchain technology and digital assets have the power to transform the financial marketplace providing an unprecedented degree of transparency and efficiency. The prospect of real-time clearing and settlement, full transparency of fund flows, and close to cost free transactions across borders are becoming a possibility with blockchain technology and digital assets, which the current financial system has not managed to attain. Additional supporting infrastructure – trade execution services including liquidity and order routing, enterprise provisioning to support largescale use cases, and mining and staking services – help ensure properly functioning financial market arrangements. Overlaying these activities, a clear regulatory framework that can support these innovations is imperative to provide clear guidance to innovators and remove legal and regulatory risk.

GBBC
Global Blockchain
Business Council

1c. Applications: Promising Use Cases

GBBC's latest Annual Report titled Stronger Together: Rebuilding after the Maelstrom of Markets and Annual Reports Archive lay out use cases and sectors that have developed in the latest years. Major companies like Accenture and Ernst & Young have launched products and services to help companies across sectors transition their business models to capitalize on opportunities in blockchain and digital assets. Below are highlighted the most relevant sectors and examples of blockchain and digital assets developments:

I) Financial Infrastructure

Today's centralized infrastructure for financial services is marked by data silos across different systems, transaction costs and fees that are often highest for those of lower socioeconomic status, and processing times for operations like clearing and settlement that add risks to buyers and sellers. Blockchain technology and digital assets enable real time settlement, full transparency of fund flows, and low-cost transactions, even across borders. Tokenization of financial products can be a gamechanger for expanding marketplaces, and transparency for trading securities can greatly improve the ability to track ownership. Case in point, transparency can improve the allocation of votes to shareholders.

Financial services built upon this infrastructure can greatly improve efficiencies and add credibility. Back-end systems are adhering to the technology pipes, as major financial institutions are experimenting with the benefits of incorporating blockchain technology and digital assets into their operations.

Examples are wide ranging, from large financial institutions to startups. Onyx by J.P. Morgan has developed blockchain-based platforms to exchange value, information, and assets. Wells Fargo has also recognized opportunities with cryptocurrency and partnered to implement blockchain technology to settle forex trades. Visa has also developed solutions to facilitate new digital currency flows, provide related value-adding services for crypto, and has partnered with ConsenSys to launch infrastructure to support institutions collaborating to build user-friendly services on Central Bank Digital Currency (CBDC) networks. Paypal has incorporated functionality to transact in cryptocurrencies. The Depository Trust & Clearing Corporation (DTCC) has also been working to reduce traditional settlement times. Digital Asset, Provenance Blockchain Foundation, Lukka, Wave Financial, and SBI Digital Markets are additional examples of organizations advancing solutions to enable meaningful blockchain adoption for financial services at an institutional level. Evertas has developed the first crypto insurance solution, and Kaiko has developed sophisticated insights on market data to manage risks for institutions.

While the infrastructure on which the cryptocurrency market operates has yet to mature, it has shown its potential by the sheer size it has attained, as shown by GBBC's Crypto Market fact card. Moreover, increasing crypto adoption in developing countries, among the highest in the world, also reflects the prospect of financial inclusion. As these marketplaces continue to flourish, they will likely be covered by standards such as the Principles for Financial Market Infrastructures (PFMIs), which will further increase adoption. VMWare, SDX, and Lykke facilitate transparent and compliant exchange of value on the blockchain, often paired with sophisticated custody solutions.

i. Decentralized Finance

Decentralized Finance (DeFi) is a case in point where alternative financial services built on blockchain networks have emerged out of open-source and peer-to-peer interactions with decentralized governance to enable community-driven decision making. Participants can build financial products from composable financial primitives and basic tooling with plug and play architecture. These activities have amassed a truly global liquidity pool comprised of digital asset deposits to enable fund flows. DeFi has shown to be a promising path to democratize access to finance through low cost, inclusive, transparent, censorship resistant, and programmable features albeit nascent today. Regulatory clarity, standards and technical developments will provide the necessary gaps to enable responsible innovation and growth.

GBBC Digital Finance's report DeFi: Moving the Dialogue on Standards and Regulation Forward discusses the challenges and opportunities of this space. Financial inclusion and disaster related use cases include the Algorand Foundation supporting the humanitarian crisis in Afghanistan with an effective payment system built on Algorand's blockchain. In addition, the Kokua wallet, also built on the Algorand blockchain, is enabling transparent relief funding disbursements for St. Vincent De Paul Disaster Services assisting people affected by natural disasters. In addition, IOV Labs has created solutions to facilitate the use of DeFi solutions for average individuals, and IMAN has built a DeFi protocol to facilitate access to Sharia-compliant funding for Muslim communities largely in frontier markets.

II) Digital Money

As money develops to adopt a natively digital format, it becomes well suited to run on the blockchain infrastructure described above to deliver the corresponding efficiencies, transparency, and cost reductions, both for domestic transactions and global trade. Central Bank Digital Currencies (CBDCs) are being actively researched and tested throughout the world, as illustrated by GBBC's CBDC fact card.

If the United States aims to maintain the competitiveness of the US Dollar as the reserve currency of the world, it is paramount to develop a thoughtful approach to the design and attributes of a digital dollar. A tokenized US currency, usable irrespective of time and space, will be an effective settlement medium to support cheaper, faster, and more inclusive global finance, while coexisting with other liabilities of the Federal Reserve. The Digital Dollar Project has greatly advanced research, discussion, and collaboration across public and private sector players to explore options where a CBDC could improve the effectiveness of monetary policy and financial stability, with the right security and privacy safeguards in place. A successful model will be scalable and enhance payments involving retail, wholesale, and international fund transfers. It will also integrate with existing financial infrastructures

Another example that also ties to the US Dollar is the National Bank of Cambodia's Bakong, developed by Soramitsu as the first blockchain-based retail payment system launched by a central bank. Anyone with a Cambodian phone number and smartphone is eligible to send and receive instant payments in Khmer Riel or USD. All other QR code-based payment systems in the country are integrated with Bakong through the KHQR standard. This also creates new opportunities for financial inclusion for unbanked and underbanked communities.

In the meantime, while there still remains a gap between the launch of a globally widespread central bank-issued digital currency that can attain the acceptance of a reserve currency, stablecoins cryptocurrencies pegged in value to fiat currencies. GBBC's Stablecoins fact card illustrates the models and uses for stablecoins today, which have unlocked the Internet of Value where sending money becomes as simple as sending an email. For this reason, stablecoins have also been a major area of focus among global regulators.

III) Sustainability and Tokenization

With the role of blockchain technology to provide transparency and accountability through open data, the increasing global interest in sustainability is recognizing the value of this technology to add the necessary element of credibility for voluntary carbon markets, impact measurement, reporting, and verification (MRV), and a vast array of socially and environmentally minded business models. The blockchain and digital assets landscape produced by GBBC includes a section with sustainability-focused blockchain use cases in operation. In addition, GBBC Digital Finance had produced the report Digital Assets: Laying ESG Foundations to discuss pathways toward decarbonization and sustainability for blockchain technology and digital assets, from energy use to climate finance utilizing this technology.

There is a wide range of promising blockchain use cases across the energy sector that facilitate the distribution of energy, especially as renewables are becoming cheaper and more attractive, often even lower cost than coal, oil, and gas. With the Paris Agreement and related regulations, accountability in the management and distribution of energy resources is becoming increasingly important. Blockchain functionalities facilitate grid management at an unprecedented granular scale, with improved metering and security through cryptography. Smart contracts enable electronic billing systems with seamless payment processing and trusted data records. Tokenization also enables micro transactions, fractional ownership of energy assets by individuals. Ultimately, rapid settlement and data management can greatly benefit all stakeholders from individual consumers, energy asset owners, and operators.

i.) Carbon Markets

GBBC has produced a Green Economy Fact Card that visually summarizes the how blockchain advances carbon markets as a core component of green economic growth, which is low carbon, resource efficient, and socially inclusive. The Interwork Alliance (IWA), a GBBC initiative to advance the use of token-powered services, has also established the Token Taxonomy Framework (TTF), a set of standards to define common language, behaviors, and properties for any token value to be used and exchanged. The first major sector to adopt TTF is in carbon markets. The second and latest volume of the Voluntary Ecological Markets (VEM) Overview discusses how blockchain technology, digital assets, and tokenization can standardize, add credibility, and incentivize scale for carbon markets.

The market for carbon credits is expanding rapidly as organizations strive to meet the commitments of the Paris Agreement toward decarbonization. Demand is coming to outpace supply for verified offsets. Carbon credits are a category of renewable energy certificates (RECs), market-based instruments that verify ownership of a standardized amount of decarbonization format that can be traded as an energy commodity to offset emissions. The lifecycle begins with third party verification of the validity of the carbon credit, issuance of the credit upon review and registration by a registry, trade, and retirement upon redemption. This process involves significant accounting work that can be prone to double counting or selling, operational mistakes, system and market inefficiencies, transaction costs, and lack of transparency. The blockchain Chia Network, which prioritizes sustainability, security, and consumer protection, is increasing access and fostering global inclusion in carbon markets. Tergo has developed a solution to ensure high quality and reliable carbon credits. Xange is also implementing blockchain solutions for climate accounting.

Blockchain technology and digital assets can bring integrity to this growing but often fragmented market, where it has been challenging to standardize units of referenced products to derive market pricing and to verify and confirm quality of carbon credits and emissions tracking. A blockchain-based infrastructure enables interoperable trading systems where tokens representing standardized amounts of greenhouse gases removed, sequestered, or avoided can be verified, priced, and transparently traded, such that they can be removed from the marketplace upon being consumed. Smart contracts can ensure seamless digital transactions across organizations, while auditability can facilitate reporting and providing certificates to regulatory authorities upon surrendering carbon credits. A blockchain-based marketplace can function as follows:

1. Smart meters can post decarbonization data send it to a registry for minting carbon credits
2. All trades are recorded on a blockchain, providing a strong audit trail
3. Settlement occurs instantaneously, either through cryptocurrencies or traditional bank transfers recorded on the blockchain
4. Upon retirement, carbon credits are burned on the blockchain, and thus permanently destroyed
5. Beneficiaries of carbon credit retirement can be issued a non-fungible token (NFT) to attest to their consumption

ii) Decentralized Energy Markets

Blockchain technology enables decentralized energy markets with agile pricing based on supply and demand. The flexibility of this energy model is a natural fit for renewables like solar and wind, where energy is delivered in intermittent spurts and often originates from numerous remote locations that may not be co-located with major power stations. Locally produced energy can be utilized efficiently, and the excess can be absorbed by the grid.

At a local level, individuals can own small-scale power sources and benefit from any offtake, trade power directly with each other in a peer-to-peer manner, take part in energy investments such as project finance opportunities with an upside, and decide to time their energy consumption at lower price points. Consumers can also be producers and owners of fractionalized energy assets through tokenization, where a blockchain-based platform can optimize metering data and network assets for near real time remuneration of asset owners. These solutions are being implemented to balance a constrained grid and allowing a democratization of energy access that puts individual consumers at the center and benefits economic growth for lower income communities. Powerledger and 2Tokens are examples of entities advancing these solutions.

IV) Supply Chains

Blockchain technology enables an unprecedented degree of transparency in supply chains, reducing data silos and connecting the journeys of data on an item's production, transportation, and delivery to the end customer. This can provide a full view that guarantees the legitimacy of a brand, the authenticity of materials used in production, and fair labor practices throughout. Consumers are increasingly demanding fair practices in the production of their purchases, and regulations are increasing sustainability requirements for business operations. In order to remain compliant, large corporates may embed these sustainability requirements into their contracts with vendors and suppliers, so as to trickle across their supply chains. They are turning to blockchain technology in order to verify and monitor that their supply chains remain responsible.

The entire transportation industry can benefit from transparent supply chains, which would significantly impact the entire commerce ecosystem including carriers, suppliers, shippers, customers, and other stakeholders. Global trade is currently far from transparent or efficient, involving complex transactions with multiple documents and entities. This increases the risk of delayed payments and verifications, as well as vulnerability to fraud. In addition, there is a global trade financing gap in the trillions. Blockchain technology can streamline processes with shared data and secure access for authorized network participants, reduce time and paperwork, and provide a single source of trust for vendor verifications. Companies, particularly small and medium enterprises, can benefit from increased access to markets to maximize business opportunities and contribute to competitiveness and economic growth.

In this context, electric vehicles (EVs), which are increasing adoption with additional EV charging infrastructure and cheaper models introduced in the market, can be a major climate change solution because they include large batteries with enough storage capacity to smooth energy disparities between peaks and troughs of renewable energy supply. These batteries allow owners to purchase energy at times when it is abundant and cheap, and sell it to the grid when it is scarce and expensive. Blockchain technology can streamline EV charging transactions and processes, storing financial information securely so as to manage processes effectively and without the risk of nefarious interference. Circulor has developed a blockchain-based traceability solution that is addressing the growing need for vehicle producers to prove the raw materials that go into vehicles and how sustainably they are produced. Its solution is being used by Volvo, providing visibility from cars to the cobalt mines where these minerals were sourced from.

2. *Goals, sectors, or applications where digital assets introduces risks or harms*

2a. Bad Actors

As with any other technology or tool, blockchain technology can be utilized by bad actors for nefarious purposes. Criminals have proven historically to be early adopters of new technologies, and there exist risks of misuse across the blockchain technology and digital assets landscape discussed above. Anonymity features including cryptography, privacy coins, and mixers can be exploited to conceal the identity of individuals committing crimes and conducting illicit fund transfers.

- Illicit activities and terrorist financing can demand payments in cryptocurrency sent to anonymous wallets, making use of the efficiency and low cost of fund transfers all over the world.
- The cryptocurrency mixer Tornado Cash, whose privacy features obscured the trail of funds to the original source by "mixing" potentially tainted coins with others, was sanctioned by the US Treasury for hosting criminal transactions at a cost to society.
- In addition, because one's private keys grant access to one's cryptocurrency, hackers can steal these keys from custody providers or individuals themselves, and thus gain access to steal their funds.
- Finally, because blockchain is only a ledger of data records, the concept of "garbage in-garbage out" applies when nefarious individuals may enter wrongful data onto blockchain records, such as "Mickey Mouse" as the owner of a shell company running illicit businesses.

2b. Technical Vulnerabilities

With respect to technical vulnerabilities, smart contracts may also be prone to failure. Unforeseen consequences from a smart contract not operating as intended can be attributed to unintended human error or intentional malicious activity.

- Undesired outcomes can arise from technical elements within smart contract code or the oracle data sources they utilize, such as code errors, backdoors, errors or manipulation from external oracles, or other mechanisms.

Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

3a. Tracking & Tracing

The immutability and transparency of the blockchain ledger provides the opportunity to implement effective tools to detect the flow of funds and trace transactions. The history of activity is permanently recorded and openly available openly. These records, when inputted into sophisticated algorithms using Artificial Intelligence and Machine Learning, can draw patterns of fund flows and detect suspicious activities. These algorithms can connect the trail of funds to the individuals behind these nefarious activities. Any numbered account identified for criminal activity can be traced to provide data, which can be useful for law enforcement purposes. Companies like TRM Labs, Chainalysis, Elliptic, and CypherTrace have built such algorithms to successfully identify major crimes committed using blockchain technology, and many government organizations around the world utilize their technology for investigations. The Blockchain Alliance, an education nonprofit, is working with enforcement agencies to solve novel issues that blockchain technology and digital assets present. There is still opportunity for R&D on the use of these specialized cryptocurrency AML compliance and intelligence/blockchain forensics tools in the following areas:

- Sectors of heightened risk such as DeFi, bridges, and cross-chain activities
- Use of these tools may be limited in certain jurisdictions, leading to potential blind spots
- The effectiveness of algorithms may become outdated if new patterns of criminal activity arise and go undetected – hence the need to constantly monitor outcomes.
- A holistic end-to-end view of fund flows across chains, even when there is use of privacy coins or mixers, may also provide challenges and add to R&D needs
- Lack of interoperabilty across systems may still lead to data silos that may add risks. For instance, a medical professional, police officer, teacher, or any licensed professional charged for malpractice in one state may move to another state and conduct activities.

3b. Data Privacy & Security

Security and privacy of personal information are crucial features underlying successful blockchain applications, from digital money to energy grids and financial transactions. Encryption, public/private key cryptography, and anonymous signatures, features inherent to blockchain technology, can advance a new level of data security that doesn’t require centralized data repositories to hold vast amounts of confidential data, such that they remain vulnerable to misappropriation attempts. Privacy preserving tools like zero-knowledge proofs can provide proof of a value without conveying additional or unnecessary sensitive information. In combination with hashing, where blockchain records are posted as anonymized record identifiers, they allow pseudonymous data to be posted on the blockchain, with the possibility of temporary de-anonymization restricted only for authorized parties to justify causes for investigation, and re-anonymization.

Blockchain's security features can ensure resiliency of information systems, trusted data, and transparency across a number of sectors. The global anti-corruption movement can greatly benefit from these security features of the blockchain, as discussed in the GBBC co-authored report [In Pursuit of The Hidden Economy](). Global taxation systems can also benefit from blockchain's security features, which allow individuals to own their personal data and decide to share it for a taxable event (e.g., purchase) only to authorized government authorities, as illustrated in GBBC's [Blockchain for Taxation]() fact card series.

Advances in digital identity are also utilizing these privacy features, safeguarding owners' right to control their personal data, where blockchain technology can safeguard data privacy and make it available only as necessary. This benefits inclusion and human agency, especially for underserved populations, increasing access to financial services and basic needs. It also benefits institutions, rebuilding public trust, reducing costs, and enhancing AML/KYC integrity.

Finally, in the energy space, security of grid systems is paramount given increasing cybersecurity risks. In a model of centralized data repositories, the risk of compromising or hacking public utilities' data systems can have catastrophic consequences that endanger access to basic services for entire communities.

It is important to test any vulnerabilities that may arise from implementing privacy-preserving technologies. With the increasing sophistication of cryptographic tools, the bar is rising to draw the distinction between pseudonymous vs. anonymous data. For pseudonymous data, it is possible to obtain the original information; for anonymous data, it is not. Personal data should be posted on the blockchain ledger in pseudonymized form, such that the natural person behind it can be identified. Research should address the following:

- Risks of unauthorized parties reversing a hashing function to obtain the underlying confidential information, either through reversal engineering or via data analysis.
- Effectiveness and application of zero-knowledge proofs
- Applicability and current practices for screening users upon onboarding, KYC practices, and any thresholds below which KYC is not conducted
- Use of digital signatures should be considered for verification purposes

3c. Technical Resilience

There is a hardware and software element to technical resilience. Execution of smart contracts as automated transactions should be seamless.

- Research should cover causes behind technical vulnerabilities, frictions, or inaccuracies with respect to oracles
- Research should address questions regarding who should be held liable in case of harm, including unforeseen harm, in the performance and execution of a smart contract

3d. Reliable Data

It is imperative to ensure quality data gets recorded onto the blockchain, which will require vetting any third parties and individuals entering such data. It would be beneficial to study:

- The availability and effectiveness of audit firms
- Quality of data that gets inputted into the screening algorithms

4. R&D that should be prioritized for digital assets

4a. Taxonomy

Common language is first and foremost a priority to enable collaborative developments. Universally accepted definitions are paramount to ensure constructive collaboration across stakeholders necessary for scale. As the space develops at lightning speed, where definitions can evolve at the pace of new applications being launched, common understanding has become both increasingly critical and progressively complex. GSMI has produced a crowdsourced taxonomy with 182 terms specific to blockchain technology and digital assets, with crowdsourced and standardized definitions that capture the full meaning of each concept as it is utilized in the industry today. Just over half of these terms encompass core concepts for blockchain technology, while the rest are categorized as terms specific to sectors where this technology is already bringing major changes – finance, environmental initiatives, digital identity, and supply chain. R&D should prioritize:

- Convergence of definitions and potential inconsistencies, gaps, or areas of misalignment
- Sectors in need of common language
- Existing definitions and their adoptions
- Advances in collaborative developments that may enhance regulatory clarity

4b. Standards

Technical standards are fundamental to ensure safety, reliability, and continued innovation. Global cross-border coordination is essential for the development of the space. Standards establish common guidelines, definitions, and rules through technical criteria, specifications, methodologies, and practices which all serve to ensure adequate functionality alongside interoperability, trust, and ease of use necessary for stakeholders to work together. Collaboration is fundamental for the growth of an industry, in ways that will ultimately lead to widespread acceptance of formalized rules and regulations. GSMI has compiled a repository of 50 technical standards bodies, providing an objective overview of the state of standards developments for blockchain and digital assets. R&D should prioritize the following:

- Convergence of standards and any potential inconsistencies, gaps, or areas of misalignment
- Intended outcomes of standards including codes of conduct (e.g., standards and best practices, governance frameworks, etc.), sets of technical specifications (e.g., engineering design and code), or a regulatory focus (e.g., compliance, regulatory developments and necessary conditions prior to regulatory enforcement)
- Advances in collaborative developments that may enhance regulatory clarity

4c. Tokenization

In the context of the use cases discussed in Question 1, tokenization should be prioritized in R&D as a tool to improve efficiencies in existing financial markets and create opportunities for new markets such as energy markets. Tokenization can represent any form of value on a blockchain, potentially bringing liquidity to otherwise illiquid assets. The blockchain Hedera has implemented TTF discussed above to standardize the wide range of applications built on its protocol. R&D should prioritize the following:

- Standards frameworks to facilitate interoperability and scale for a token-based economy. TTF is currently being successfully implemented across various sectors and provides an example of components to consider.

5. Opportunities to advance responsible innovation in the broader digital assets ecosystem

5a. Regulatory Developments

Regulatory developments are a fundamental driver of responsible innovation and are continuing to take form for blockchain technology and digital assets, as government bodies increasingly recognize the role of this technology in financial markets, infrastructure, and all economic sectors. The growth of this technology can benefit greatly with increasing regulatory clarity, a harmonized approach across jurisdictions so as to minimize regulatory arbitrage, and a balance that will support innovation in a way that fosters inclusion without forsaking security and protections for consumers and investors. Government bodies are increasingly taking part in discussions and assessments for regulatory requirements, regulatory sandboxes are facilitating testing environments, and enforcement actions and case law are setting new precedents for the legal treatment of this technology.

GSMI has compiled an interactive map of regulatory developments for blockchain technology and digital assets across 210 jurisdictions. These include sovereign countries, monetary unions (European Union and African monetary unions), and states (US states). Regulatory developments span a wide range of issues where responsible innovation is front and center (e.g., central bank digital currencies, banking, financial surveillance, consumer protections, taxation, etc.) and take various forms including legislation, circulars, official statements, and guidance released by government bodies. The most common areas of focus have been comprehensive regulatory frameworks, financial surveillance including AML/KYC, and consumer protection. Enabling statutes that support rather than stunt innovations will be most successful in the long term to foster responsible innovation.

Several landmark regulatory developments are already shaping the trajectory of innovations, such as the European Union's Markets for Crypto-Assets Regulation (MiCA) and the United States White House's multiple reports following the Executive Order on Ensuring Responsible Development of Digital Assets. Many regulatory approaches are underway around the world as a result. Successful frameworks in one jurisdiction serve not only to attract blockchain technology and digital assets activities to pursue registration and boost economic activity, but also provide learnings for other jurisdictions to consider.

5b. Collaboration

GBBC members have actively engaged in dialogue on how regulators can protect the interests of citizens without creating obstacles that would stifle innovation, which would ultimately drive away innovation in a "flight to the bottom" to other jurisdictions with the least number of regulatory requirements. GBBC has actively engaged with leading global regulatory bodies, as well as national regulators and trade delegations around the world, providing consultation responses, working groups that lead to standards and best practices, and meaningful conversations including closed-door meetings between authorities and key industry stakeholders that have led to promising initiatives for the space.

- Response to the OECD on the crypto-asset reporting framework and amendments to the common reporting standard
- Response to Updated AML FATF Guidance
- FSB Consultation on International Regulation of Crypto-Assets Activities
- Industry Roundtable with BIS and IMF
- GDF IOSCO Membership

US regulators, on a bipartisan basis, are already benefitting from participation in roundtables and tailored meetings, which provide input to develop the most effective regulatory framework.

- Governance in a Digital Age Panel with Superintendent Harris of the New York Department of Financial Services
- GBBC CEO Testifies at US Senate Committee on Agriculture, Nutrition, and Forestry
- Unlocking the Future of Finance Panel with SEC Head of Strategic Hub for Innovation and Financial Technology Valerie Szczepanik
- Fireside Chat on Regulation and Risk with CFTC Caroline Commissioner Pham
- Government Accountability Office closed door session
- Discussions with state regulators
- Discussions with US agencies

5c. Education & Training

As blockchain technology scales and transforms business models are carried out, there's a need for adequate education and training for a future workforce to implement these innovations correctly. Education and training can also help retain new jobs in blockchain technology and digital assets within the United States, safeguarding domestic supply chains and strengthening security measures to prevent abuse from bad actors. Ultimately, unlocking the value of this new technology in the most responsible and effective should depend on making training accessible to the mainstream population, with an inclusive approach that ensures jobs are not lost but replaced with better opportunities to lift communities economically.

Blockchain technology is being increasingly incorporated into the curriculum taught at universities and other educational institutions around the world, offering academic degrees and other certifications. GSMI has compiled a repository of over 700 courses spanning multiple academic disciplines, which is meant to serve as a resource for students and professionals looking to get a access quality training, as well for educators and researchers looking to share knowledge and collaborate.

6. Other information that should inform the R&D Agenda

6a. Public-Private Partnerships

Collaboration across public institutions, which set safeguards and compliance requirements, and private parties, which advance technological developments, will be fundamental. Innovators can better understand how licensing can impact the technology, as well as opportunities to create and test better products in a compliant manner. Regulators can better understand how decentralized governance mechanisms and other novel issues presented by blockchain technology and digital assets can be integrated within existing regulations or necessitate new rules.

VIA ELECTRONIC SUBMISSION
March 3, 2023
White House Office of Science and Technology Policy (OSTP)
[redacted]
United States
[redacted]

SUBJECT: OSTP Request for Information RFI - Digital Assets Research and Development [88 FR 5043 / Document Number: 2023-01534]

Dear Sir or Madam,

The Global Digital Asset & Cryptocurrency Association ("GDCA") welcomes the opportunity to comment on the US Federal Government's National Digital Assets Research and Development Agenda. We are pleased to see the White House taking note of the transformative power of Distributed Ledger Technologies (DLT) and digital assets, which are revolutionizing the way we interact with each other and with businesses. This recognition demonstrates a forward-thinking approach to the rapidly evolving digital landscape and a commitment to leveraging cutting-edge technologies to drive innovation, promote transparency, enable secure financial inclusive opportunities, and enhance economic growth.

About GDCA

The Global Digital Asset and Cryptocurrency Association ("GDCA") is a global, voluntary Self-Regulatory Association for the digital asset and cryptocurrency industry. It was established to guide the evolution of digital assets, cryptocurrencies, and the underlying blockchain technology within a regulatory framework designed to build public trust, foster market integrity and maximize economic opportunity for all participants. In defining the membership base, GDCA has sought to ensure representation from the many actors comprising and adjacent to the digital assets and cryptocurrency ecosystem. Our broad-based membership pulls from all facets of the ecosystem, and includes spot and derivative exchanges, proprietary trading firms, investors, asset managers, brokerage firms, custodians, decentralized technology organizations, banks, legal firms, audit firms, insurance professionals, academics, consultants, and others. GDCA is now made up of approximately 80 entities from around the world, most of which are based in the U.S.

Overview

By acknowledging the potential of DLT to create decentralized systems that empower users and promote trust, the White House is paving the way for a more equitable and efficient digital economy. Further, these technology applications have the power to not only enable greater digital engagement, but also provide tools that better protect individuals, households and businesses as they interact in a native web-based environment with capabilities that bring transparency, privacy and security in tandem. This includes providing critical banking services to millions of underbanked Americans and reducing costs to the un-/under-banked individuals by up to 80%. This positive step will inspire further dialogue and collaboration between policymakers, industry leaders, and technologists to build a more resilient and inclusive future for all.

Below are responses to the topics addressed in the Request for Information from the Office of Science and Technology Policy. We have limited our responses to topics 1 and 4, so as to provide both sufficient background and reasoning for the ideas presented as well as to remain well within the page limits provided.

GOALS, SECTORS, OR APPLICATIONS THAT COULD BE IMPROVED WITH DIGITAL ASSETS AND RELATED TECHNOLOGIES.

ECONOMIC GROWTH AND JOB CREATION

Digital asset technology presents a tremendous opportunity to enable financial inclusive opportunities that extend the reach of the US dollar and its economy all over the world. The decentralized web has already transformed employment in the US technology sector**.** As of 2021, there were over 18,000 active decentralized web developers, and the market is expected to grow by an estimated 43% per year[1] during the next decade. According to LinkedIn, job postings for positions in Web3 grew 395%[2] from 2020 to 2021, outpacing the wider tech industry by four times. Although the majority of Web3 jobs are in software and finance, adjacent services like accounting are also experiencing significant demand.

The demand for talent spreads across company size coming from both the largest US companies in technology and finance, as well as nascent startups. Crunchbase, the leading aggregator of early stage company investments, estimates that since the second quarter of 2021, venture capital and private equity funds have invested $40 billion into emerging Web3 companies[3], and with the maturity and greater adoption of Web3 applications, the nascent industry could grow to account for 1 million jobs by the end of the decade.

The US is also home to the lion's share of financial technology and alternative financial services companies in the world. Here are a few statistics to consider from research conducted by Circle, Uniswap, TRM Labs, the World Bank and others:

- Decentralized finance payment rails utilizing stablecoins could reduce costs to the un-/under-banked individuals by up to 80%. The US could enable more underserved populations in remittance corridors (which accounts to roughly 3 times foreign aid/official development assistance) with a radically reduced cost for services and helping to achieve a marquee sustainable development goal.

- According to TRM Labs, approximately 99% of fiat backed stablecoin value is associated with the US dollar[4]. One of the most stable, liquid and transacted USD backed stablecoin is USD Coin or USDC which has grown in circulation by 860% since 2018.

- As global transaction volumes grow—including corporate payments, trade finance, etc.—the ability to transact in near real time with a USD-backed asset, in a programmable way, we can extend US financial and banking power globally even when traditional banking is 'off-hours'. GDCA members like GoQuant have partnered with industry leaders to provide low-latency digital asset market data 24 hours a day, allowing for significant increases to potential industry profits and positively contributing to America's economic outlook.

- With over $45B of USDC in circulation backed 80% in short dated (3-month) Treasuries and the balance in USD cash across eight US-banking partners and in segregated accounts, users are easily able to redeem USDC and use it as interoperable as cash for day to day transactions where

[1] Financialnewsmedia.com, "Global Web 3.0 Market Size Expected to Reach $81 Billion by 2030 as Branding & Marketing Needs Increase."
[2] "LinkedIn News on "Work Shift Labor Market Activity."
[3] Metinko and Metinko, "Web3 Funding Sees Huge Drop As Big Rounds Dip."
[4] "TRM's Ari Redbord Testifies before the U.S. House Committee on Financial Services | TRM Insights."

the 'holding' of value and associated liquidity and market volatility risks remain low. Users of USDC are operating in an extended US dollar domain, but unlike use of cash transactions, USDC transactions can be driven 24/7 by users anywhere in the world, and whose tie back to reserves in USD cash and Treasuries reinforces the backing by the US.

- According to McKinsey[5], the decline in the use of hard cash continues and was expedited during the pandemic, with Circle estimating that $30B of economic activity was facilitated with approximately "15% being wallet-to-wallet transactions (compared to 2% for non-financialized transfers in traditional payments)[6]." As global remittances continue to grow—and at double digit rates in many countries[7]—the 'income economy' that enables cross-border flows in near real time and cheaply continues to be a major concern. Increasingly, every day transactions are happening digitally – more so with tokenized value – which means the extension and reach of tokenized value will increasingly become more mainstream and allow direct facilitation (aid, government stimulus, balance of payments, etc.) of transactions including by and between government entities and private sector businesses and individuals.

Sustainable Climate Investing

The use of digital assets along with the transparency of DLT can significantly improve the landscape for sustainable investing, increasing the flow of investment to sustainable projects, enabling the tracking of their impact and creating liquidity for new impact-linked securities. Despite the growth of sustainable investing over the past decade, the industry is now facing challenges due to its lack of transparency and a distrust by investors skeptical of "greenwashing", meaning investment products that are labeled as sustainable but do not offer the impact they have promised. Meaningful, sustainable investments into projects that fight climate change and reduce greenhouse gas emissions are critical to our nation's security and prosperity.

Specifically, the United Nations Framework Convention on Climate Change[8] has identified the following ways in which DLT and digital assets can accelerate the efforts to combat climate change. They include:

- Improved carbon emissions trading where carbon assets are recorded on a public ledger to ensure transparency.
- Peer-to-peer trading platforms for trading of renewable energy. The platforms would allow the purchase or sale of renewable energy using tradable digital assets representing a certain quantity of energy production.
- Enhanced climate finance flows including DLT-supported investment frameworks that ensure financing is allocated to climate projects in a transparent way with their impact monitored, tracked and recorded.
- Better tracking and reporting of greenhouse gas emissions reduction to avoid double counting.

New tokenization frameworks have made it easier to successfully invest in and track sustainable projects. For example, the Guardian framework, offered by Hedera Hashgraph, is an open source policy workflow engine that tokenizes climate assets, such as offsets and emissions. The framework provides auditable, traceable, reproducible records that document the emissions process and the lifecycle of carbon. More recent work into Automated Regression Market Makers (ARMMs) also allows for price discovery of semi-fungible digital assets such as carbon tokens, allowing market makers to provide liquidity and incentivizing greater investment into such projects.

[5] "Accelerating Winds of Change in Global Payments,"
[6] "Circle Releases First Annual 'State of the USDC Economy' Report."
[7] "Remittances to Reach $630 Billion in 2022 with Record Flows into Ukraine."
[8] Ultimate Nations Climate Change, "How Blockchain Technology Could Boost Climate Action."

Logistics

The global supply chain is paramount in today's interconnected and interdependent economy, however, several challenges impact the efficiency and effectiveness of today's supply chains which could be solved through the use of DLT. Participation of multiple states and countries makes it difficult to manage and coordinate all parties involved and the lack of visibility into the supply chain can make it difficult to track progress and identify bottlenecks.

Below are example of how DLT can improve global supply chain processes:

- Automate recordings of delivery times and receipt of goods into inventory
- Automate payments for inventory received and enable 'programmability' as inventory/goods are delivered to which payments would immediately be processed and settled into vendor accounts/wallets
- Automate recording of commodity transfers between supply chain members from the factory to the consumer.
- Alert relevant parties if the commodity held in inventory will expire or if the price of the commodity has met a strike price.
- Execution trade deals automatically by connecting importers, exporters, and their respective banks to the DLT to reduce duplicative paper and redundant quality assurance processes through the programmability of smart contracts.

DLT can provide increased traceability of commodities, improve transparency across the supply chain, and enable the automation of payments—businesses can track the movement of commodities in real-time and when paired with smart contracts (self-executing agreements that automatically enforce the contract terms when conditions are satisfied) can increase efficiency, reduce the risk of error and provide valuable insights to make data-driven decisions. TruckCoinSwap, an innovative fintech transportation company and GDCA Member Firm, have introduced an original use for digital asset technologies in the logistics sector by purchasing invoices directly from transportation workers and companies, providing immediate liquidity via tokens, and settling the outstanding invoices directly with the shipper. TruckCoinSwap places the expected industry savings due to the reduction in intermediary and transaction costs at $3 billion. By improving the profitability of our transportation industries, we can expect greater consistency in the results that the industry provides - food on our nation's kitchen tables, stocked medicine shelves, and fuel to power our cars, homes, hospitals and schools.

Access to Finance (for businesses and individuals)

Over the past decade, innovation in securities regulation, such as the Regulation A crowdfunding registration exemption for small and medium sized companies (SMEs) to sell their securities to the public, has made it cheaper and less burdensome for these companies to raise capital. The benefit of the Regulation A crowdfunding framework is two-fold: 1) it allows SMEs to raise capital on similar terms to the public markets and scale more efficiently, and 2) it gives the public access to high yield investment opportunities previously accessible only to institutional and accredited investors. For example, Regulation A has made it possible for retail investors to access competitive risk-adjusted returns from financial products such as real estate and private equity, which were previously only available to institutional and accredited investors.

Despite the positive impact of crowdfunding vehicles for both SMEs and retail investors, their lack of liquidity and transparency have hindered adoption on a larger scale. At present, investors can redeem their shares on specific dates only and the vehicles lack transparency into their holdings and prior transactions. Tokenizing shares of the investment vehicles would allow those shares to be traded on a decentralized exchange, making the sale and purchase of shares easier, and would allow for a corresponding audit trail of those transactions stored on a decentralized ledger. Further embedding AML/KYC controls through the application of digitally verifiable credentials, would also automate the client and counterparty verification process as tokenized shares and corresponding value was sent and received. Such a process builds trust and transparency into the holders and holdings of an investment vehicle, improves the process of raising capital for SMEs and facilitates the adoption of new crowdfunded investment opportunities for the public.

FINANCIAL INCLUSION

(FOR INDIVIDUALS AND ENTITIES/BUSINESSES - UNBANKED / UNDERBANKED)

According to a 2019 report by the Federal Reserve[9], 22% of American adults (63 million) are either unbanked or underbanked. In this vein, Decentralized Finance (DeFi) and digital assets have the potential to help the unbanked and underbanked meet their financial services needs without using alternative financial services products that can be both costly and predatory. Unbanked adults do not have a checking, savings or money market account and 40% use some form of alternative financial services – such as money order, pawn shop loan, auto title loan or payday loan. The underbanked include those who may have a bank account but also (primarily) use an alternative financial service product. According to the 2021 FDIC Survey of Unbanked and Underbanked Households,[10] the main reasons people are underbanked are because they can't meet minimum balance requirements, the lack of trust in banks, privacy concerns and high banking fees.

Financial services that can be facilitated by decentralized finance include the ability to make payments, store and transfer funds, and borrow and invest through peer-to-peer and community lending–all at low to no cost and with minimal friction of engagement with and through traditional bank and nonbank financial institutions. These services can be accessed through a mobile phone, with fast transfer times and often at a fraction of the cost of traditional banks.

Part of this effort should include a recognition of the attributes of DLT that provide new mechanisms in banking and payment processing that can support marginalized populations in furtherance of US national and international economic security interests. Disparaged communities, including those in areas of conflict or humanitarian disarray, can be enabled with funding through digital wallets equipped with virtual assets including USD-backed stablecoins with connectivity to US based bank accounts. These assets ensure access to vital economic resources, as well as the ability to engage in peer-to-peer (P2P) transactions between individuals and merchants providing essential services. Blockchain technology is a powerful tool for nonprofit, non-governmental, and intergovernmental organizations working to deliver aid, and especially so for the recipients in their time of need.

Often, anti-money laundering/financial crimes compliance (AML/FCC) is cited as a cost and efficiency barrier to driving inclusion efforts given the risks of engaging potentially malign or illicit actors. Alternative, decentralized, web-native financial services applications and cryptographically tokenized value systems built on distributed ledger technology carry essential attributes to enhance the core elements of financial system integrity, and therefore help modernize essential AML and consumer protections that are required to enable equitable and secure access. Many in the digital asset industry such as GDCA Member Firm Finclusive, have been working proactively to develop and implement comprehensive frameworks for AML/FCC–such as the industry led Rulebook[11]–that better align with the technological and operational

[9] "Banking and Credit,"
[10] "2021 FDIC National Survey of Unbanked and Underbanked Households."
[11] Driven by the industry and informed by global regulators and policy makers, the "Rulebook" is a dynamic framework that reflects the operational realities of P2P/Defi/web3 and blockchain-enabled payment and exchange networks and builds upon existing governance and data privacy rules from the following organizations:

- Financial Action Task Force (FATF)
- Society for Worldwide Interbank Financial Telecommunication (SWIFT)
- National Automated Clearing House Association (NACHA)
- National Institute of Standards and Technology (NIST)
- European Union's General Data Protection Regulation (GDPR)
- Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures (CPMI)

realities of web-based/blockchain-enabled financial activities, and in keeping with the international standards for AML/FCC.

Further, they provide the appropriate tools for law enforcement and regulators to proactively combat—and interdict—financial crimes and illicit/malign actors who perpetrate them, which is essential in driving confidence in the security of financial transactions, and the appropriate consumer protections inherent in driving trust in financial services. DLT's underlying attributes reaffirm these core principles including their being permissioned, distributed, privacy enhancing and immutable – enabling essential controls, transparency and auditability in both the proactive enablement of system integrity and in the advancement of law enforcement and financial regulatory enforcement essential to manage AML/CFT objectives in tandem.

Housing Equality

According to the Federal Reserve[12], the largest source of wealth for the average American is their home and while many Americans today struggle to access the housing market, digital asset technology has presented new and unique ways to reverse this course. For Americans in the bottom 50% percentile, their home accounts for over 60% of their total wealth. In addition to being a primary source of wealth, higher homeownership rates have been shown to reduce crime, improve school performance and build resilient communities. Unfortunately, the US faces a large disparity in homeownership rates. According to the US Treasury[13], as of the second quarter of 2022, the homeownership rate for white households was 75% compared to 45% for Black households and 48% for Hispanic households. Saving for a down payment is the single biggest barrier to homeownership with over two-thirds of respondents from the Urban Institute's Policy Center[14] study citing it as their biggest obstacle.

Digital asset technology such as blockchains have also produced unique opportunities to access homeownership. GDCA member Safe Rate is a mortgage marketplace platform built on blockchain which offers a flexible mortgage product that provides homeowners with automatic payment reductions in difficult times. By leveraging blockchain technology, Safe Rate is helping drive sustainable homeownership in the US which in turn supports a more stable economy.

Decentralized finance has the opportunity to increase the number of homeowners by helping prospective homebuyers save for a down payment more quickly and efficiently. Prospective homebuyer s can directly invest into low-risk, fixed income assets such as US Treasuries and mortgage-backed securities that offer significantly higher yield than traditional savings accounts to more quickly save for a down payment.

Payments are tracked and audited on a distributed ledger, offering greater transparency than what is provided by banks and other savings products today, and decentralized exchanges allow for the sale and purchase of shares providing price discovery and liquidity. Additionally, a decentralized approach to fixed income investing allows younger homebuyers who have more recently accumulated their wealth in digital assets, to access lower risk, fixed income assets in the decentralized ecosystem to responsibly save for a down payment.

R&D That Should Be Prioritized for Digital Assets

Given the large amount of private sector investment into decentralized technology, we encourage government research efforts to focus on use cases where there are inefficiencies in how consumers engage with both the government and the private sector, and create sandboxes to pilot new decentralized solutions that improve the lives of consumers. Below are use cases we have prioritized where the government can proactively work with private partners to improve the quality of life of

[12] "The Fed - Comparison: Compare Wealth Components across Groups."
[13] "Racial Differences in Economic Security: Housing."
[14] "Barriers to Accessing Homeownership Down Payment, Credit, and Affordability."

American citizens, including helping lower their costs, reducing the risk of fraud, and improving their quality of medical care.

Decentralized Identity

Verifying one's identity is essential to accessing fundamental services such as government programs, financial products, and medical care; this process can become even more secure through the use of blockchain and DLT. Traditionally, financial institutions run their own Know Your Customer (KYC), Know Your Business (KYB), and basic Customer Due Diligence (CDD) to Enhanced Due Diligence (EDD) processes to verify potential customers that would like to use their banking services. Unfortunately, the current process of verifying one's identity exposes individuals to mismanagement of highly sensitive data by multiple and often unknown parties, creates process and regulatory burden on private companies to securely manage the data, and creates the risk of theft and hacking of highly sensitive data which puts further burden on individuals, organizations, and the government.

Decentralized identity technology introduces the ability for the subject to take ownership in sharing this compliance information multilaterally with any financial institution they choose—enhancing essential privacy protection associated with personal identifying/entity identifying information (PII/EII), while providing a 'utility' for KYC/KYB verification near real time. The reuse of such information would decrease the cost and time required to securely onboard such a customer, while maintaining the subjects' control over their personal financial identity and account/wallet information. This empowers consumers with the authority to grant and withdraw their financial data, while streamlining compliance and decreasing costs for financial institutions. The result is a more widespread institutional adherence to regulatory compliance, as well as an overall increase in consumer data privacy and enabling secure and equitable financial inclusion–especially for those historically perceived as higher-compliance risk (e.g. low/moderate income, global poor, lack of financial/credit history, small businesses, international remittance and payments participants, etc.).

Consumer Credit Reports

The information conveyed in a credit report contains highly sensitive personal data and impacts both the approval and final cost a consumer incurs for rent, mortgage loans, automobile loans, and credit cards. DLT allow consumers to maintain a single verifiable identity on ledger that can be accessed and updated by parties who have permission. Currently, these reports are generated and managed by three main credit bureaus who aggregate and score data from businesses the consumer has previously used. However, this information is hidden from the consumer and often contains errors. To get a snapshot of their information or to dispute an error, a consumer must engage with each of the main credit bureaus, in an industry that still relies heavily on fax, phones and third parties. The process is time consuming, requires multiple follow-ups, and can jeopardize a consumer's ability to access necessary financial services and products.

DLT allow consumers to maintain a single verifiable identity on ledger that can be accessed and updated by parties who have permission. For example, instead of each credit bureau having a different set of information about a consumer stored on their servers, a consumer would have one on-ledger identity. Businesses that the consumer engages with can be given permission to augment the data, as with recent purchases, employment history, and other personal information. In this framework, consumers have a real-time snapshot of their digital identity, know what information has been shared, who it was shared by and when, and have the transparency they need to dispute inaccuracies.

Consumer Data Privacy

The current way of shopping for financial products leads to consumers losing access to their personal information, however, DLT can help put control back into the hands of the consumer by creating a standard means by which any business can access sensitive data. For example, with a decentralized identity, consumers can grant access to their personal financial information when they are shopping for a product or service, and revoke it once finished. Also, instead of having their full credit profile shared with businesses, consumers can give permission to a business to see only the information they need to make an accurate quote or approval. With decentralized identity, there is a single copy of a consumer's information with the information used, accessed and stored as-needed, and with consumers in control of that data.

Standardized Medical Record Keeping

In order to ensure an individual is receiving the best medical care, the parties involved, including care providers, insurers, hospitals, pharmacies, labs and others must operate on the same pieces of information which can be more securely identified, communicated and accessed through the use of DLT. Unfortunately, given the number of parties involved, and the sensitivity of the information, the fact that much of this information must be repeatedly collected and shared across providers means that there is a high risk of data degradation and inaccuracy. The federal government could conduct research on how to ensure a patient's medical record could be securely recorded and accessed across parties using DLT. This would ensure a higher quality of patient care and remove the many frictions that can occur in the onboarding and sharing of patient information.

Standardized Property Record Keeping

The federal government could consider research on how to drive adoption of DLT for management of property records given the many unrelated parties who may have claims to a property, ranging from lenders with loans secured by the property to home renovators who have mechanics liens, and the need for a single, accessible source of truth. Currently, consumers are still required to pay for costs like title insurance to ensure that their ownership in a property is properly recorded. Given the average title insurance policy ranges from 0.5% to 1.0% of a property's value, consumers are spending thousands of dollars per transaction to verify and protect their ownership in an asset they just purchased. Widespread adoption of DLT for property recording would reduce the administrative burden on settlement agents to verify ownership, reduce home transaction delays, and save consumers thousands of dollars on their home purchase.

Utility Operating Systems

DLT systems can add new levels of security to utility operating systems (UOS) by leveraging their inherent features of decentralization, immutability, and transparency. The use of DLT systems can enable UOS to quickly detect and respond to any changes or disruptions in the system. Smart contracts can be used to automate processes, enabling deterministic responses to predefined conditions. This can eliminate the need for human intervention, reducing the risk of human error and enhancing the reliability of UOS.

DLT systems can enhance the security of UOS by providing enhanced access control mechanisms. Permissioned DLT networks can restrict access to authorized participants only, ensuring that only authorized individuals can access and modify the UOS. This can prevent unauthorized individuals or groups from accessing or manipulating the system, reducing the risk of data breaches, cyber attacks, or ransomware.

Conclusions

As the White House Office of Science and Technology Policy (OSTP) moves forward and weighs the value of digital assets as well as considers key areas of emphasis for further research, we encourage the OSTP to embrace the transformative power of Distributed Ledger Technologies (DLT) and digital assets, which are revolutionizing the way we interact with each other and with businesses. With appropriate research and through nurturing responsible innovation oriented digital asset industry firms, our country may leverage cutting-edge technologies to drive innovation, promote transparency, enable secure financial inclusive opportunities, and enhance economic growth.

GDCA appreciates the opportunity to comment on this important proposal and welcomes the opportunity to respond to any questions or inquiries.

Sincerely,

[redacted]

Gabriella Kusz
CEO
Global Digital Asset & Cryptocurrency Association (Global DCA)

ADDITIONAL SIGNATORIES & CONTRIBUTORS
Shima Rayej
Co-founder and Chief Investment Officer, Safe Rate
Policy Fellow, GDCA

Amit Sharma
Founder and CEO,
FinClusive Capital

Daniel Lis
Director of Public Policy,
GoQuant

Adem Peters
Policy Fellow,
GDCA

Samuel Peters
Policy Fellow,
GDCA

GeoComply

March 3rd, 2023

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy,
Executive Office of the President

Eisenhower Executive Office Building
[redacted]
Via: Electronic submission - 88 FR 5043

Dear Rachel Wallace,

On behalf of GeoComply, thank you for the opportunity to comment in response to the Office of Science and Technology Policy's Request for Information regarding a National Digital Assets Research and Development Agenda. We appreciate the Office of Science and Technology Policy's willingness to garner input from the public and industry stakeholders to address technical complexities associated with the digital asset space.

Founded in 2011, GeoComply provides fraud prevention and cybersecurity solutions that detect location fraud and help verify a user's true digital identity. GeoComply's solutions incorporate location, device, and identity intelligence with advanced machine learning to detect and flag fraudulent activity. The company's software is installed on over 400 million devices worldwide and processes over 1 billion transactions per month, placing GeoComply in a unique position to identify and counter both current and newly emerging compliance and fraud threats.

This comment letter will address the Office of Science and Technology Policy's inquiries into the inherent risks of the digital asset industry addressed in topic two: "Goals, sectors, or applications where digital assets introduce risks or harms," including illicit financing, money laundering, financing of terrorism, and sanctions. The letter will also highlight how advanced geolocation intelligence -beyond IP address- can mitigate these risks. Accurate geolocation data signals serve as the basis of a robust compliance program. In the digital age, knowing a customer's true location is critical for determining

GeoComply

whether a platform has exposure to OFAC sanctioned or high-risk jurisdictions, AML/CFT risks, as well as enhancing a user's digital identity. Unfortunately, the rise of location-obfuscating technology, such as VPNs, TOR exit nodes, and DNS proxies, present risks to compliance-focused organizations, making it even more important to rely on advanced geolocation intelligence, such as GPS, Wi-Fi Triangulation, Cell Tower data, etc.

Illicit Finance & Location Obfuscation Risks

The illicit use of digital assets is a crucial concern for industry stakeholders and policymakers. While illicit use of cryptocurrency remains relatively small, with transactions involving illicit addresses representing 0.24% of cryptocurrency transaction volumes in 2022,[1] this percentage still reflects billions of dollars of transactions. As the crypto ecosystem develops into a mature pillar of the U.S. financial system, these percentages of illicit activity may become increasingly threatening should they go unaddressed.

The composition of illicit finance in the crypto ecosystem changed markedly in 2022. At the onset of Russia's invasion of Ukraine, the U.S. government imposed robust sanctions against the Russian economy. The growth of the U.S. sanctions regime in the last year correlates with an increase in the use of cryptocurrency to evade sanctions. Blockchain analytics firm Chainalysis estimates that 43% of all illicit blockchain activity in 2022 was associated with sanctioned entities, compared with relatively negligible crypto-based sanctions evasion in 2021.[2]

The use of crypto to circumvent financial restrictions has directly contributed to the undermining of U.S. national security objectives. For example, Alexander Lyubimov, Director of the Novorossia Aid Coordinating Center and prolific fundraiser for the Russian Military, has stated that "(The NACC) had PayPal once, but it had been blocked multiple times, and now it doesn't work as a tool for foreign donations anymore. A lot of people living far away want to support our work, and the only available way for them now is crypto...the group long ago figured out ways to avoid getting its crypto blocked by exchanges."[3] In short, digital assets flow into Russia from global markets and are used to purchase Russian military hardware. Such national security concerns necessitate an

[1] Chainalysis Team. 2023. The 2023 Crypto Crime Report. *Chainalysis*
[2] Ibid.
[3] Baydakova, Anna. 2023. Coins of War: How Crypto Keeps Feeding Russia's War Despite Sanctions. *CoinDesk*

GeoComply

evaluation of the illicit finance vulnerabilities present in the digital asset ecosystem, as well as an assessment of the robustness of jurisdictional compliance programs.

As part of the President's E.O. 14067, the Department of Treasury published an Action Plan aptly emphasizing the inherent vulnerabilities of cross-border virtual currencies opening financial transactions to a globalized market, including gaps in AML (Anti Money Laundering) requirements across foreign jurisdictions.[4] Further, the Action Plan describes how "in some cases, foreign-based VASPs have intentionally provided services to **U.S. persons without proper registration, including instructing U.S.-based customers to use a virtual private network to obfuscate their location,"** an act of non-compliance that constitutes "significant risk" and a violation of US laws and regulations.[5]

As highlighted by the Treasury's Action Plan, one form of location obfuscation is a Virtual Private Network (VPN). VPNs create a private connection between a user and its servers to hide a user's IP address, making it seem a user is somewhere they are not.[6] Virtual private network use skyrocketed at the beginning of the pandemic, with Surfshark estimating in 2022 that nearly a third of all Internet users use a VPN in 2022.[7] Although there are legitimate reasons to use a VPN, GeoComply's experience across varying industries demonstrates that obfuscating location, also referred to as location spoofing, is a common denominator of online fraud and compliance evasion.

The utilization of VPNs puts Virtual Asset Service Providers (VASP) at risk of non-compliance, especially jurisdictional violations. Moreover, location obfuscation via VPNs and other tools, such as DNS proxies and TOR exit nodes that manipulate an IP address, have been successful in bypassing compliance programs due to the financial industry's reliance on IP Addresses to detect a user's location. To put it into perspective, IP address technology is over 40 years old; it was first deployed in 1983.[8] 25 years later, in 2008, Apple released the iPhone 3G with GPS chips. Despite the availability of GPS geolocation data, a more accurate and reliable form of geolocation, to verify a user's location, the majority of the financial industry still relies on IP addresses for anti-fraud and

[4] US Department of Treasury. 2022. Action Plan to Address Illicit Financing Risks of Digital Assets.

[5] Ibid.

[6] Max Eddy, 2022. Why You Need a VPN, and How to Choose the Right One. *PC Mag.*

[7] Pijus Jauniskis, 2022. VPN statistics: Users, markets, & legality. *SurfShark, Cybersecurity and Internet Security.*

[8] Internet Assigned Numbers Authority (IANA). 2022. Number Resources. *Overview.*

compliance, allowing cybercriminals to easily circumvent jurisdictional restrictions as this technology is outdated and various workarounds have been developed since its inception.

For this reason, detecting accurate geolocation information has been codified as a key pillar of financial law enforcement. For example, in its Guidance on Digital Identity, the Financial Action Task Force (FATF) states:

"Digital ID authentication for authorising account access may enable regulated entities to capture additional information, such as **geolocation**, IP address, or the identity of the digital device used to conduct transactions. This information can help regulated entities develop a more detailed understanding of the client's behaviour as a basis for determining when its financial transactions appear to be unusual or suspicious, and may assist law enforcement in investigating crimes." [9]

However, location spoofing via a VPN is just the tip of the iceberg. Location obfuscation is done through a variety of tools that alter a user's IP address, GPS location, or other location data points. Cybercriminals leverage various forms of location-altering technologies to hide their location and, therefore, their identity, allowing them to conduct illicit activities in an anonymous manner. Advanced cyber criminals may employ a multitude of location obfuscation strategies such as Remote Desktops, Proxy Servers, TOR exit nodes, emulators, and jailbroken or rooted devices.[10] Location spoofing is a cybercriminal's first line of defense in the internet threat landscape, including bot traffic, cyber-attacks, account takeover, and identity theft.[11]

This cements the importance of further researching and developing analysis on the proliferation of these location-anonymizing technologies within the digital asset ecosystem as well as assessing the risks that they pose to compliance programs as well as the integrity of the U.S. financial system.

OFAC Sanctions & Jurisdictional Evasion Risks

Screening IP address is currently considered the standard in geolocation technology used by financial institutions (FIs), FinTech, and digital asset companies during onboarding and ongoing KYC for jurisdictional sanctions compliance and AML/CFT processes. This creates a compliance gap as IP Address is an easily manipulated and

[9]Financial Action Task Force. 2020. Financial Action Task Force's Guidance on Digital Identity
[10] GeoComply. 2021. Geolocation Compliance, KYC and Fraud Detection Solutions.
[11] GeoComply. 2022. Location Spoofing is the Root of All Fraud. *The Internet: Threats Landscape.*

GeoComply

highly inaccurate data point, making prevention of jurisdictional sanctions evasion or detecting money laundering a difficult task.

The importance of enforcing jurisdictional sanctions compliance has been recently highlighted by OFAC's enforcement actions to a range of companies, including virtual currency companies Bittrex, BitPay, and BitGo. In a recent enforcement action, Bittrex settled with OFAC for a little over $24 million, the largest settlement between OFAC and a VASP to date.[12] Instead of utilizing customers' IP address information received during the onboarding process to block sanctioned jurisdictions, Bittrex allowed transactions from sanctioned jurisdictions, including the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria.[13] However, insights derived from data are only as good as the quality of the data collected. A similar consent order was filed against Coinbase by the NY DFS in early January 2023, highlighting that:

"In addition to the SDN lists, OFAC maintains geographical sanctions against broad sectors of the economies of certain nations such as Iran, Cuba, Syria, Russia, and North Korea. Such prohibitions necessarily require a company like Coinbase to understand where its users are physically located. However, Coinbase allows its users to access its sites while using Virtual Private Networks ("VPNs") or The Onion Router ("TOR"). VPNs are a means of using a proxy web address as an interface between a user and a website. TOR disseminates web traffic across a distributed and anonymous network, such that the exit nodes for the network appear to be the user's web address. **Both methods allow a user to appear to be located in a jurisdiction other than that of the user's actual, physical location.[14]"**

This emphasizes the importance of detecting these types of location obfuscation tools as well as detecting the true location of a user to protect companies from sanctions evasion risks.

The current OFAC guidelines require companies to assess risk to determine whether location monitoring is necessary for compliance.[15] OFAC's enforcement actions against institutions that neglect to utilize IP address monitoring signals that regulators

---

[12] Department of the Treasury. 2022. OFAC Settles with Bittrex, Inc. for 24,280,89.20 related to Apparent Violations of Multiple Sanctions Programs. *Department of the Treasury Enforcement Release.*
[13] Ibid.
[14] NYDFS.2023. Superintendent Adrienne A. Harris Announces $100 Million Settlement with Coinbase, Inc. after DFS Investigation Finds Significant Failings in the Company's Compliance Program. *NYDFS Press Release*.
[15] Office of Foreign Assets Control. 2021. "Risk Assessment." *Sanctions Compliance Guidance for the Virtual Currency Industry.*

expect stronger frameworks addressing sanctions evasion. Although the IP address indicates a device's geolocation, it is susceptible to spoofing and lacks the accuracy of multi-source geolocation. The digital asset industry should implement advanced and readily available geolocation technology to comply with OFAC jurisdictional sanctions and block transactions originating from sanctioned jurisdictions.

It is incredibly difficult to comply with sanctions without accurate location data and geofencing sanctioned countries. By utilizing pinpoint accurate geofences VASPs and other FIs can prevent and block transactions from sanctioned regions that require increasingly precise accuracy, such as Crimea, the Donetsk People's Republic (DNR), and the Luhansk People's Republic (LNR) regions within Ukraine. VASPs and FIs can integrate multiple forms of location intelligence, which can include GSM, GPS, Wi-Fi triangulation, IP Address, and detection of location anonymizers (such as VPNs, emulators, RDPs, etc.) to meet the level of location accuracy required.

Conclusion

The highly anonymized nature of the crypto ecosystem demands more robust safeguards. A true risk profile and robust digital identity should incorporate multi-source geolocation data, including GPS information, Wi-Fi triangulation, GSM (cellular) data, and IP address monitoring, in addition to the detection of advanced location spoofing technologies.[16] Employing solutions that operate in the full breadth of the available data sources ensures that non-compliant persons and territories are obstructed from engaging with the U.S. financial system.

In summary, incorporating comprehensive multi-source geolocation data (GPS, WiFi Triangulation, and GSM data) into compliance programs yield numerous positive effects, such as

i. Facilitating more robust and reliable Know Your Customer (KYC) and Customer Due Diligence (CDD) processes to authenticate identity;

ii. Ensuring that suspicious activity can be monitored and prevented in real-time (for example, account location jumping, signaling account takeover);

iii. Creating an audit trail for improved reporting and traceability of all transactions;

[16] Ibid

GeoComply

iv. Supporting law enforcement and creating efficiencies in investigations;

v. Effectively geofencing FATF high-risk countries and sanctioned jurisdictions; and

Vi. Enhancing Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT)/Proliferation Financing (PF) compliance.

As FinTech and digital assets continue to globalize, so too will cybercriminals – and their ever-advancing techniques. The innovation of fraud prevention and compliance must race ahead of cybercriminal innovation. Multi-source geolocation data is a valuable part of authentication that helps digital identity verification, consumer authentication, and compliance by accurately determining the end user's location. It is a non-biased, privacy-preserving strategy to ensure compliance and fraud prevention by verifying the identity of end users. Geolocation and location spoofing detection are essential parts of creating a transparent and safe internet and digital economy for all.

GeoComply offers these recommendations with the aim of assisting the OSTP in its mission to ensure the responsible adoption of digital assets in order to protect the integrity of the U.S. financial system. Thank you for OSTP's long-standing commitment to advancing technology and innovation, and we look forward to continued collaboration on these critical issues.

Sincerely,

[redacted]

Anna Sainsbury
CEO & Co-founder
[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Glossi.fi

From: Donald Josey
To: [redacted]
Subject: Re: Request for Information: US Digital Assets R&D Agenda; across diverse use cases and technologies 02 09 12pm
Date: Thursday, February 9, 2023 1:17:49 PM

To whom it may concern-

I just wanted to follow up to express our intention to submit a comment to this RFI for digital assets R&D.

Our project Glossi.fi is an NSF funded startup whose mission has been closely related to several of the goals of the digital assets fast track committee from day one.

We have been working to prove that our research into smart contract-incentivized data marketplaces can drive more secure and user-friendly interactions at the point of transactions in the digital asset space. In essence, I think our project addresses the questions posed by the committee from two separate but important angles:

1. Proving the concept that incentivized Data Marketplaces (a novel implementation of Blockchain technology) are in themselves a value-add inherently on their own merit.

2. Demonstrating that those marketplaces can be used to provide UX value via enhancements of security and usability to users -- in particular helping to highlight and address digital asset risks to users at the point of the transactions.

Our alpha release is forthcoming within the next few months and in the meantime we are excited for the opportunity to engage with the committee whose questions we think are so closely aligned with our motivation behind what we do every day.

Thank you!
Don Josey
Founder @ Glossi.fi
[redacted]

On Thu, Feb 9, 2023, 8:58 AM Brady-Estevez, Anna S. [redacted] wrote:

> Dear Innovators and Colleagues!
>
> Recently, the White House Office of Science and Technology Policy (OSTP) and the National Science Foundation (NSF) publicly published a Request for Information on Digital Assets Research and Development. We are seeking comments to help inform the development of a National Digital Assets R&D Agenda.
>
> This R&D Agenda will help the United States better harness the benefits and mitigate the risks of digital assets and its underlying technologies. It will help ensure that sometimes-

overlooked topics like environmentally-friendly consensus mechanisms receive appropriate levels of R&D support. It will support research on developing new tools for detecting and mitigating risks from digital assets. It may help illustrate how to design a U.S. Central Bank Digital Currency (CBDC) system that would be aligned with Policy Objectives for a U.S. CBDC System, if the United States were to pursue a CBDC. And, it aims to support R&D that could also fuel technological progress in domains adjacent to digital assets, such as the traditional financial services industry, payments and other industries.

Digital assets have generated interest across a range of use cases that could help grow the economy, provide societal benefits, and advance equity and inclusion. There are a number of potential use cases that support these goals. Such areas represent diverse fields in addition to financial technologies and payments that include but are not limited to: internet architectures, healthcare and public health, supply chain management, manufacturing, distributed energy and clean energy resources, payments and humanitarian aid; amongst a wide range of other uses. Responses are welcome relevant to all areas of digital assets and related technologies, and use cases.

Comments will be accepted until Friday, March 3, 2023 at 5PM ET. Please feel free to forward this email to anyone who might be interested in submitting a comment. Please note that you are welcome to submit a response to of the topics for which information is requested.

For additional information, to share your ideas, or express interest please email the co-chairs from White House OSTP (Nik Marda and Alan Mislove) and from NSF (Anna Brady-Estevez and James Joshi) and at the official Digital Assets Fast Track Action Committee email: DARD-FTAC-RFI@nitrd.gov.

Sincerely,

Anna Brady-Estevez

National Science Foundation

Anna Brady-Estevez

SBIR/STTR Program Director

National Science Foundation

OFFICE OF SCIENCE AND TECHNOLOGY POLICY
GLOSSI.FI RESEARCH GROUP
REQUEST FOR INFORMATION

Response Topic: Community-Driven Data Feedback Loops as Infrastructure for Next-Generation Web Architecture

****
Respondent: Glossi.fi Research Group -- NSF STTR Awardee #2052118
Designated POC: Don Josey, Glossi.fi PI, [redacted]-[redacted]
Academic Research Lead: Dr. Richard Brooks, Clemson University - [redacted]
****

Executive Summary

There is a contradictory dynamic that has played out in the design space of applied cryptography for millenia. Society's relationship with cryptography and codebreaking has been complicated going back for thousands of years, with many techniques in use dating all the way back to even earlier than 1000 BC. Governments have long relied on these techniques to secure communications, but they've brandished the tools like a double edged sword, having also to fiercely protect their underlying primitives to stay steps ahead of the enemies who would want to gain access to confidential information, as we saw with the designation of technologies like RSA as munitions and the resulting US restriction of export of commercial cryptography in the nineties.

We note that this complicated dynamic has only carried on into the modern era, with blockchains -- the latest generation of applied cryptography -- being used by public and private sector actors to build trust use cases as diverse as new financial primitives, security tools enabling the novel zero-trust military communications domain, and recording real estate transactions. This set of contradictions has been carried forward, with the underlying technology frequently being seen as a tool that can be used by good or bad actors.

We don't think this tension will ever resolve, and we would praise the current administration for taking the pragmatic approach of seeking input on how the current bleeding edge technology around blockchains should be supported on the one hand and be proactively regulated on the other. Modern blockchains are essentially the application of a turing-complete playing surface to cryptographic systems which were previously much more one-dimensional. Governments who simply had to control encryption technologies previously had it easy; we are at a moment that we like to describe as a Cambrian explosion of applied cryptography, with innovation in ‘smart contracts’ taking place at an exponential rate relative to what we saw before the 2010s.

This complexity presents a stark challenge: how can the state take a hand in protecting individuals from systems which can gain traction in massive, viral liquidity events, and similarly spiral out of control and implode, harming users in myriad ways? And to what extent should these systems be supported? Should research resources in the US be going towards shutting down blockchain ecosystems, or towards encouraging innovation?

We think the answer involves taking both paths simultaneously, and we are far along in the development of a set of tools that can help align priorities not only for research and development, but also for regulation and retail assurance of interactions in new blockchain-based financial primitives. The US position is traditionally to allow the free market with its potential for innovation and “creative destruction.” The public sector role in markets has traditionally been to maintain a fair, transparent, and orderly market, and this is a dynamic which is enhanced by this new breed of community-driven feedback systems. It’s difficult to imagine how such an open collaborative ecosystem could square with the authoritarian top-down controlled and vertically integrated internet walled gardens which are emerging in some foreign markets.

We are responding to items 3-6 in the RFI. Our intention is to take a position of neutrality on items 1&2. Those first two topics are more related to positives and negatives of the digital assets space as a whole; we are building tools that are intended to answer questions 1&2. We think it makes more sense for the community members using our service to answer those questions, and for us to provide a rails for them to do so -- our software stack does use some novel blockchain-based features like composable interfaces and collaborative data marketplaces, so in that sense we are not entirely unbiased -- but we think that sort of neutrality is important in building out this sort of platform.

R&D Approaches

In this RFI response, we don’t want to bias our answer towards any particular policy direction the US should take with regards to the key policy questions facing regulators around blockchain ecosystems (Should the US have a CBDC? Should the US favor fintech entities over the traditional financial sector? Should tokens be regulated like securities, or based on their smart contract functionality?).

We grant that even though collectively we have a fair amount of expertise in researching the characteristics of blockchains and related financial systems, the answer to these questions of interoperability between blockchain-based software systems and the complex universe of applications of digital money is beyond our pay grade and beyond the scope of this paper. We have opinions here, but we humbly accept that the institutions who are in charge of making these decisions can be correct in landing on any regulatory path across these spectra.

We are happy in particular that the committee's focuses -- on inclusion, on climate risk mitigation, on fraud resistance, on future internet architectures, and on getting at the positives and negatives of the digital asset ecosystem -- are strong motivators behind everything we do at Glossi.fi.

As a thought experiment, we often consider what the internet would have looked like if many of the technologies available to us now had been developed around the same time that consumers were first logging on en masse in the 90s. Humor us for a moment in considering: if financial technologies like blockchains, cognitive tech such as openAI and big data processing frameworks, and security tools such as TLS had been available to consumers as open source software -- what would the web ecosystems have looked like? Would they have evolved into a different shape than the oligopoly that shapes the web today? Would it have been better or worse for consumers?

Each of the web titans has protected their competitive space, frequently to the detriment of open competition in favor of their own profit margins as private entities. But users have been forced into a position of tunnel vision via the network effects of these platforms and the total control management has over their APIs and frontends.

At Glossi.fi we imagine a more open information space for the development of web applications, and we have built a system which is focused on using a blockchain as the cryptographic foundational layer for allowing the creation of collaborative feedback loops and application experiences from users. We have built this community-driven interface with a focus on building user-contributed UX and fraud-prevention feedback loops, in what is essentially a federated cryptographically signed ticketing system for the entire internet. This is a new model for thinking about how the web might work, and we wish it would have been available to users going all the way back to the dawn of the web.

How a collaborative cryptographically verified anti-fraud system could work on smart contracts versus on analogues in traditional markets:

- **Surfacing arbitrage risks and mitigation techniques to users:** Identifying risks of dark pool markets/payment for order flow versus identifying risks of miner extracted value (MEV) on ethereum.
- **Real-time context on financial primitive fundamentals:** Surfacing financial audits on financial statements versus surfacing data on smart contract usage, and liquidity, to users at the point of the transactions.
- **Real-time alerting on security incidents:** Surfacing information on traditional web app security and data breach events as well as information on smart contract

exploits and code audits will help users avoid pitfalls in their transaction processes.
- **Financial primitive underlying data integrity**: Identifying securities with broken underlying data feeds / smart contracts with weak/flawed/underfunded oracle services.
- **Risk management:** Showing potential lenders and borrowers information on the health of underlying assets of bonds and mortgage backed securities/collateralization of assets in defi ecosystems.

Our intent is to encourage government contribution for and support to this kind of data layer, which we see as extensible not only to blockchain apps, but all the way through the traditional financial system and web. The applicability of this kind of system across these different types of ecosystems is why we can happily say, contradictorily, that the collaborative community driven feedback layer we've built can be used under any future digital asset regime -- from within a future US CBDC regime, all the way over to the other end of the spectrum in a blockchain digital currency-enabled world.

Composable Web Experiences: Democratization and Extension of Web Architecture

Our framework is not only about constructing feedback loops for the purposes of anti-fraud. An interesting property of blockchains is that they are built around web clients that connect to an open interface. Put simply, for most of the applications users are interacting with on a day-to-day basis, anyone can deploy a frontend that talks to the same APIs and replicates the interactions that are developed initially by the people who build the applications in the first place.

This type of interaction might not make sense to everyone. Product owners have a vested interest in getting users into their own app portals. But basically all applications impose a sort of tunnel vision on users which may not be in their best interest. Take as an example the website for one of the leading automated market maker applications (AMMs). You can go to one of these sites today to make a trade, and they basically only present you with a few data points -- the price of the token to be traded on their application, and the names and contract address of the token pairs in question. But there is a lot of information that users would do well to be aware of during that interaction, such as the likelihood that they will be arbitraged by MEV agents, or the price of the same trades on competing services, or tools to avoid MEV, or historical performance of the token pairs in question.

We imagine that much of the web could be redesigned around these sorts of interfaces, where users select or are recommended templates of reports and visualizations that support their needs. And if that were the case, we would make the argument that that would be a boon for consumers and their desires to opt in to or out of any particular content that they want associated with their browsing experience.

We see with antitrust cases currently, such as the probe into the Adobe-Figma merger, or the outrage over the lack of a probe that should have happened into the Facebook-Instagram merger, that many have come to a recognition that perhaps the current state of play -- with tech giants dominating markets for ads and access to information -- may be better for stakeholders of those giant corporations than for the interests of individual consumers; we are attempting to do our part in creating a path to an alternative.

Data Marketplaces

The development of cryptography plus digital signatures and decentralized identifiers have paved the way for a new way of thinking about creating verified, structured data references. Digital signatures on blockchains tied to a hash of a data payload allow users to create a cryptographic proof -- not necessarily that the user created the piece of data or that it is original, but at least that the piece of data was attested to by the signer.

Our software stack relies on a graph of these attestation tickets. Individual pieces of data are collected and delivered to users in such a manner as to build the underlying metadata models that can build our user experience feedback loops. Many of these pieces of the graph are objective or permanent characteristics, but many are subjective pieces or dynamic pieces that can be updated.

These data attributions are the democratic expression of a community's knowledge and expertise. And in markets where hacks can happen instantly and put following users at risk, timeliness is also critically important. This is why we hope these information systems are supported -- the financial health and well-being of users is constantly at stake.

Conclusion: Paths to Public Sector Contributions

This RFI is focused on policy with regards to federal participation in the digital assets research and development ecosystem. We see several paths where the public sector support for this sort of these commons data integrity processes could be a game changer:

- **Funding for development of community-governed risk metadata ecosystem infrastructure:** Ours and other projects are developing processes for focusing the wisdom of crowds using systems of incentives.
- **Funding of incentive pools:** We are exploring layered mechanisms for funding the pools which will pay out our incentives to contributors to the system. Public funding would definitely give these data curation communities more firepower to build out an ecosystem of contributors of fraud-resistance data and start protecting users as quickly as possible.

- **Funding for research into incentive alignment mechanisms on data marketplaces and community-driven fraud-resistance metadata systems:** We have designed a naive mechanism for rewarding users of our community-driven data submission systems. Getting the incentives right to efficiently encourage participation in this ecosystem is something that will require testing and iteration.
- **Participation in feedback submission through risk metadata systems:** Public servants could participate in submission of data points into this sort of system just as easily as anyone else. The imprimatur of the public sector could carry extra weight in our identity-based system. We recognize there could be some hurdles to this actually happening, but given the public sector's role in regulating so many other markets, we hope this sort of active participation in curation of consumer protection data -- with the appropriate guardrails and checks and balances -- would be not entirely outside the range of possibility.
- **Agency hosting of user contribution databases:** We are creating an open data structure with federated hosting. This means users can choose to access different databases with different queries surfacing different subsets of data depending on the preferences of the curator. It would absolutely make sense for the public sector to have a hand in curating an instance of this data, and deciding which individually submitted data points should be shown to users. There are some difficulties in this process seeing as much of this data is 'subjective.' But we think such a guide would be valuable.
- **Contributions to composable app ecosystems:** Another goal of the project we are building out is related to building out composable app ecosystems, where web clients are developed which talk to standardized protocols. Our further efforts will help drive the vision of a more user-friendly internet where information is presented to users based on their own preferences rather than those of some systems administrator.

We also think it would be fair to characterize this sort of ecosystem as an initiative that is a private sector attempt to build infrastructure which is in the domain of what the public sector could be responsible for. We think the public sector can more effectively weigh in on the innovation and disruption in the space by utilizing tools that fall short of resorting to legislation, administrative actions, and especially the noxious and innovation-killing trend of rulemaking by enforcement. The active impact of public sector efforts to encourage or discourage the use of dangerous financial primitives, especially on this sort of application which will tie in directly to the user wallets, could not be understated -- it could be enormously helpful in enabling participants to make sound decisions for interaction with web3 markets.

We should note also, however, some of the weaknesses in bureaucratic processes which make private participation in this sort of system so critical: public sector actors are rightfully criticized for having too heavy a hand at picking winners and losers in industry, and communities can oftentimes identify good and bad patterns in app ecosystems more readily than public services who have regime biases and layers of administrative review and red tape.

Appendix I: Our R&D Effort

The committee has requested feedback towards advancing a 'holistic vision of a digital assets ecosystem that embodies democratic values and other key priorities.' The entire flow of our service is built around the principle that any users can submit feedback on any digital asset ecosystem interactions into networks of federated data ecosystems with their own ranking and assurance services for aligning incentives on what comprises a quality data submission.

At Glossi.fi, with NSF support we are building a service that brings in user feedback on individual smart contract abstractions. Our project is a rethinking of how access to and evaluation of financial services can work. We create feedback loops, using a next generation blockchain-enabled data marketplace, that enables safety and fraud resistance of digital asset ecosystems.

Our 'hyperstructure' is a neutral surface for this data uptake process. With regards to the first two questions which are response topics -- the reader of this RFI response should understand that we are trying less to answer that question with this document here than we are with our entire system and data structure. Glossi.Fi is concerned with maintaining our credible neutrality on those questions, and on not tipping the scales towards answers which should be provided by our data ecosystem contributors.

A critic of our system might call it not entirely democratic, as we intend to use financial protocols to help align incentives on data submitters, voters, and consumers. Realistically, there is no clean and total de-linking of market and democratic processes in any of the structures in our modern liberal democratic system of systems, at any level. We live in a world that is about striking a balance between the incentives of capital and those of all other stakeholders in a system.

We will be leaning on the goal of neutrality, and gearing towards building those processes with the intention to be neutral not only to competing ideas and interests but to use mechanisms inspired by quadratic funding to help tilt the balance of power towards submitters with less funds versus the interests of the whales. And we think this sort of structure naturally tilts the power and agency from product owners of decentralized finance applications and towards their users, no matter how much of a balance any individual user has in their wallet app. That redistribution of information and of agency is ultimately what makes us the most excited about the whole web3 ecosystem.

Appendix II: References

Amadeo, Kimberly. “The Causes of the Subprime Mortgage Crisis.” *The Balance*, The Balance, https://www.thebalancemoney.com/what-caused-the-subprime-mortgage-crisis-3305696.

Auer, Raphael, et al. *Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi* . BIS, https://www.bis.org/publ/bisbull58.pdf.

Berret, Charles. *The Cultural Contradictions of Cryptography: A History of Secret Codes in Modern America*. https://academiccommons.columbia.edu/doi/10.7916/d8-pf8n-s992/download.

CAE-R / CAE-CDE Consortium, et al. “Implementing Zero Trust at the Tactical Warfighting Edge.” *DOD University Consortium for Cybersecurity Second Round of Requests for Information*, 24 Sept. 2024.

Diffie, Whitfield, and Susan Landau. “The Export of Cryptography - Privacyink.org.” *Privacy Ink*, 19 Apr. 2005, https://privacyink.org/pdf/export_control.pdf.

“Dubai Land Department - Dubai Land Department Achieves a Technical Milestone with the Adoption of Blockchain Technology in Cooperation with Smart Dubai and Other Partners.” *Dubai Land Department - Dubai Land Department Achieves a Technical Milestone with the Adoption of Blockchain Technology in Cooperation with Smart Dubai and Other Partners*, Government of Dubai, 7 Oct. 2017, https://dubailand.gov.ae/en/news-media/dubai-land-department-achieves-a-technical-milestone-with-the-adoption-of-blockchain-technology-in-cooperation-with-smart-dubai-and-other-partners/#/.

Dzyatkovskii, Anton. “The Strengths and Weaknesses of Defi Price Oracles.” *HackerNoon*, 6 June 2021, https://hackernoon.com/the-strengths-and-weaknesses-of-defi-price-oracles-x7l35ui.

Faife, Corin. “Wormhole Cryptocurrency Platform Hacked for $325 Million after Error on Github.” *The Verge*, The Verge, 3 Feb. 2022, https://www.theverge.com/2022/2/3/22916111/wormhole-hack-github-error-325-million-theft-ethereum-solana.

Geron, Tomio. “Payment for Order Flow Made Robinhood Huge. Now Everyone's Arguing About It.” *Protocol*, Protocol, 9 Feb. 2022, https://www.protocol.com/fintech/payment-for-order-flow-explained.

Joseph, Susan. “Award Abstract #2042690 SBIR Phase I: Coronavirus API (Covid-19).” *NSF AWARD SEARCH: Award # 2042690 - SBIR Phase I: Coronavirus API (COVID-19)*, NSF, 21 Apr. 2021, https://www.nsf.gov/awardsearch/showAward?AWD_ID=2042690&HistoricalAwards=false.

Josey, Donald. “Award Abstract # 2052118 STTR Phase I: Blockchain Ontology and Services for Monitoring and Performing Analytics on Smart Contracts.” *NSF AWARD SEARCH: Award # 2052118 - STTR Phase I: Blockchain Ontology and Services for Monitoring and Performing Analytics on Smart Contracts*, NSF, 11 Jan. 2022, https://www.nsf.gov/awardsearch/showAward?AWD_ID=2052118&HistoricalAwards=false.

MacPherson, Sam. “Protocol Frontends as Competitive Marketplaces.” *Medium*, Medium, 19 Jan. 2022, https://hexonaut.medium.com/protocol-frontends-as-competitive-marketplaces-457b0c4ec1c7.

Michaelsen, Marcus, and Marlies Glasius. *Authoritarian Practices in the Digital Age | Introduction*. https://ijoc.org/index.php/ijoc/article/viewFile/8536/2458.

Morris, David Z. “Why Defi Might Be Safer than Traditional Finance.” *CoinDesk Latest Headlines RSS*, CoinDesk, 23 July 2022, https://www.coindesk.com/layer2/2022/07/22/why-defi-might-be-safer-than-traditional-finance/.

Nylen, Leah, et al. “Facebook Faces Antitrust Allegations over Deals for Instagram and WhatsApp.” *The Guardian*, Guardian News and Media, 8 Dec. 2020, https://www.theguardian.com/technology/2020/dec/08/facebook-antitrust-lawsuits-instagram-whatsapp.

Nylen, Leah, et al. “US DOJ Preps Antitrust Suit to Block Adobe's $20 Billion Figma Deal.” *Bloomberg.com*, Bloomberg, 23 Feb. 2023, https://www.bloomberg.com/news/articles/2023-02-23/doj-preparing-suit-to-block-adobe-s-20-billion-deal-for-figma.

Picardo, Elvis. “An Introduction to Dark Pools.” *Investopedia*, Investopedia, 2 Feb. 2023, https://www.investopedia.com/articles/markets/050614/introduction-dark-pools.asp.

Richard Alm and W. Michael Cox, et al. “Creative Destruction.” *Econlib*, 27 June 2018, https://www.econlib.org/library/Enc/CreativeDestruction.html.

Rogoswami. “SEC Charges Do Kwon, Terraform with Fraud in Connection with Terra Collapse.” *CNBC*, CNBC, 16 Feb. 2023, https://www.cnbc.com/2023/02/16/sec-charges-do-kwon-with-fraud-in-connection-with-terra-collapse.html.

Roose, Kevin. “What Is Defi?” *The New York Times*, The New York Times, 18 Mar. 2022, https://www.nytimes.com/interactive/2022/03/18/technology/what-is-defi-cryptocurrency.html.

Sidhpurwala, Huzaifa. “A Brief History of Cryptography.” *Red Hat - We Make Open Source Technologies for the Enterprise*, 12 Jan. 2023, https://www.redhat.com/en/blog/brief-history-cryptography.

Staff, the Premerger Notification Office, and Stephanie T. Nguyen. “FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers.” *Federal Trade Commission*, 15 Sept. 2022, https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers.

Surane, Jennifer, and Katherine Doherty. “Ion's Derivatives System Hack Sparks Caution in Equities Market.” *Bloomberg.com*, Bloomberg, 3 Feb. 2023, https://www.bloomberg.com/news/articles/2023-02-03/ion-s-derivatives-system-hack-sparks-caution-in-equities-market?leadSource=uverify+wall.

Vitalik, Buterin. “Quadratic Payments: A Primer.” *Vitalik Buterin's Website*, Vitalik.CA, https://vitalik.ca/general/2019/12/07/quadratic.html.

DEPARTMENT OF DEFENSE
UNIVERSITY CONSORTIUM FOR CYBERSECURITY
SECOND ROUND OF REQUESTS FOR INFORMATION

Response Topic: Implementing Zero Trust at the Tactical Warfighting Edge

---

Lead Institution: The University of Memphis, Memphis, TN.
Designated NCAE-C Program Path Name: CAE-R / CAE-CDE Consortium .
Designated POC: Dipankar Dasgupta, [redacted], [redacted].
Response Subtitle: *Holistic Implementation of Zero Trust at the Tactical Warfighting Edge for Devices, Users, and Communication Infrastructure.*

Consortium Members

1. **The University of Memphis:** Dipankar Dasgupta (PoC); Hasan Ali [redacted]; Arunava Roy [redacted].
2. **Massachusetts Institute of Technology (MIT):** John R. Williams [redacted]
3. **Syracuse University:** Vir Virander Phoha [redacted]
4. **Purdue University:** Bharat Bhargava [redacted]
   Chris Clifton [redacted]
5. **Clemson University:** Richard Brooks [redacted] Kuang-Ching Wang [redacted] Fatemeh Afghah [redacted]
6. **Texas A&M University:** Nitesh Saxena [redacted]
   Guofei Gu [redacted] Srinivas Shakkottai [redacted]
7. **University of Delaware:** Lena Mashayekhy [redacted]
8. **Missouri University of Science Technology (MST):** Sanjay Madria [redacted]
9. **Penn State University:** Syed Rafiul Hussain [redacted]
10. **University of Illinois at Urbana-Campaign:** Narendra Ahuja [redacted]
11. **University of Illinois at Chicago:** Venkat Venkatakrishnan [redacted]
12. **University of North Carolina at Charlotte:** Chao Wang [redacted]
13. **University of Wyoming:** Diksha Shukla [redacted]
14. **Clark Atlanta University:** Kishor Datta Gupta [redacted]
15. **Roosevelt University:** Meng Yu [redacted]

Executive Summary

In modern warzones and battlefields, higher cyber dominance and counterintelligence capabilities are essential for a successful outcome. Nation-states and cyber adversaries use various deceptive techniques which are very difficult to detect before they cause severe negative impact. At the warfighting tactical edge, secure communications for information sharing and among the headquarter (HQ), sub-HQ and entities are very important in making robust and effective decisions to have appropriate and timely actions. By integrating the 5th generation (5G) cellular technology, IoBTs at the warfighting edge, this initiative will enhance and evolve with improved monitoring and management of the fighting operational zones.

A crucial element of modern warfare is a digital soldier (of any form or shape, such as an Internet of Battlefield Things (IoBTs) which should be capable of handling situations quickly in a hostile and zero-trust environment at the tactical edge.

We formed a consortium of 15 Universities (from 12 states) to explore a holistic and actionable approach to provide Zero Trust (ZT) functionalities for warfighters operating at the tactical edge. The Consortium members have expertise in Cybersecurity, Edge Computing, AI/ML, Federated/Distributed Computing/Learning, Networking (Ad-Hoc, Wireless, SDN, NDN, cellular/satellite Communication (4G/5G/6G)), Software design & development, low-powered IoTs, and SmartGrid.

The ***overarching goal*** of this initiative is *to develop foundational principles and full-stack security modules for Internet of Battlefield Things (IoBT) systems against cyber-attacks by developing a suite of zero-trust functionalities across tactical edge networks for situational awareness.* The context of the project encompasses the implementation of zero-trust at the squad, platoon, company, brigade, and corps level of warfighters in a denied, disrupted, intermittent and limited (DDIL) environment. We propose a holistic approach that addresses authenticating IoBTs, edge platforms device, and the data and provide security to data as it moves from edge to edge—and back through the chain of command. Our approach replaces a human-intensive authentication and logic chain with automated processing of security of the individual, device, and communication in tactical environments, thereby reducing the warfighter's cognitive burden and providing utmost security at the tactical edge of warfighting.

The proposed federated computing environment will form a cyber fence while ensuring various aspects of Zero Trust at the Tactical Warfighting Edge. Each edge platform (edge cloud) will not only serve as a command and control of context-aware decision-support systems but also support associated IoWTs, information fusion, communications channels, guidance to various sensory warfare, and establish real-time chain-of-custody of all managed assets.

The proposed research will address the following questions as mentioned in RFI: the boundary between Enterprise Networks (High Availability) and Tactical Edge Networks (Intermittent/No Availability) by extending Zero Trust to edge systems. In particular, leveraging the principles of micro-segments with their own micro-perimeters with a software-defined network (SDN), implementing, implanting, or designating a Zero Trust capability.

Thrust I and Thrust II provide solutions for handling the Identity, Credential, and Access Management (ICAM) process at the Edge using Zero Trust concepts.

Various testbeds as described in Section 3 will be considered for Federated/Enterprise ZT implementation to components/systems in a DDIL environment using the proposed holistic approach.

We will develop a Proof-of-the-Concept framework to demonstrate the functionalities of the framework as deliverable.

Keywords– Tactical Edge, Edge platform, IoT, IoBT, Security, Blockchain, ZT Authentication, AI/ML.

Project Description

In this initiative of university consortium comprising experts from various domains of cybersecurity research, we set out to address – how to ensure seamless, Zero-Trust functionality for devices and users (i.e. device to device, user to device, and user to user) communication, data access, and source authentication, and the security of communication and network infrastructure operating at the tactical edge (of the warfighter) in a denied, disrupted, intermittent and limited (DDIL) environment.
As we look more closely at ZTA, we see the possibility of confusion—because many different topics and concepts are implicated—but also a clear indication of opportunities to build better, more flexible, and more secure software systems. What are some of the principles that can help guide us through both the confusion and the opportunities?
One guiding principle for Zero Trust is that while the conceptual model decreases reliance on network location, the role of network controls and perimeters remains important to the overall security architecture. In other words, the best security may come by using effectively the combination identity-centric and network-centric tools to establish zero trust.
Another guiding principle is that Zero Trust conceptual model and associated mechanisms will continue to improve defense in depth, and continue to make security controls which work better through the increased visibility and software-defined nature of the cloud and its segmentation.

1 Innovative Approaches

The innovative approach consists of both developing a suite of research methods and a team with expertise that can solve various security challenges. The technical approach comprises five interconnected thrusts working synergistically towards a holistic zero-trust security solution for mission-critical IoBT systems. The sections below detail the background and research ideas. A common theme of the five research thrusts centers around zero-trust security, and functional and timing correctness in IoBT systems. In Thrust I, we focus on deriving markers of trust and situational awareness in communication infrastructure at the tactical edge. Thrusts II, III and IV deal with developing a suite for secure data access, source authentication, and secure and holistic communication and network infrastructure for IoBT systems.

We define this cyber fence with a generalized formulation that involves headquarter (HQ) and sub-HQs on multiple warzones, each of which runs a separate edge platform. E_1 is the leader node of HQ, connected with multiple reserved IoBTs $E_{ij} : j = 1, 2, \cdots$, which can be used to reinforce different warzones as needed. $E_i : i = 2, 3, \cdots n$ are the leader nodes from the warzones between 1 and $(n - 1)$ respectively and connected with multiple IoBTs $E_{ij} : j = 1, 2, \cdots m$, where each of the IoBTs within a warzone is connected with others through Device-to-Device (D2D) communication (Figure 1). Each E_i collects information from $E_{ij} : j = 1, 2, \cdots m$ (in several passes) before making final decisions for E_{ij}. This process can be federated learning/computing since each of the IoBTs has low computing abilities and may have non-iid data. Moreover, all the edge computing platforms (E_i) are connected with others including the HQ and may help each other by sending necessary reinforcements to the weak warzones (Figure 1).

1.1. Device-Edge-Cloud Architecture for Mission-Critical IoBT

To create a more secure and resilient cyber infrastructure, President Joe Biden signed the Executive Order on Improving the Nation's Cybersecurity, which calls on agencies to adopt a zero-trust security model. A Zero-Trust Architecture (ZTA) shifts away from the old standard of perimeter security to a higher standard of security using micro-segmentation. Micro-segmentation allows files and folders within the storage infrastructure to be sectioned off which results in attacks being cut short by giving users the least privilege access (i.e., the users are given the least amount of access) while still being able to function in their role at mission-critical applications. Zero-trust requires a user/device/process to be continuously validated, authenticated, and authorized.

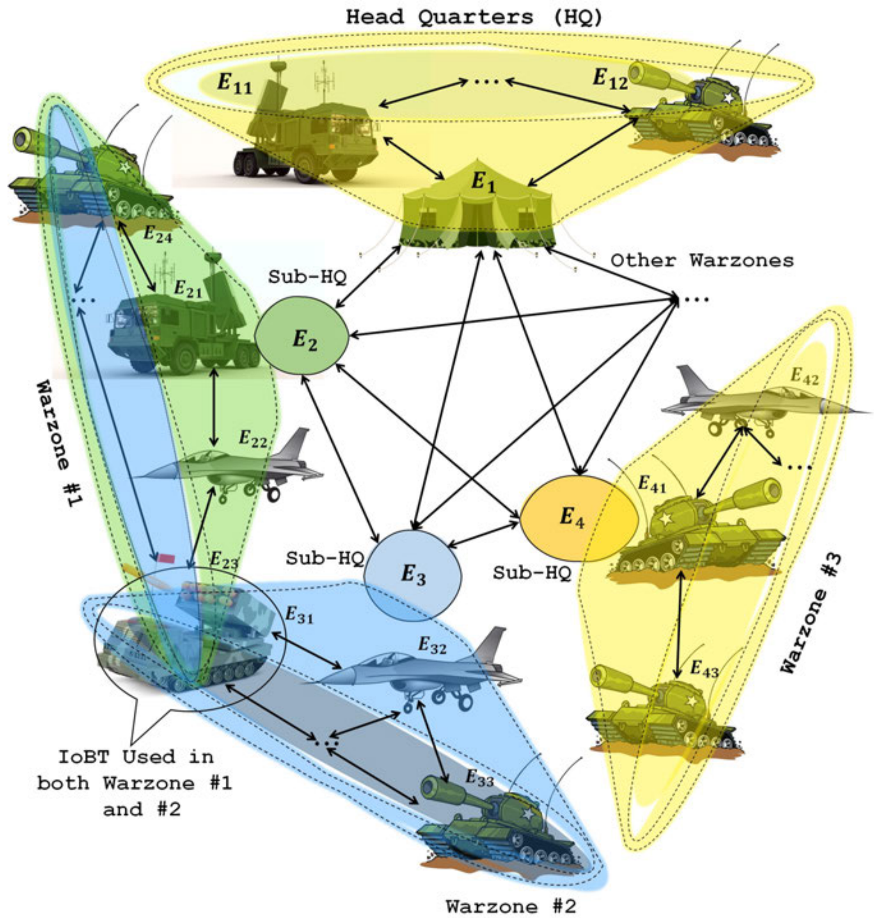


Figure 1: A warfighting scenario with cyber zones for command, control, and mitigation components. All E_is communicate through secure communication channels with high situational awareness capability, where the IoBTs inside each E_i can exchange data and share critical information through D2D communications. Some of the IoBTs can be shared among multiple edges. The enemy can selectively destroy specific channels and packets, resulting in the deletion of communication links in the network.

Commercial IoT systems are adopting ZTA framework to ensure the security of resources. The ZTA is defined by various industry guidelines [1] and is a multilayer cybersecurity approach to mitigate threats that could materialize due to sophisticated attacks and anomalies. The current ZTA use complex and critical algorithms. These approaches are not suitable for IoBT operating at the tactile edge because of the required computing power for heavy calculations, and bandwidth for data transition. Additionally, current IoTs use network communication and remote data access and transfer, which can lead to malware hazards and alter the transmission of data.

Hence, there is a need for extensive research to provide full-stack security protection for device-edge-cloud architecture for mission-critical IoBT systems. This becomes a challenging issue for IoBT systems operating at the tactile edge due to operational impacts from DDIL environments, including limited bandwidth. IoBT is a technology for mass data collection and processing, composed of a system of interconnected and heterogeneous devices, protocols, application software, and users. IoBT is distinguished from commercial IoTs by its required performance guarantees, certifiable security, fault tolerance, and resilience. In particular, IoBT is a network of sensors, wearables, and IoT devices that uses cloud and edge computing to create a coherent combat force, and connect warfighters with intelligent technology in armor, radios, weapons, and other warfighting assets. Figure 1 shows a warfighting scenario with cyber zones with command and control components (HQ and sub-HQ IoBTs).

2 Scientific Research Plan for Mission-Critical IoBT Systems

This initiative will create synergistic research outcomes and will integrate research efforts from partners with different research expertise from multiple institutions towards the design and deployment of full-stack security with ZTA for mission-critical IoBT at warfighting edges.

2.1. *Thrust I: Resilience and Zero-Trust Functionality for Identity, Authorization, and Authentication Ecosystem*

Overall Idea: This thrust focuses on designing markers of trust and situational awareness for (1) device-to-device, (2) user and device, and (3) user and user, communication at the tactical warfighting edge. Zero-trust in identity management requires continuous monitoring and authenticating of users, systems, or applications to ensure the right people, devices, and applications are always accessing the right data. A key feature is tracking, and logging sessions initiated by internal and external users and connected systems.

To effectively connect sensing devices, intermediary gateways, backend application servers, and client devices for data exchange and information delivery, a new infrastructure is required. IoBT systems must adopt a lightweight authentication protocol to reduce their time and energy consumption when a device wants to authenticate and transmit data to its targeted peer. This project proposes to develop new lightweight continuous verification protocols with the design goal of optimizing computational complexity to reduce the time and energy consumption for consecutive authentications. The performance of the system will be rigorously analyzed for device-to-device authentication in IoBT environments.

Having the ability to transfer data and perform intelligent computing over a network without requiring human-to-human or human-to-computer interaction, IoBT significantly improves the autonomy of computing systems and is among the disruptive technologies. The mission-critical IoBT system aims at creating a unified sensing, computing, and control system to ensure both functional and timing correctness of applications at the tactile edge, and optimize the system performance.

Adaptive Multi-Factor Authentication (A-MFA) – All critical infrastructures are becoming tightly coupled with cyber-enabled systems and services; also, these are being remotely managed and controlled via mobile devices. In order to securely access such infrastructure, context-aware, adaptive authentication, and authorization mechanisms become essential. Based on our prior work with adaptive multi-factor authentication technology, we develop a just-in-time, dynamic selection of authentication factors at the time an authentication event occurs. The dynamic selection process uses ML and optimization techniques to determine the best set of authentication factors for a particular environment in real-time. The objective is to make it more difficult for attackers to gain illegitimate access to critical systems or resources by making the authentication unpredictable which credentials will be required, using an intelligent decision support mechanism for adaptive decisions under varying operating environments. This approach can provide administrators with some degree of trust over the authentication process that works best for any critical infrastructure without compromising security.

Another aspect of MFA is that the users need to be explicitly involved in the authentication process and put in more cognitive effort (like copying one-time PIN codes) while validating their identity. Such human involvement makes the authentication process more cumbersome and may not be possible in mission-critical settings where on-the-fly access is necessary. To address this challenge, the consortium will be focusing on designing MFA mechanisms enhanced by ML that can automatically, and likely constantly, authenticate the users' trusted devices to the network without any human involvement. Based on a series of our prior work [2, 3, 4, 5, 6, 7, 8, 9, 10], the team will design, implement and test adaptive MFA mechanisms best-suited for mission-critical settings.

Context & Risk-based Authentication-Access Control – Accordingly, A-MFA uses contextual information about the user's operating environment to determine the optimal set of authentication factors (active or passive). Characteristics of the user's operating context may include things like the type of networks, devices, applications, the sensitivity of infrastructure resource/service access, the user's role, location, authentication history, physical characteristics (light, noise, etc.) in each environment. This context-aware fine-grained authorization and access control are based on real-time assessment of attributes of users, protected resources, and environmental factors [6]. The robustness of the A-MFA system can be assured by designing the framework in such a way that if any modality data get compromised, the system can still perform flawlessly using other non-compromised modalities. Scalability can also be achieved by adding new and/or improved modalities with the existing set of modalities. A-MFA provides secure authentication by choosing modalities based on device and context (surrounding conditions) thus maintain the perfect balance between powerful security and low-maintenance usability.

2.2. *Thrust II: Secure Data Access and Information Sharing*

Overall Idea: On a battlefield, one group of agents may need to collaborate with another group under the DDIL environment. In defense applications, multiple groups can work on different missions using Disruption-Tolerant Networks (DTNs) and their missions can be updated dynamically. Secure data sharing in this particular setting is really challenging and existing schemes do not offer any immediate solution. Passing secure messages using DTNs (Figure 2) is challenging because existing public-private key cryptographic approaches may not be always accessible across different groups due to the unavailability of Public Key Infrastructure (PKI). Thus, it is difficult to use public-private cryptography as one group may not have access to the public key of other groups as there will be no central infrastructure. In addition, connectivity may be intermittent so finding a reliable route is also difficult. Thus, instead of sending the complete message in a single packet, fragmenting the messages and sending them via multiple nodes can help achieve better security and reliability when multiple groups are involved. Therefore, encrypting messages before fragmentation and then sending both the data fragments and the key fragments (needed for decryption) provide much higher security. However, in this fragmentation process, a few redundant fragments are created to increase the probability of a message being delivered to the destination node in such an environment. Since DTN has high data loss, this redundancy helps the destination node to retrieve the original message with fewer key and data fragments than those created at the source. In order to verify that each key- and data-share is not corrupted before decryption at the destination, an integrity check is also set up which helps in conserving the device's battery. In order to find the corrupted nodes in the path of message traversal from source to destination, the blockchain approach will be used.

Objective 1: Security of Disseminated Mission-oriented Fragmented Content and Associated keys in DDIL Environment – The objective is to develop a scheme to provide improved security by generating multiple key-shares and data fragments of each message and disseminating them via some intermediate nodes. In this fragmentation process, we also create a few redundant blocks to guarantee a higher data arrival rate at the destination when the message drop rate is higher like in the DTN environment.

Once fragments have been identified, now to deliver those fragments securely using DTNs is challenging. Due to the limitations of the DDIL environment, the existing public-private key cryptography may not be possible due to the inaccessibility of keys caused by the unavailability or access restriction of Public Key Infrastructure (PKI) across different groups. In such a situation, instead of encrypting with some specific node's public key (which may not be available), the source node encrypts the fragments for security with some intermediate (commander) node's public keys or with the attribute-based keys based on fragments. Note that fragments help in two ways: instead of sending the complete message (video/image) in a single packet, fragmenting the objects of interest and sending them via multiple nodes can help handling the DDIL environment as well as to achieve better security and reliability when multiple groups are involved. Therefore, encrypting messages before fragmentation and then sending both the data fragments and the key fragments (needed for decryption) with redundant copies through different paths provide much higher security. Keys are also fragmented as sending a key in a single packet can hamper security if it is forwarded to some corrupted nodes who may try to tamper or drop it (next section provides a unique solution to this as well). Decoupling fragmented data and key reduces redundancy while providing better security because one node needs to get both; enough key-shares as well as all encrypted data fragments to realize the full message.

In this work, we will develop a scheme to provide improved security by generating multiple key-shares and data fragments of each key as well as messages and disseminating them via some intermediate nodes. In this fragmentation process, we also create a few redundant blocks to guarantee a higher data arrival rate at the destination when the message drop rate is higher like in the DIL environment. Hence, the source node generates multiple key-shares using some Recursive Secret Sharing (RSS) approaches, and data fragments using an algorithm like with Cauchy Reed Solomon (CRS) to disseminate them via some intermediate nodes. In this fragmentation process, RSS CRS create a few redundant blocks which guarantee a higher data arrival rate at the destination when the message drop rate is higher. Note that to retrieve the correct fragment and key, only some k fragments (out of n) and i key shares (out of m) are needed which addresses the issues in the DIL environment. When enough key-shares and data-fragments arrive at the destination, it can regenerate the key and encrypted data. It then uses this key to retrieve actual data. We also use proxy re-encryption [11] that eliminates the necessity of decryption in each step except for the destination. Source creates several proxy re-encryption keys by using its own private key and other chosen public keys of some intermediate nodes. After receiving a key-share encrypted with a proxy re-encryption key built from its public key, intermediate nodes also create a proxy re-encryption key using its own private key and other chosen intermediate or destination node's public key. This proxy re-encryption key is used to change the domain of the encrypted key-share from one intermediate to another intermediate or destination node. Those key-shares and data-fragments for one message do not necessarily need to arrive at a single destination node in a group. When the members of the same group get a certain number of unique fragments, they can combine them to generate the actual message. The integrity of a key-share or data fragment can be checked by applying Merkle Hash Tree and traditional signature method but authentication and provenance information cannot be guaranteed, which we discuss next.

Objective 2: Source Authentication for Fragmented Objects in DDIL – The information flow of fragments could be highly confidential and sharing this needs to be secured from unauthorized access; that is, the fragments should be arriving from authenticated sources, so they are tamper-free, and their provenance must be tracked during DTN transition. The receiver must make sure that the fragments are generated and sent from an authentic source. However, authentic and secure data fragments can be corrupted by some malicious intermediate DTN nodes while carrying the message fragments and those nodes should be identified and possibly stopped from forwarding the fragment. The encrypted fragments are signed by the source node using the symmetric key provided by the server. For a specific time interval, the source generates a time-based key from the symmetric key, and signs all the data fragments with the respective key and forwards them to the network. A destination, upon receiving the fragment(s), can verify the signatures by generating the key from the fragmented key shares for that time interval to check if this fragment(s) has come from an authorized source. If the object comes after the time interval, it cannot be verified, and hence, it is necessary to receive $k < n$ forwarded fragmented objects which are signed with a key. The near-optimal time interval can be set using the average message delivery delay or it can be mission dependent. In order to find the corrupted nodes in the path of message traversal from source to destination, the keychain-based approach can also be used as follows:

To find out the corrupt nodes in a path for a fragment data arrival, the keychain-based approach can be integrated with the fragments. A keychain is a one-way backward chain of the hash outputs of a predefined hash function where the first key k_n is created randomly. Then the next key $k_n - 1$ is created by the hash of k_n and it keeps doing it until we get k_0. The first and last values for different keychains are distributed by the information server to the senders and receivers at bootstrap. A sender, when sending fragments, also sends k_n to the first intermediate node I_1. When it meets another intermediate node I_2, I_1 signs the previous node's id (source id S), its id (I_1) and next node id (I_2) by the key k_n and calculate $k_n - 1$ (Figure 2). Then it sends the signatures and $k_n - 1$ to the I_2. I_2, when meeting another node I_3 will sign the three nodes id (I_1, I_2, I_3) by $k_n - 1$ and calculate $k_n - 2$. At some point, the destination will get the list of all signatures and some key k_m. It can calculate k_0 from the k_m and verify if any key has been corrupted on the way. If not, the destination checks all the signatures with the respective keys to see if any id has been

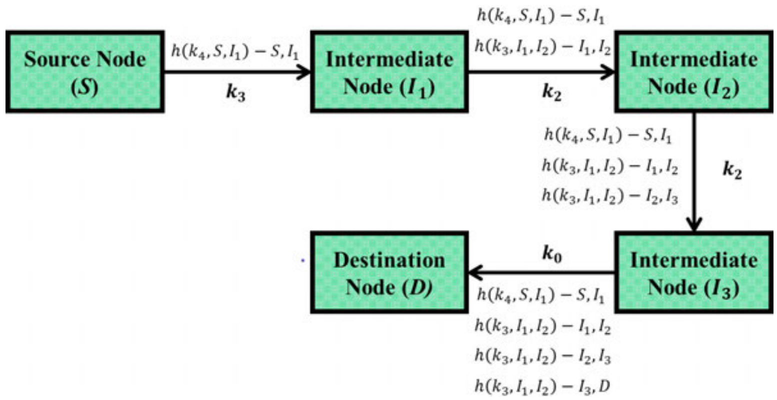


Figure 2: Hash chain created by Source/Relay nodes for a message in DTN. S selects the keychain and obtains k_4 from its storage before transferring the message. It creates a keyed hash using SHA-256 from k_4 and the IDs of source S and I_1. It also sends k_3 and IDs of S and I_1 to I_1. When I_1 meets I_2, it creates a keyed hash from k_3 and IDs of I_1 and I_2. This keyed hash along with previous keyed hash values generated for this message is sent to I_2. k_2 along with IDs of I_1 and I_2 are also sent to I_2. The same process continues until it reaches D. When D receives k_0, it obtains k_4 from its storage. From k_4 and the pair of IDs associated with each hash, the destination node recalculates and validates all the hashes associated with the message.

altered or skipped or has taken a longer route then anticipated to find out the corrupted node. Any node which might have contributed to altering any key or path information will be kept out of consideration for further distribution of data. To achieve secure tactical edge computing at warfighting zone to support zero trust and continuous verification, the designed mechanisms must have the following properties**:**

Property 1: Verifiable and unchangeable history log: It allows the operations such as re-authentication or re-verification in a DDIL environment after tactical nodes become reconnected and they have to re-initiate the trust relationship. This property is also important for AI/ML-based behavior analysis in the DDIL environment for compromise detection.

Property 2: Selective verification: This is an extension of property (1) since in tactical edge environments the nodes usually have limited computation and network resources. They could not afford the end-to-end verification as blockchain. At the same time, such selective verification must support quantifiable detection capability so that end users know the trade-off between overhead and achieved detection capability.

Property 3: User configurable confidentiality and integrity protection methods. Depending on the available resources and the importance of data/information, different methods must be designed to achieve protection with user-configurable overhead and safety.

2.3. *Thrust III: Security of Communication and Network Infrastructure for Mission-Critical IoBT Operations at the Tactical Edge*

The main innovation promised by NIST's zero trust architecture is pushing authorization further to the edge by combining the policy decision point (PDP) and policy execution point (PEP) into a single unit that is associated with each resource. This is inspired by the eXtensible Access Control Markup Language data authorization standard from OASIS, which manages authorization with policy administration points (PAP), PDP, PEP, policy information point (PIP), and policy retrieval point (PRP). XACML is an XML-based authorization policy definition language, as is Security Assertion Markup Language (SAML). Where SAML is a standard for authentication tokens, XACML is a language for defining authorization policies. A more complete view of distributed authorization approaches for grid applications is in [12] XACML supports a fuller range of authorization needs than the traditional POSIX security rules of allowing 3 classes of access (RWX) to three classes of users (UGO), which was designed to minimize the number of bits required in file system metadata in the 1960s.

The issues faced by DoD in their larger enterprise resemble the authentication and authorization problems faced by high-performance computing distributed file systems. The need is to have a fuller range of possible policies that are sensitive to environmental factors, user roles, and the current context. Centralized decision-making would be both a bottleneck and a single point of failure. Authorization decisions need to be made and enforced at the resource access point. For secure distributed file systems (ex. LWFS, PVFS, and LUSTRE) [13] , often decisions are made by a local daemon when access is first requested and cached. This avoids the delay caused by evaluating policies with each access. Caches can be flushed to revoke access and force reauthorization when the current context changes.

Unlike POSIX rules, policies are in essence a set of first-order predicate assertions that can be evaluated to determine whether access is allowed (TRUE or 1) or denied (FALSE or 0). Since XACML is XML-derived, policies can be hierarchical but the hierarchical nature is not necessary in this case since we are dealing with first-order predicate logic. This resembles both firewall rules and access control lists (ACLs). One difference is that this approach includes logical variables concerning the resource being accessed, the entity requesting access, the computing environment, etc. Policy execution can use the current environmental context to infer an entity's current role, etc. Also, in our DARPA Joint forces Air Component Controller (JFACC) program, subject matter experts discussed how "border crossing authority," when granted, changes the options available to combatants.

It is fair to assume that policies will be defined in advance. One issue to consider is that Goedel's incompleteness theorem [14] proves that logic can not be both consistent and complete. This means that any policy defined runs the risk of either having no answer (neither 1 nor 0) or having multiple answers (1 and 0) to a resource access request. It is also undesirable to use time and resources to execute logic programs for each process access request.

Cellular Communication: 5G/6G Zero trust at the edge – 5G and 6G technologies can offer superior communication performance for WTG by rapidly transmitting a large amount of operating data collected by sensors and quickly sending dispatching commands from one tank to other tanks with low latency, ultra-high speed, and improved reliability.

In the context of our current GVSC project, we are working on autonomous control of military ground fleets. Autonomy is defined by a variant of the Robot Operating System (ROS), where group actions are defined by publish/subscribe requests. Issues arise when connectivity is disrupted. In this environment, access to the name server is lost when connectivity is lost and the vehicles are disabled. We are therefore defining resource authorization policies that include definition of roles for entities within a given context and what actions entities may take given those roles. This approach is consistent with Van Creveld's rules for effective command and control [15] that insist on allowing lower echelons of command the ability to take initiative. Security rules only forbid inappropriate actions. This requires access to environmental attributes that would affect authorization decisions.

5G and Beyond 5G networks offer advanced security compared to previous cellular networks including unified user authentication protocol for 3GPP and non-3GPP access networks, enhancing equipment identity protection; and implementing the security edge protection proxy (SEPP). However, the diverse set of services, large number of devices, and cloud-based control create a large attack surface in 5G networks. The security threats are even more significant for DoD users operating in non-DoD zero-trust 5G networks where the network operator is untrustable. Based on zero-trust principles of trust never, verify always to protect data, assets, and services, we develop end-to-end security protocols for "operate through" scenarios where the serving non-DoD 5G network is untrustable, and legitimate DoD devices (e.g., autonomous vehicles) are in continuous risk of cyber and physical attacks. In such untrustable 5G network, the essence of chain of key derivations in 5G authentication and key agreement (5G-AKA) protocol which is relying on a secure long-term secret key shared between the network and user is no longer valid as the network cannot be trusted; therefore, the long-term keys can be exposed during the initial key distribution and production of the universal subscriber identity module (USIM) or being extracted from the devices via hacking attacks. Our recent works funded by the Air Force Research Laboratory focus on developing security solutions using pseudo-homomorphic authentication mechanisms rooted in tamper-resistant and unique embedded physical unclonable devices which not only authenticate the devices but also frequently authenticate the servers in zero-trust networks.

Security implications of Disaggregated O-RAN NextG Architecture – With the advent of open radio access network (O-RAN) standards, the disaggregation available with an O-RAN stack makes a modular microservices-based architecture possible. Here, individual configurable modules of the 5G/6G stack can be developed as microservices using standardized communication and information sharing modalities between modules. These microservices can then be orchestrated on a variety of mobile, edge and cloud computing resources to tie together new sensors, phased arrays and hardware acceleration on the one hand with AI/ML-based learning and optimization algorithms on the other. Jointly, these will provide the desired dynamic configurability to support the highly demanding DoD applications of the future. The approach yields computational and management efficiencies, along with increased reliability. Thus, the defining feature of O-RAN is the ability for a number of organizations to create elements of the disaggregated stack by virtue of microservices, and to scale them as needed by providing appropriate computing resources.

Major challenges immediately arise in the security context, since these microservices must each be authenticated and only allowed to communicate via a fixed set of modalities for each interacting pair. For example, each microservice must carry a certificate of authenticity and in a Zero-trust regime, the certificate and its issuer must be validated between information exchanges. The service will then be provided only as much access as its credentials enable. In the context of O-RAN the functional units of O-RU, O-CU, O-DU and the 5G core must all follow the zero-trust notion and mutually authenticate their credentials before communication. The communication itself must be encrypted to prevent eavesdropping between the functional units.

We will develop an open source, modular, 5G RAN stack, so we can incorporate new communication systems developments. We will build modular microservices consisting of different elements of the Lo-PHY, Hi-PHY and MAC layers of the open RAN stack to facilitate integration of high-bandwidth, low-latency communication systems into an existing open source 5G communication stack that we have considerable experience in working with. This architecture will help developers easily add new communication modalities and additional hardware, such as high-frequency phased arrays for experiments and demonstrations, without needing to modify the rest of the RAN stack. Each such module will possess different capabilities, can be configured at different timescales, and will have state information that can be used for decision and control. We will then develop a zero trust framework across these modules permitting the authentication encrypted communication approaches outlined above. This research thrust will provide security analysis of the 5G-enabled warfighting tactical edge by investigating the vulnerabilities under various cyberattack scenarios and develop AI/ML based detection and mitigation techniques, where a predictive model on cyberattacks will be trained with prior data collected from the sensors. This model will be evolved through continuous and transfer learning using the real-time data transmitted by 5G networks to detect cyber-attacks and deploy mitigation solutions.

RTOS implications to SDN in relation to zero-trust and edge computing – SDN separates the network control and data planes. By decoupling control plane decisions from the network forwarding hardware, network decisions from accessibility to forwarding can be controlled by software from separate and flexible locations away from the forwarding hardware. SDN also made the data plane highly customizable. While early day SDN solutions like OpenFlow is based only on Ethernet for packet header matching and rewrite/forward/drop actions, the latest Programming Protocol-independent Packet Processors (P4) paradigm supports design of new fields in packet headers and flexible user-designed actions by way of FPGA-based hardware. Contemporary SDN use cases have been based on header matching without timing considerations. Network control commands are executed based on best effort on the network hardware and can incur queuing delays of uncertain and variable nature. Implementing SDN on a RTOS paradigm will have significant implications by incorporating the time dimension into network control abstractions and implementation. Technologies like P4 make it possible to integrate precision timing sources, e.g., GPS-based PTP, into the control semantics. For ZT at the edge, this means that SDN control points can be deployed around the edge with time sensitive strategies, that the network can dynamically adapt the network boundaries based on the perceived level of threats, and that precise timing can become a strategy to detect anomalies due to network attacks or MITM attempts. End-to-end security protocols for "operate through" scenarios where the serving non-DoD 5G network is untrustable, and legitimate DoD devices (e.g., autonomous vehicles) are in continuous risk of cyber and physical attacks. In such untrustable 5G network, the essence of chain of key derivations in 5G authentication and key agreement (5G-AKA) protocol which is relying on a secure long-term secret key shared between the network and user is no longer valid as the network cannot be trusted; therefore, the long-term keys can be exposed during the initial key distribution and production of the universal subscriber identity module (USIM) or being extracted from the devices via hacking attacks.

2.4. *Thrust IV: Privacy, Trust, and Security in Data Dissemination*

The biggest threat to mission assurance is the lack of sharing of critical information in a timely and accurate manner in the cross-domain environment. This initiative will contribute to the science of privacy, trust, and security in data dissemination among security domains. In this initiative, we propose a framework for decentralized information sharing to overcome data dissemination problems while considering multiple aspects of the framework including privacy, integrity, and trust.

The enlarged attack surface along with the constant use of zero-day exploits hampers attack mitigation, especially when attacks originate at the kernel level. In a virtualized environment, an adversary that has fully compromised a virtual machine (VM) and has system privileges (kernel level, not the hypervisor) without being detected by traditional security mechanisms exposes the cloud processes and cloud-resident data to attacks that might compromise their integrity and privacy, jeopardizing mission-critical functions. The main shortcoming of traditional defense solutions is that they are tailored to specific threats, therefore limited in their ability to cope with attacks originating outside their scope. There is a need to develop resilient, adaptable, reconfigurable infrastructure that can incorporate emerging defensive strategies and tools. The architectures need to provide resiliency (withstand cyber-attacks, and sustain and recover critical function) and antifragility (increase in capability, resilience, or robustness as a result of mistakes, faults, attacks, or failures).

There is a need to build systems capable of collecting, analyzing, and reacting to dynamic cyber events across all domains while also ensuring that cyber threats are not propagated across security domain boundaries and compromise the operation of the system. Solutions that develop a science of cyber security that can apply to all systems, infrastructure, and applications are needed. The current resilience schemes based on replication lead to an increase in the number of ways an attacker can exploit or penetrate the systems. It is critical to design a vertical resiliency solution from the application layer down to physical infrastructure in which the protection against attacks is integrated across all the layers of the system (i.e., application, runtime, network) at all times, allowing the system to start secure, stay secure and return secure+ (i.e. return with increased security than before) after performing its function.

The research involves the discovery, propagation, and aggregation of information shared by multiple participants across domains under varying situations and contexts. The thrust of this research includes the dissemination of private data, privacy, and trust, privacy metrics. Data dissemination should assure that different organizations can share their sensitive data without compromising privacy. Algorithms will be designed to evaluate the privacy loss due to disclosure of information and gain trust. A series of experiments will provide guidelines in privacy measurement, trust assessment, and quantification of the tradeoff between privacy and trust. A privacy assessment metric will be developed that employs information-theoretic approaches to measure privacy. Various privacy violator models and user behaviors will be used as benchmarks for testing and evaluating different privacy-preserving techniques.

Innovative Claims – A fundamental paradigm for decentralized information sharing to overcome existing hurdles in collaboration while considering privacy, integrity, and trust is proposed. The research integrates disciplines of database systems, quality of service (QoS), privacy, trust, and contextual/situational awareness. The proposed research introduces a new paradigm that should change the way we think about data. Currently, we use data as a passive entity that cannot protect itself. Data require the use of a trusted entity to protect them, e.g., a trusted processor or a trusted third party. In contrast, in the proposed research we transform passive data into an active entity, able to self-protect.

The research increases the efficiency of data self-protecting solutions by eliminating the application of inefficient approaches such as the use of trusted hardware, the use of trusted third parties, or the use of threshold-based multi-party computing. Algorithms for data filtering and apoptosis for various levels of classification (top secret, secret, confidential and unclassified) will be developed. Algorithms for proactive dispersion of information, situational-aware paradigm, integrity checks and violator identification methods, information adaptability, and active bundles will result from this effort.

Significance – Privacy threats increase with accidental uncontrolled data diffusion or malicious data disclosures by means of intentional attacks. Critical facts and hidden problems are often revealed and confirmed by the sharing and aggregation of information that is seemingly irrelevant to each other. The Cross Domain Solution (CDS) is the key enforcement point for the security of the information. The current CDS has very limited ways to respond to an attack and when compromised, simply "shut down" into a secure state, eliminating the flow of information into and out of that device. A CDS that is able to adapt policy can cut off other channels, but keep mission-critical information flow active and maintain survivability. The proposed research will contribute to a variety of collaborative missions including Cloud Computing and continuous flow of information for mission planning and assurance and continuous collaboration.

Bias-aware Zero Trust Few Shot Federated Learning – On the battlefield multiple different entities or edge equipment utilize ML models for accomplishing a task without the requirements of human maneuver. The performance of these ML models enhances with the enrichment of data or situational information. Under the DDIL (denied, disrupted, intermittent, and limited) environment of the battlefield sharing such information may not be feasible in all cases. To overcome this issue, in this task we will develop a few shots of a federated learning environment that can enhance collaboration among edge devices as well as can train ML models with limited training sets. Moreover, we will utilize the homomorphic encryption technique for model aggregation and averaging on the server side of the federated learning. This will eliminate the risk of model parameter hijacking/inference attack during sharing and also comply with the zero trust notion of the project.

However, few-shot learning itself suffers from bias issues due to the scarcity of training data, and in battlefield aggregating and pre-processing (labeling) large amounts of training data may not be a feasible option. This situation exacerbates when none of the entities, in federated learning, is trustworthy and the server side can only compute over ciphertext. To address the bias issue, we propose a fairness-aware multi-agent diversified training scheduler that can dynamically diversify the training mechanism by interchanging the local training models during each global training epoch. The scheduler will utilize the reinforcement learning approach to optimize between the performance and bias of the global model while making the interchanging decision of local models. The goal of this project is to task independently reduce the impact of biases in federated few shots learning and develop a generalizable (or easily configurable to different tasks) fairness-aware federated few shots learning platforms. The challenging part of this will be enabling the operation of a multi-agent scheduler in the presence of encrypted ciphertext.

Our team has experience in building provenance graphs to model and monitor activities inside multi-host networks spanning hundreds of millions of events per day, with the goal of detecting malicious behaviors. We propose to use our expertise to define a graph-based modeling approach to the activities in the scenario and define context-aware policies of permissions as rules on this graph. E.g., if we envision a network composed of wearable routers, routers on vehicles, etc, this network would be represented as a provenance graph with policies to match specific scenarios).

3 Testbed Design and Overall Assessment Plan

3.1. Testbed Design Plan

To evaluate the performance of the proposed holistic solutions in terms of resilience and security, appropriate mission-critical IoBT testbeds become necessary. We plan to design real-life testbeds to serve this purpose. During the initial phase, we will conduct research and experiments in small teams having relevant expertise. The testbeds will follow the structure of IoBT systems comprising the following aspects. ***(i) Mobility:*** testbeds will include many mobile edge devices including a number of stationary edge devices. ***(ii) Capacity:*** testbeds will be designed to keep the energy and computing budget suitable for the tactical edge. ***(iii) Workload:*** testbeds will be designed to handle dynamic workload (due to the system mobility) compared to well-defined traffic patterns. ***(iv) Heterogeneity:*** we will incorporate the heterogeneity in the designed testbed in two ways. First, heterogeneous computing platforms (e.g., X86, ARM, and GPU) will be selected for individual or a set of IoBTs. Second, various hardware units (e.g., communication and computing modules, sensors) will be assembled and examined. Overall, we will perform the system assessment under different hardware and software setups, with diverse computing/communication capacities and workloads.

The proposed solutions will be thoroughly validated through high-fidelity simulation tools (e.g., DETER, PlanetLab, NS3, Simulink, Simu5G, FABRIC, and facilities supporting distributed automotive systems) and experiments on real-world testbeds designed as discussed above.

The performance of the developed identity verification system, mutual authentication, and anomalous behavior detection system will be evaluated using the metrics per the ISO/IEC standard 19795 for verification system performance evaluation [16]. This includes verification/detection accuracy, equal error rates (EER), false accept rates (FAR), false reject rates (FRR), RoC area measurements, cost, usability, and versatility.

3.2. Research Thrust Level Assessment Plan

The proposed research will be evaluated initially by extensive simulations. The IoBT system will be evaluated for its performance in different deployment setups such as data sharing and dissemination scenarios like edge cloud, mobile cloud, SOA, etc., and investigate how changing the distribution of the cyber-enabled warfighting devices affects the performance of the proposed zero trust model. This will help us further evaluate the balance between performance and security level.

We will use AWS Zero Trust systems and other vendor ZT platforms to test our warfighting IoBTs considering both identity-centric and network-centric defenses as these are two key building blocks for Zero Trust. In the cloud these are their IAM (Identity Management) and VPC systems (Virtual Private Cloud). Experiments will be conducted to evaluate the "parent" IAM and VPC when these are become compromised and contain malicious actors. Thus, the key problem is to be able to create "on-the-fly" new VPC and IAMs that are capable of operating with "bad-actors" present. We will explore the solution by constructing or deploying new micro-segments with new IAM and VPC Zero Trust Capabilities. Evaluation results will be analyzed to determine a suitable privacy threshold to control the dissemination, restrict it or adjust it dynamically based on the amount of content already disseminated and other contextual information to identify the amount of data the destination host can deduce through the available information.

Experiments will be conducted to determine suitable methods to provide selective disclosure by deploying cryptographic methods such as polymorphic and incremental encryption/decryption and Blockchain technologies such as distorting the sensitive data by adding noise to the data and then using various data filtering techniques to disseminate the correct amount of data, for example, in case of masking image data, techniques like low dynamic range rendering, pattern recognition, and blurring, etc.

Overall, methods will be developed and evaluated in different models such as with and without a trusted third party, multiparty computation, publish-subscribe model, peer-to-peer model, service-based model (SOA), etc.

Appendix A - Partnerships: Expertise and Responsibilities

Table 1 presents a list of core participants and their roles and responsibilities for the project. The project team represents a unique combination of foundational world-class expertise in both basic and applied research and world-class expertise in technology transition involving multiple research to products pipeline.

Table 1: List of Core Participants and their Expertise and Responsibilities

Name (PoC)	**Areas of Expertise and Responsibility**	**Affiliation**
Dipankar Dasgupta [redacted]	Computational Intelligence in Cybersecurity	Dept. of Computer Science, University of Memphis
John R. Williams [redacted]	Cloud Computing, Applied Cybersecurity, Blockchain Disruptive Technology	Dept. of Civil and Environmental Engineering, Massachusetts Institute of Technology (MIT)
Vir Virander Phoha [redacted]	Authentication, Machine Learning, Non-linear Prediction	Dept. of Electrical Engineering and Computer Science, Syracuse University
Bharat Bhargava [redacted]	Privacy Preserving Data Dissemination and End-to-End Security	Dept. of Computer Science, Purdue University
Chris Clifton [redacted]	Data Privacy, Data Mining	Dept. of Computer Science, Purdue University
Nitesh Saxena [redacted]	Aspects of Cybersecurity, with Emphasis on Computer Systems and Network Security	Dept. of Computer Science, Texas A&M University
Guofei Gu [redacted]	Network and Systems Security, Malware and APT Defense	Dept. of Computer Science, Texas A&M University
Srinivas Shakkottai [redacted]	Multi-agent learning, Game Theory, Wireless Networks, Reinforcement Learning	Dept. of Computer Science, Texas A&M University
Lena Mashayekhy [redacted]	Edge Computing, Cloud Computing, IoT	Dept. of Computer and Information Science, University of Delaware
Sanjay Madria [redacted]	Cybersecurity and Access Control in Tentacle Networks	Dept. of Computer Science, Missouri University of Science & Technology
Syed Rafiul Hussain [redacted]	Systems and Network Security, IoT	Dept. of Computer Science, Penn State University
Narendra Ahuja [redacted]	Computer Vision, Pattern Recognition	Dept. of Computer Science, University of Illinois at Urbana-Campaign
Venkat Venkatakrishnan [redacted]	Authorization and Access Management, Threat Detection and Analysis	Dept. of Computer Science, University of Illinois at Chicago
Chao Wang [redacted]	Authentication and Network Protocol Security, Dynamic Identity Management	Dept. of Computer Science, University of North Carolina at Charlotte
Diksha Shukla [redacted]	Secure and Trustworthy ML, Authentication, IoT and Wearable Devices Security	Dept. of Electrical Engineering and Computer Science, University of Wyoming
Kishor Datta Gupta [redacted]	AI-based Models Security including Model Robustness Evaluation	Dept. of Computer Science, Clark Atlanta University
Meng Yu [redacted]	Computer and Networks Security	Dept. of Computer Science, Roosevelt University

Appendix B - Preliminary Works/Publications

The core participants have expertise in the area of the proposed initiative and have conducted extensive prior work in the closely related area [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31].

References Cited

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture (2nd draft)," National Institute of Standards and Technology, Tech. Rep., 2020.

[2] P. Shrestha, N. Saxena, D. Shukla, and V. V. Phoha, "Press @$@$ to login: Strong wearable second factor authentication via short memorywise effortless typing gestures," in *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2021, pp. 71–87.

[3] C. Shi, Y. Wang, Y. Chen, N. Saxena, and C. Wang, "Wearid: Low-effort wearable-assisted authentication of voice commands via cross-domain comparison without training," in *Annual Computer Security Applications Conference*, 2020, pp. 829–842.

[4] P. Shrestha and N. Saxena, "Hacksaw: biometric-free non-stop web authentication in an emerging world of wearables," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 13–24.

[5] B. Shrestha, M. Mohamed, and N. Saxena, "Zemfa: zero-effort multi-factor authentication based on multi-modal gait biometrics," in *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 2019, pp. 1–10.

[6] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *computers & security*, vol. 63, pp. 85–116, 2016.

[7] D. Dasgupta, A. K. Nag, and A. Roy, "Adaptive multi-factor authentication system," Mar. 6 2018, uS Patent 9,912,657.

[8] S. Jarecki, H. Krawczyk, M. Shirvanian, and N. Saxena, "Device-enhanced password protocols with optimal online-offline protection," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 177–188.

[9] M. Shirvanian, S. Jarecki, N. Saxena, and N. Nathan, "Two-factor authentication resilient to server compromise using mix-bandwidth devices." in *NDSS*, 2014.

[10] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication," in *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2014, pp. 163–171.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89–98.

[12] W. Jie, J. Arshad, R. Sinnott, P. Townend, and Z. Lei, "A review of grid authentication and authorization technologies and support for federated access control," *ACM Computing Surveys (CSUR)*, vol. 43, no. 2, pp. 1–26, 2011.

[13] R. Brooks, B. Husain, S. Yun, and J. Deng, "Security and performance evaluation of security protocols," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 2013, pp. 1–4.

[14] P. Smith, *An introduction to Gödel's theorems*. Cambridge University Press, 2013.

[15] M. Van Creveld, *Command in war*. Harvard University Press, 1985.

[16] E. P. Kukula and S. J. Elliott, "Beyond current testing standards: A framework for evaluating human-sensor interaction," in *International Biometric Performance Testing Conference*, 2010.

[17] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE transactions on sustainable computing*, vol. 4, no. 1, pp. 88–95, 2018.

[18] A. Kott, A. Swami, and B. J. West, "The internet of battle things," *Computer*, vol. 49, no. 12, pp. 70–75, 2016.

[19] S. Rose, "Planning for a zero trust architecture: A planning guide for federal adminstrators," National Institute of Standards and Technology, Tech. Rep., 2022.

[20] R. Ranchal, B. Bhargava, P. Angin, and L. ben Othmane, "Epics: A framework for enforcing security policies in composite web services," *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 415–428, 2018.

[21] N. Wang, J. Fu, J. Zeng, and B. K. Bhargava, "Source-location privacy full protection in wireless sensor networks," *Information Sciences*, vol. 444, pp. 105–121, 2018.

[22] B. Bhargava, P. Angin, R. Ranchal, R. Sivakumar, M. Linderman, and A. Sinclair, "A trust-based approach for secure data dissemination in a mobile peer-to-peer network of avs," *International Journal of Next-generation Computing*, pp. 01–12, 2012.

[23] Y. Lu, W. Wang, B. Bhargava, and D. Xu, "Trust-based privacy preservation for peer-to-peer data sharing," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 36, no. 3, pp. 498–502, 2006.

[24] L. Lilien and B. Bhargava, "A scheme for privacy-preserving data dissemination," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 36, no. 3, pp. 503–506, 2006.

[25] X. Cao, S. Datta, R. C. Bolla, and S. Madria, "Targeted content-sharing in a multi-group dtn application using attribute-based encryption," in *2022 23rd IEEE International Conference on Mobile Data Management (MDM)*. IEEE, 2022, pp. 306–309.

[26] M. A. Islam and S. Madria, "Attribute-based encryption scheme for secure multi-group data sharing in cloud," *IEEE Transactions on Services Computing*, 2020.

[27] D. Dasgupta, A. Roy, and D. Ghosh, "Multi-user permission strategy to access sensitive information," *Information Sciences*, vol. 423, pp. 24–49, 2018.

[28] A. Roy and D. Dasgupta, "A robust framework for adaptive selection of filter ensembles to detect adversarial inputs," in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2022, pp. 59–67.

[29] P. Shrestha and N. Saxena, "Listening watch: Wearable two-factor authentication using speech signals resilient to near-far attacks," in *Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks*, 2018, pp. 99–110.

[30] S. Jarecki, H. Krawczyk, M. Shirvanian, and N. Saxena, "Two-factor authentication with end-to-end password security," in *IACR International Workshop on Public Key Cryptography*. Springer, 2018, pp. 431–461.

[31] B. Shrestha, M. Shirvanian, P. Shrestha, and N. Saxena, "The sounds of the phones: Dangers of zero-effort second factor login based on ambient audio," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 908–919.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Haun Ventures

HAUN

The Role of Digital Assets in Supporting Sustainable Open-Source Software Development

Response to Request for Information on Digital Assets Research and Development Agenda from the White House Office of Science and Technology Policy

March 3, 2023

For additional information on this response please contact:

Tomicah Tillemann
Chief Policy Officer
Haun Ventures
[redacted]

About Haun Ventures

Haun Ventures is a venture capital firm founded in 2022 by former federal prosecutor and Andreessen Horowitz partner Katie Haun. We currently invest through two vehicles, a $500 million early-stage fund, and a $1 billion acceleration fund, both of which are dedicated to exclusively investments across the digital asset ecosystem. Our firm's executive team has extensive experience serving at the highest levels of every branch of the federal government, and our limited partners include leading foundations, university endowments, and healthcare providers.

Questions Addressed

This submission addresses the following thematic areas outlined in the RFI:

1. Goals, sectors, or applications that could be improved with digital assets and related technologies;
2. Goals, sectors, or applications where digital assets introduces risk;
3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets; and
4. R&D that should be prioritized for digital assets.

Recommendations

The primary recommendations described in this submission include:

1. Research strategies to incentivize open-source software development and open-source networks.
2. Pursue research into staking as a means of securing open-source networks.
3. Encourage responsible governance mechanisms for overseeing the development of open-source software.
4. Help policymakers regulate centralized applications responsibly without undermining the innovation and the development of decentralized protocols.
5. Advance a research agenda to address the risks to U.S. competitiveness associated with a failure to embrace digital asset technology, including by following the lead of California and other states working to expand government's capability to serve citizens by applying web3 technology effectively.

Digital Assets and Open-Source Technology

Open-source software has a long, successful history dating back to the early days of the internet. However, siloed, proprietary models of software development have driven the rise of Big Tech over the past two decades. Open-source software is a compelling alternative model: one where core protocols are built by communities of technologists that come together to create more effective and secure approaches to problem-solving. Generally speaking, open-source software development prioritizes transparency, in that anyone can conduct audits and recommend improvements. Large, sophisticated open-source software repositories enable far more people to enjoy benefits from—and participate in—rapid, inclusive innovation. Open-source software is particularly vital to small startups and others seeking to challenge legacy incumbents. It helps new projects with good ideas but limited resources compete against entrenched monopolies. Community-owned, community-governed open-source platforms can help give individuals far more control over their data. They have the potential to provide meaningful alternatives to Big Tech and democratize an increasingly feudal digital economy.

However, realizing this potential will require policymakers to foster new, sustainable models for incentivizing contributions to open-source projects. Despite its significant benefits, open-source software has historically lacked sustainable funding models. Many open-source software contributors and maintainers are volunteers. They write code for open-source projects in their free time or as part of their employment with larger tech firms. Traditionally, due to a lack of incentives, it has been difficult or impossible to make contributing to open-source software a viable career. Digital tokens are one of the only proven solutions for building world class, financially sustainable open-source software and open-source networks. The United States needs a national research agenda to capitalize on that potential.

The stakes are high. The current dominant technology paradigms offer users a choice between two broken models: one, an authoritarian approach emanating from Beijing, aggregates users' private data to manipulate behavior for political purposes. The other, a Big Tech model emanating from Silicon Valley and Seattle, aggregates private data to manipulate behavior for commercial purposes. Neither is compatible with a healthy, open society. For the foreseeable future, centralized, authoritarian systems are likely to have access to more data to power artificial intelligence algorithms due to their almost unlimited use of surveillance. This will give them an edge in AI-powered applications. The rapid innovation and iteration enabled by open-source development provides open societies with what may prove to be a critical mechanism for outcompeting and out-innovating authoritarian adversaries.

U.S. policymakers should embrace open-source development and decentralized open-source networks as the alternative to the discredited approaches of Big Tech and authoritarian governments. However, expanding the use of open source will only be financially viable and sustainable if government provides policy architecture that can help incentivize the long-term development and maintenance of open-source code. The use of digital tokens to incentivize contributions to open-source software projects and networks is a key breakthrough that merits additional study.

OSTP should consider the following areas for further research:

1. Clarifying compensation for open-source contributors through digital tokens
2. Expanding the use of privacy-preserving technologies, such as zero-knowledge proofs
3. Encouraging staking as a means of securing open-source networks
4. Facilitating responsible governance of open-source software
5. Regulating centralized applications, not protocols
6. Addressing the risks to U.S. competitiveness associated with a failure to embrace digital asset technology

Recommendations

1. Provide clarity on how to compensate open-source contributors with digital tokens

Broadening the use of open-source software depends on fostering more sustainable models for incentivizing the open-source development. Digital tokens have proven their utility as a powerful tool for encouraging the ongoing development and maintenance of open-source software by facilitating the type of long-term developer activity required to deliver open-source breakthroughs such as the Ethereum merge. However, uncertainty about the regulatory framework surrounding digital tokens is crippling their use to support open-source software development in the United States.

The European Union, United Kingdom, Japan, Australia, and many other jurisdictions are moving to provide regulatory clarity that will facilitate the use of digital tokens to compensate open-source software contributors. The United States is not. This is likely to accelerate the ongoing migration of talent away from the United States. Already, research by Electric Capital shows that the share of U.S. contributions to open-source web3 projects has fallen from almost 70% in 2015 to under 50% today. Policymakers should move quickly to provide clarity on the use of digital tokens in order to halt the ongoing exodus of talent from the sector.

2. Expand the use of privacy-preserving technologies

Blockchains, as originally developed, are public by default. All transaction history, account balances, and smart contract execution is available for anyone to inspect. But web3 cannot scale without unlocking privacy, for the simple reason that mainstream participants and institutions won't use technologies where all of their data is available to the public.

Zero-knowledge proofs (ZKPs) are an exceptionally powerful method of privacy-preserving computing that will have far reaching applications. ZKPs enable one party to prove to another party that something is true without revealing the underlying data or requiring the underlying information. For example, ZK cryptography would allow you to verify that you were over 25 to rent a car without having to disclose your birth date, or prove that your income qualifies you for a government benefit without having to disclose your salary.

In 2016, the Zcash protocol launched using ZKPs to obfuscate the details of user transactions in a Bitcoin-like payment network. In the last few years, advances in ZK circuit constructions, accelerations in prover efficiency, and more efficient software implementations have paved the way for ZKPs that support private general purpose smart contract execution. ZKPs are practical because the proofs they generate are fast and efficient, and they represent a promising class of technology for verifiable computation and data compression—both core, unsolved problems for scaling a privacy-preserving internet.

There are currently dozens of teams building privacy-focused infrastructure that leverages ZK computing, including our portfolio company Aleo. Other teams, including our portfolio company Sovereign Labs, are using ZKPs for their scalability benefits. More privacy-focused infrastructure will lead to more privacy-focused applications. However, it will also introduce new challenges into the ecosystem. This dynamic is already playing out with the U.S. Treasury Department's decision to sanction the Tornado Cash application, a piece of privacy-preserving code running on Ethereum.

Over the last six years, ZKPs have made great strides moving from theory to application, but it is still very early in development of the technology. With appropriate input from policymakers, the industry will be better positioned to converge on best practices. ZKPs are a revolution in computer science and cryptography. Unlike the consumer internet that we know today, they will be built in public. Policymakers will benefit from engaging early and often with builders in the space as they work to adapt regulation and systems to take advantage of the opportunities around ZK technology.

3. *Encourage staking as a means of securing open-source networks*

The transparency and built-in accountability of open-source networks make them compelling alternatives to the walled gardens of Big Tech. Securing these networks efficiently is often achieved through staking, where community members use their network ownership to help secure and maintain the integrity of network data. Current tax guidelines unnecessarily penalize staking by treating it differently than similar activity in other parts of the economy. OSTP should consider two lines of staking research: first, examination of how staking can secure open-source digital networks and democratize the financial benefits of network participation among network users. Second, joint research with the Treasury Department, the

Internal Revenue Service, or other relevant agencies to assess how best to place staking activity on an equal footing with other forms of economic engagement. Current IRS rules penalize staking by treating it differently from analogous activity in the traditional economy. Establishing clear policy in this area will encourage broader use of secure, community-owned open-source digital networks.

4. Facilitate responsible governance

In some cases open-source software is being managed by communities through decentralized autonomous organizations, or DAOs. These new structures for communal decision-making provide a more democratized, transparent framework for building and maintaining open-source software. Recent regulatory actions have had the unintended consequence of forcing many actors to pull back from participation in DAO structures and governance, which is already negatively impacting the development of open source code. (Haun Ventures recently filed a petition to address this issue with the CFTC.) Policymakers should move quickly to research and embrace new rules that will make it possible for DAOs to provide good governance over open-source protocols.

5. Regulate applications, not underlying protocols

Applications provide the onramps that consumers use to access digital services. Many centralized applications are businesses. As businesses, they need to address a variety of compliance issues and provide a logical point of engagement for consumer protection regulation. Protocols—such as email, SMTP, and HTML—operate independently of any business. They are not structured or equipped to run compliance efforts. OSTP should support research into best practices for facilitating innovation-forward approaches to regulation that protect consumers and allow for appropriate regulatory oversight of businesses, while safeguarding the autonomy and decentralized independence of protocols.

6. Advance a research agenda to address the risks to U.S. competitiveness associated with a failure to embrace digital asset technology

A failure to develop policy architecture that facilitates the responsible growth of new technology paradigms will not only risk an exodus of good jobs and economic activity from the United States, it could also limit U.S. access to digital rails that would otherwise be essential to American national security and global influence. The United States and its allies have used their influence over the SWIFT network—the Society for Worldwide Interbank Financial Telecommunication—to freeze international payments by individuals and organizations that finance terrorism, engage in criminal behavior, and, most recently, violate international law by invading their neighbors. However, while well-intended, SWIFT was built for a different age and, as a result, can no longer compete effectively with the sophisticated systems championed by authoritarian governments.

Many traditional payments technologies, such as cash, checks, bank wires, and credit cards have proven expensive, slow, and vulnerable to exploitation by bad actors. Harvard economist Ken Rogoff estimates that one-third of all U.S. currency in circulation is used for crimes and tax evasion. Credit card fraud costs the global economy over $32 billion annually. Tens of millions of credit card users have also been subject to data breaches that increase their vulnerability to identity theft. Check fraud is an old problem, but it has surged back into headlines as governments have distributed fiscal stimulus in response to the pandemic. Initial estimates suggest that criminals stole $100-400 billion in U.S. pandemic assistance funds that were intended for needy families.

During the earliest days of the internet, the use of money online was prohibited by the U.S. government. Because the internet was a government research project, any commercial activity on the web was a violation of its terms of service. Predictably, the network that grew from these initial regulatory decisions was poorly equipped to handle financial transactions.

Today, Alipay and Tencent's WeChat Pay, the two dominant Chinese payment platforms, include tightly integrated, instantaneous access to everything from bill payment and bank account transfers to food delivery, social media, ride shares, transit tickets, insurance, digital ID, and credential storage. These platforms are among the most ambitious, successful payments solutions available anywhere on the planet, and the Chinese Communist Party (CCP) is encouraging their global adoption through its Digital Silk Road and Belt and Road Initiatives. The CCP is also introducing a Digital Yuan or eCNY with a digital form factor that is far superior to the U.S. dollar. According to the Atlantic Council, the eCNY system has achieved higher transaction throughput than the Visa network and gained widespread adoption. As of December 31, 2021 there are already 260 million active eCNY wallets, and users enjoy settlement speeds and transaction costs that are orders of magnitude better than U.S. systems. The People's Bank of China (PBoC) is now working with the Bank of International Settlements on cross-border interoperability with Hong Kong, Thailand, and the UAE. Growing adoption of the eCNY will enable the Chinese government to monitor transactions in real time, freeze the assets of ethnic minorities and dissidents, and "de-platform" users at will. These trends should be deeply concerning to democratic governments.

The U.S. AML/KYC (anti-money laundering / know your customer) framework is also struggling. Current U.S. AML/KYC compliance processes allow an estimated $300 billion in illicit transactions each year yet cost American and Canadian Banks roughly $56 billion annually to implement. These costs do not include losses from the thousands of legitimate projects, small businesses, and transactions that never move forward due to prohibitively high compliance fees. These regimes also prevent millions of Americans and billions worldwide from accessing financial services. The Wall Street Journal reported that independent ATMs are vanishing in parts of America that need them most – areas with the highest percentage of unbanked and underbanked Americans – due to prohibitively high costs of compliance.

These challenges are having a direct impact on the U.S. economy, national security, and working families. The long waits required to process and clear transactions are a prime reason for the roughly $30 billion spent each year on check cashing, payday lending, and bank overdraft services.

Developed responsibly, web3 platforms can provide alternatives to an increasingly dysfunctional status quo. While nascent and certainly not a panacea, the web3 toolbox can help policymakers construct a new generation of digital infrastructure. Web3 can provide individuals with much greater control over personal data and ownership of the networks they use. The successful, extensive use of web3 platforms to respond to the crisis in Ukraine is the latest compelling evidence that web3 can help democracies create resilient digital infrastructure while strengthening national security. Ukrainian authorities have used web3 platforms to gather over $100 million in support from individuals worldwide. They have also used web3 storage networks such as Arweave to create permanent copies of critical government records and secure evidence of wartime atrocities perpetrated by Russian forces. FinCEN and other law enforcement and intelligence agencies have stated repeatedly that the public nature of blockchains coupled with use of analytics platforms such as Chainalysis, TRM, and Crystal enables U.S. officials to effectively police sanctions compliance. California has announced plans to help fix one of the most dreaded forms of citizen-government interaction – the Department of Motor Vehicles – onto blockchain.

There are other promising templates that demonstrate how web3 can help strengthen trust in open societies and institutions. For example, while a much smaller country, Estonia's digital platforms allow government agencies and financial institutions to offer nearly universal access to a broad range of sophisticated services. Utility payments, pension contributions, and taxes all rely on shared digital infrastructure to channel information between government agencies and citizens' accounts. At the core of the system is a digital identity and data framework that securely moves information and assets between individuals, companies, and government agencies. The availability of a trusted digital identity solution streamlines KYC compliance for banks, and enables financial institutions to process mortgages, loans, and even requests to open new accounts entirely online. The system has powerful benefits for public administration, enabling citizens to file their taxes in minutes. Estonia's digital systems also do a better job of safeguarding personal data. Users see who is accessing their information in order to help identify and deter any illicit use of personal information. The system is so efficient that it generates savings equivalent to 2 percent of GDP each year.[1]

Conclusion

As with almost any technology, open-source software can be harnessed for good and bad—and society needs clear rules of the road to help mitigate the bad. However, concerns about the potential misuse of digital assets are currently overriding the responsible development of the technology. This dynamic in the face of intensifying foreign competition risks the U.S. falling behind in leveraging digital assets and web3 technology to advance our national values and interests, including the accelerated development of open-source software. OSTP research can help realize the potential of digital assets and open source software to address widespread failures of legacy systems. The responsible development and governance of next generation open digital systems would benefit from a multistakeholder approach, consistent with how the U.S. has historically approached such challenges. Ideally, multi-stakeholder councils with participation from civil society, government, and the private sector should provide oversight of these systems as they mature.

[1] For additional discussion of these and other forms of open source digital public infrastructure, please see Tillemann, Tomicah. 2022. "How Digital Systems Will Transform the Future of Money and Development." In *Breakthrough: The Promise of Frontier Technologies for Sustainable Development,* edited by Homi Kharas, John W. McArthur, and Izumi Ohno. Washington, DC: Brookings Institution. (attached)

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Hedera Hashgraph, LLC

March 3, 2023

Ms. Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

Re: FR Doc. 2023-01534, "Request for Information; Digital Assets Research and Development"

Dear Deputy General Counsel Wallace:

We welcome the opportunity to provide the Office of Science and Technology Policy with our feedback to the Request for Information titled Digital Assets Research and Development. We want to express our appreciation for your efforts to prioritize research and development related to digital assets and their underlying technologies. We agree that responsible innovation in these technologies and their applications will provide significant benefits for the American people, and we appreciate the Administration's approach to advancing innovation within this emerging technology with a whole-of-government approach that starts with collecting relevant details, often from industry participants such as ourselves, which we are more than happy to provide.

The Hedera Council ("Council")[1] is a coalition of twenty-eight (28) independent and unaffiliated organizations who collectively operate and govern a Distributed Ledger Technology ("DLT") network based on the hashgraph consensus algorithm (the "Hedera Network")[2]. As with other DLT networks, the Hedera Network provides a network-native digital asset for application developers and users to utilize when making the micropayments required whenever they consume a Hedera Network service, i.e., whenever their application makes an API call to the network. In the case of the Hedera Network, that digital asset is called an "hbar." This is a fundamental requirement of any public implementation of digital asset technology because

[1] https://hedera.com/council
[2] https://hedera.com/how-it-works

anyone can use such APIs to build Web3 applications with high throughput, fair ordering, and low-latency consensus finality in seconds without relying on centralized infrastructure, but only if there is a cryptographically secure method of fairly compensating all of the decentralized infrastructure providers responsible for making these services available to the public. In the case of the Hedera Network, our coalition of independent network node operators provides these services in an environmentally and financially sustainable manner, as documented in a 2021 study from University College London that was updated earlier this year[3]. This is partially due to the fact that the Hedera Network uses a proof-of-stake security model, which is an increasingly popular and environmentally sustainable method of securing a distributed public ledger.

We have focused our response on Question 4, "R&D that should be prioritized for digital assets." Below we highlight the importance of the development of digital identities, useful in helping a potential U.S. CBDC system align with policy objectives.

* * *

Digital identity is a nascent yet critical component of digital asset infrastructure for a wide range of digital asset applications. While there are also significant privacy considerations that must be accounted for, the implementation of flexible and secure digital identity functionality will enable various applications to achieve regulatory compliance, manage risk, and adhere to public policy goals. Additional research and development on digital identity is likely a prerequisite to the implementation of a central bank digital currency aligned with the Biden-Harris Administration's *Policy Objectives for a U.S. CBDC System*.

Additional research, development, and testing of identity token[4] functionality and other digital identity implementations is necessary to ensure a balance is achieved between protection of privacy rights and mitigation of illicit finance, and to ensure the tools are used to promote democracy, equity, and fairness as part of a future U.S. CBDC. Specific areas of research and development include appropriate standards for determining identity, appropriate cybersecurity standards for identity tokens and any vendors or contractors hired by the U.S. Government to implement a digital identity system, and ensure that updates of the digital identity infrastructure are efficient and secure to avoid breach of confidentiality, economic losses, or downtime of the digital identity system.

* * *

[3] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4324137
[4] https://hedera.com/blog/the-rise-of-the-identity-token

We welcome additional dialogue on digital identity and its associated standards and privacy considerations, as well as other ways Hedera can support research and development efforts to achieve the Administration's *Policy Objectives for a U.S. CBDC System*.

Sincerely,

[redacted]

Brett McDowell, Chair
Hedera Hashgraph, LLC

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Homeopenly

From:	Dmitry Shkipin
To:	DARD-FTAC-RFI
Subject:	RFI Response: Digital Assets R&D Agenda
Date:	Sunday, January 29, 2023 2:35:18 AM
Attachments:	Outlook-https ho.png

A digital asset is anything that exists in digital (binary) form and comes with a distinct usage right, such as copyrighted works. Digital rights management (DRM) is the management of legal access to digital assets. Digital assets may include things like digital movies (ex. Finding Nemo), software (ex. Microsoft Windows), or websites (ex. Google) that are copyrighted, typically serve a genuine purpose to consumers, government, and businesses, and typically produce some form of revenue.

Binary data that do not possess some form of right to use are not considered assets. The one and only definition of a term "digital asset" is not up for a debate, or some form of re-definition - if some data has no right to use, it is not an asset.

Binary data is, by itself, useless and cannot be used to generate revenue. A digital token (ex. Bitcoin) is a form of binary data that may unlock some "assumed" stored value within another database (ex. Bitcoin ledger) but by itself, binary data is useless, it is merely just sets of 1s and 0s. On the other hand, "Crypto exchange" website is a digital asset because it is tied to some entity and is subject to copyright (the requirement for a conversion into fiat by some type of a legally formed entity with bank account is an Achilles heel of all alternative currencies.)

This Digital Assets R&D Agenda RFI asks the public to submit comment on the matter of digital assets, but the request's definition is flawed. The request really asks the public to comment on certain sets of binary data stored as 1s and 0s that have no rights to use, that are unable to produce revenue. The attempt to redefine the term speaks of ignorance, rather than knowledge.

That same way plain old paper can be used to print fiat currency, binary data can be used to create, store, and maintain virtual currency (not as a security, or investment contract, but a pure medium of exchange) issued to the general public for the purpose of serving as currency.

Presently, virtual currency is defined by the United States Treasury as “a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; and is neither issued nor guaranteed by any jurisdiction.” (Source: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626)

In 2013, FinCEN issued guidance stating that the definition of a money transmitter includes an individual who offers exchange services between virtual currency and fiat currency. See United States Treasury FinCEN Guidance, Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013- G001 (Mar. 18, 2013). The

FinCEN Guidance stated, among other things, that those who are money transmitters because they offer exchange services between virtual currency and fiat currency also come within the regulations applicable to MSBs. That guidance was reaffirmed in May 2019. United States Treasury FinCEN Guidance, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (May 9, 2019).

The FinCEN guidance on virtual currency conflicts with United States Congress' monopoly power to maintain all currency systems. (Source: https://constitution.congress.gov/browse/essay/artI-S8-C5-1/ALDE_00001066/) Congress's coinage power, without any doubt, is exclusive and it restrains the circulation of any currency (or currency systems) not issued under its own authority. Despite this, United States Treasury and FinCEN, with their flawed guidance have defined virtual currency as legitimate a medium of exchange, and have "de facto" authorized the transmission of "pirate currency" within United States borders.

There are, in fact, only three real ways to "regulate crypto" (1) full ban on "mining" in support of decentralized proof-of-work cryptocurrency ledgers (ex. Bitcoin network) (2) full ban on centralized proof-of-stake "pirate currency" systems (ex. Ripple) and (3) full ban on exchange of any currency to be circulated nationally not issued under the United States Congress' authority. Congress may only regulate currency that it itself authorized. If the currency is not authorized by the Congress, the Congress has zero power over it - that same way any government that authorizes national currency, has absolutely zero power over a currency in another country.

If the United States government fails to adopt all three of these elements, and, instead, chooses to legalize the act of conception, creation, maintenance, and exchange of private "virtual currency" systems as medium of exchange that is neither issued nor guaranteed by any jurisdiction within our borders, it will, in effect, authorize private persons and organizations to print money out of thin air.

"I give you warning; don't blame me if you make an injudicious choice." - Alexander Hamilton (Source: https://litesand.com/2021/01/07/bitcoin-the-pirate-currency/)

--
Dmitry Shkipin
Development and Operations at homeopenly.com
[redacted] | [redacted]
homeopenly™

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Horizen Labs

RESPONSE TO REQUEST FOR INFORMATION
DIGITAL ASSETS RESEARCH AND DEVELOPMENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY

FILING FROM: HORIZEN LABS
RESPONDENT TYPE: INDUSTRY
NOTICE ID 88 FR 5043
3 MARCH 2023

Horizen Labs is pleased to respond to this Request for Information to support the US government's research and development related to digital assets and distributed ledger technology.

Founded in 2019 by an Air Force veteran, Horizen Labs leverages zero-knowledge cryptography to ensure data privacy within a secure decentralized network. Our platform empowers developers, enterprises, and government agencies to create scalable blockchain applications that expand global access, increase economic opportunities, and promote greater freedom. Horizen Labs addresses a large gap in the blockchain industry by providing building tools that create blockchain solutions for real-world usage while ensuring information integrity and data confidentiality.

Zero Knowledge Proofs are our core competency and give us a competitive advantage. Horizen Labs was created by the same team that developed the Horizen public blockchain and its native cryptocurrency, Zen. Horizen is a leading blockchain platform that uses Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) to facilitate permissionless horizontal blockchain scaling through a unique sidechain and cross-chain transfer protocol. zk-SNARKs is an advancement in cryptography that enables transactions to be fully encrypted (aka "shielded") on the blockchain. Shielded transactions can still be verified as valid transactions under the network's consensus rules.

This cryptographic technology is emerging and yet to be widely adopted, with very few firms in the blockchain industry that have a team of trained cryptographers. Horizen Labs sees the enormous potential of Zero-Knowledge cryptography in the government and defense industry and has invested significant resources in building a highly skilled (Ph.D. level) cryptographic team.

Horizen Lab's ecosystem is a broad collection of stakeholders, including the Zen Blockchain Foundation (ZBF), the Horizen Community Council (HCC), an open-source developer community organized into a curated and compensated Horizen Developer Environment (HDE), a free educational resource called Horizen Academy, various corporate and academic partners, miners, node operators, and end-users. The ecosystem is perpetually shifting as new stakeholders join and others grow their involvement.

---

1. Question 3 RFI - R&D that should be prioritized for digital assets:

Horizen Labs has uncovered use cases through our research and discovery that support protecting critical industry and government data using Zero Knowledge cryptography.

Space Object Tracking on Blockchain

Decentralized and tamper-proof space object databases can be updated in real-time by various stakeholders (Governments, Space Agencies, and Private Companies).

<u>Current Problem</u>

In the space sector, there exists a problem between industry and government with the sharing of data related to space objects. Different organizations and countries use different space object databases, which are often out of sync, and do not all track the same objects or the same parameters for objects. This problem complicates coordination between organizations, especially as space is becoming proliferated with orbital debris.

The current systems struggle to keep up with the increase of tracked space objects and maintain up-to-date information, threatening the US security of assets in space. Furthermore, as the systems that track space objects age, problems arise due to security. Centralized systems are vulnerable to cyber attacks, which can cause major disruptions. Aging systems can also pose the risk of malfunctioning.

<u>Recommended R&D focus area</u>

A solution that merits further research and development and government interest is how space object digital assets can be tracked and secured in data transmission with blockchain. An example of an approach is in developing dedicated sidechains to replace or complement a space object database to track changes in their parameters. Parameters include object type, NORAD ID, Orbital Parameters, Launch date/site, and more. With zero-knowledge proofs, the system will enable privacy for all data, ensuring that only authorized individuals or entities can access it.

Early Threat Validation System on Blockchain

Decentralized network of early detection sensor data, such as missile warning systems. Blockchains' inherent data authentication/verification processes and extensive safety features provide additional security for such a delicate network.

Current Problem

False Alarms - Current systems may generate false alarms due to technical errors, erroneous sensor data, or misinterpretation of data, which leads to unnecessary panic and wasted resources.

Single Point of Failure - Centralized systems are vulnerable to spoofs, hacks, and other cyber threats, which can in turn trigger false alarms or even worse, real responses to a fake threat.

Lack of Interoperability - Countries use different systems and communication protocols, which can result in inefficiencies while sharing information or coordinating responses.

Recommended R&D focus area

Blockchain R&D can focus on an on-chain network of data from radar sensors all over the globe to detect ballistic missile launches and other threats and to ensure the validity of sensor data by cross-checking it through different nodes.

Part Certification/Documentation Tracking

Horizen Labs has uncovered numerous use cases with large suppliers in the aerospace, automotive, and defense industries that use different systems to track parts and part documentation. A problem exists in the handoffs between vendor/company teams that lead to errors and subsequently, costly delays in industrial/government programs.

Furthermore, tracking state changes, such as documentation revision of supply parts, edits, and changes, currently require manual processes and signatures which can introduce delays and are generally inefficient. The process of finding information on tracking a supply part and its availability, and status in a logistical system is confusing and adds time to a supply chain.

Recommended R&D focus area

Dedicated blockchains (side chains) and custom smart contracts that enable state change visibility for consolidating part tracking and traceability. Every certification or failure of a part through its delivery, acceptance testing, and assembly is recorded in the blockchain and provides instant visibility of a state change. With the use of zero-knowledge proofs, the system will enable privacy for all data, ensuring that only authorized individuals or entities have access to it, while at the same time leveraging blockchain's inherent immutability to maintain the system as a "single source of truth" across stakeholders.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

HSBC

HSBC

March 3, 2023

Via electronic mail to [*DARD-FTAC-RFI@nitrd.gov*](mailto:DARD-FTAC-RFI@nitrd.gov)

Rachel Wallace, Deputy General Counsel
Office of Science and Technology Policy
The White House

Dear Ms. Wallace:

HSBC appreciates the opportunity to provide feedback on the White House Office of Science and Technology Policy's request for information (RFI) on priorities for research and development related to digital assets.

HSBC, headquartered in London, is the second largest foreign bank operating in the US and is the world's leading trade bank. HSBC serves customers worldwide from offices in 62 countries and territories in its geographical regions: Europe, Asia, North America, Latin America, and Middle East and North Africa. With assets of US$2,967bn as of December 31, 2022, HSBC is one of the world's largest banking and financial services organizations.

HSBC supports responsible financial innovation, conducted in a manner consistent with existing regulations, consumer and investor protections, and the promotion of the safety and soundness of the financial system. The burgeoning digital assets ecosystem is a growing segment of the financial sector and one that warrants thoughtful research. We, therefore, appreciate the opportunity to detail HSBC's initiatives regarding digital assets, and areas of research we think would be beneficial.

At the outset, we would encourage policymakers to adopt a common lexicon with respect to digital assets, and to distinguish among digital assets, including cryptocurrencies, tokenized assets, and the underlying technology providing the infrastructure (e.g., distributed ledger technology) when taking action in this area. These digital asset categories carry significantly varying degrees of risk and volatility, and as such, should be treated by policymakers in a manner consistent with their nature. For example, the risk presented by un-backed cryptocurrencies is much different than traditional banking organization using DLT or the tokenization of traditional assets by incumbent financial firms subject to prudential and markets regulations.

Provided below are observations to selected questions posed in the RFI. Where the RFI seeks information related to the development of central bank digital currencies (CBDCs), we would encourage OSTP to reference HSBC's response to the Federal Reserve Board's request for comment in response to its publication of discussion paper entitled, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*.[1]

1. *Goals, sectors or applications that could be improved with digital assets and related technologies:* Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefit are already being delivered. This includes explanations of the current limitation in how those goals, sectors, and applications are currently advanced with limited use of digital assets and related technologies, and how increased or better use of digital assets could provide a specific advantage over existing approaches in advancing these objectives. Where relevant, respondents are encouraged to justify how digital assets provide unique value to advancing that goal, sector or applications compared to the use of traditional databases or other technologies (e.g., as outlined in the *National Institute of Standards and Technology Internal Report 8202,* Figure 6).

HSBC is developing, testing and deploying new technologies in an effort to provide efficiencies for the bank and its customers. While involvement with certain speculative digital assets, such as cryptocurrencies, is currently outside HSBC's risk appetite, we are exploring the wider digital asset ecosystem to achieve these efficiencies. These efforts include, but are not limited to, pioneering one of the first tokenized bond platforms and advising central banks globally on their development of CBDCs.

HSBC sees value in asset tokenization, which can simplify and accelerate transfer of assets in capital markets. To this end, HSBC launched its own proprietary tokenization platform called *HSBC Orion* in 2022. Assets on *Orion* are "natively on chain," which means they live solely on our own blockchain in a fully approved and regulated platform, which HSBC built and owns.

Orion's technology is self-developed by HSBC and aligned with the required legal approach in Luxembourg, the launch regulatory jurisdiction. HSBC launched *Orion* in Luxembourg due to the favorable legal climate that allows such financial innovation. Specifically, Luxembourg law allows token transfer to be aligned with legal asset transfer if a platform is awarded the status of "Central Account Keeper." *Orion* is the first platform to be awarded such status. Luxembourg law has a comprehensive and dedicated approach to digital assets. Among other things, Luxembourg law provides for the same legal recognition for tokenized securities as traditional financial instruments, is technologically neutral regarding the characterization of securities, and includes a framework that means that fungible securities may be transferred entirely on a DLT environment when they are kept in securities accounts.

[1] Available at https://www.federalreserve.gov/files/cbdc-public-comments-8-20220624.pdf, pp. 565-571.

Other jurisdictions (e.g., the European Union overall, and United Kingdom) are actively seeking to introduce a similar model to Luxembourg's approach to digital asset innovation. HSBC would like to conduct similar activities in the US, given its prominence as the largest and most liquid capital market. However, certain legal and regulatory hurdles/uncertainties would prevent such an expansion. Further details are provided in the answer to Question 4, outlining potential jurisdictional competitiveness concerns.

The process of tokenizing assets, such as under HSBC's *Orion* platform, may create significant efficiencies in affected markets, and we encourage the Administration to investigate ways to reduce barriers to this activity in the US.

4. *R&D that should be prioritized for digital assets*: Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and the U.S. national interests from risks or harms that digital assets might present. This includes topics for technical research, topics for research in the social sciences and across disciplinary boundaries, and opportunities for hardware and software development. This also includes information about emerging areas that could enable new opportunities to leverage digital assets, as well as information about technical limitation of digital assets and the associated business models and governance arrangements they often rely upon. Respondents are encouraged to, where relevant, describe how the discussed R&D topic could be useful in helping a potential U.S. CBDC system align with the *Policy Objectives for a U.S. CBDC System.* Respondents are also encouraged to share how discussed R&D topic could help advance U.S. competitiveness and leadership in the world.

As mentioned above, HSBC developed an innovative bond tokenization platform called *Orion*, launched in Luxembourg. HSBC chose Luxembourg due to a legal environment that aligned with the goals, objectives and sought-after outcomes of the program. For the purposes of this question, HSBC would encourage the Administration to research (a) the legal environment in other jurisdictions, including proposed or pending legislation, related to the responsible development of digital asset strategies, and (b) potential hindrances in existing US law to the development and deployment of tokenization platforms. Ultimately, HSBC would welcome the opportunity to launch *Orion* or a similar platform in the US. We view other jurisdictions' comparatively accommodative legal frameworks or developments in digital asset legislation as a potential competitive disadvantage for innovation in the US.

Other jurisdictions are exploring avenues to encourage the responsible development of tokenization and other digital assets activities. For example, the EU differentiates between crypto-assets already governed by EU legislation, and other crypto-assets. The former (e.g., bonds, shares) will remain subject to existing legislation, but the European Parliament has approved a pilot regime for market infrastructures for trading and settlement of transactions in financial instruments in crypto-asset form. This EU Pilot Regime – part of the EU Digital Finance Package, allows market participants and regulators to gain experience with the use of DLTs exchanges that would trade or record shares or bonds on the digital ledger and facilitate testing the benefits of this new technology.

The EU pilot regime will allow regulated institutions to develop and test DLT-based infrastructure for issuing, trading, and settlement of financial instruments (i.e., security tokens). Security tokens are digital assets, similar in nature to traditional securities under EU legislations, issued using blockchain technology (n.b., *not* cryptocurrencies).

The United Kingdom is developing legislation with proposed powers to set up a "sandbox" using secondary legislation for the use of DLT. The framework for the bill allows to make permanent changes to the UK legislative framework based on what is learned from the sandbox. The sandbox will cover trading venues (trading) and central securities depositories (CSDs -issuance, settlement and maintenance). The central use-case would be participants being able to combine the functions of both a CSD and trading venue together, though participating firms could potentially choose not to do this. The UK sandbox is focused on enabling the legislation governing traditional finance to evolve and does not incorporate cryptocurrencies into the scope.

We encourage the Administration to research how existing and developing laws in other jurisdictions may create a competitive disadvantage for the US, including by incentivizing financial firms to launch innovative platforms in those jurisdictions rather than the US.

In addition to reviewing actions by other jurisdictions, we encourage the Administration to review potential hurdles to innovation in the US legal framework, specifically with regard to asset tokenization. This includes specific guidance from prudential regulators about digital asset activities; issues relating to clearing agency involvement, cross-border issues; clarity about property rights of customers who hold digital assets through exchanges; and commercial law foundation for direct issuance of securities on DLT.

Please direct any questions to Dan Taylor, Senior Vice President of Federal Government Relations, HSBC North America [redacted] HSBC thanks you for the opportunity to provide feedback to this RFI.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Independent Community Bankers of America ("ICBA")

INDEPENDENT COMMUNITY BANKERS *of* AMERICA®

March 3, 2023

Via Electronic Submission

Rachel Wallace
Deputy General Counsel and Chief Operating Officer
Office of Science and Technology Policy
Executive Office of the President
[redacted]

RE: Request for Information – "Digital Assets Research and Development" (88 FR 5043)

Dear Ms. Wallace:

The Independent Community Bankers of America ("ICBA")[1] welcomes the opportunity to provide feedback on the Office of Science and Technology Policy's ("OSTP") Request for Information ("Request") as it seeks to create a National Digital Assets Research and Development Agenda.[2]

ICBA and its members welcome the OSTP's engagement with community banks to understand how academic and government research efforts can help policymakers assess the potential impacts and risks from digital assets. Community banks support responsible innovation in financial services as they develop new ways to serve their customers and provide technologies and experiences that support the 21st century economy. While advocates for digital assets argue entities outside the regulatory perimeter can increase speed, efficiency, and transparency in financial services for consumers and businesses, the reality does not yet seem to match the rhetoric. Last year alone, multiple cryptocurrency lenders and exchanges failed, leaving users unable to access their assets as bankruptcy courts must now grapple with these complex cases.

---

[1] *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services. With nearly 50,000 locations nationwide, community banks constitute roughly 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding nearly $5.9 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at* www.icba.org.

[2] Office of Science and Technology Policy, Notice of Request for Information, "Request for Information; Digital Assets Research and Development," *Federal Register* 88, no. 17 (January 26, 2023): 5043, https://www.govinfo.gov/content/pkg/FR-2023-01-26/pdf/2023-01534.pdf.

Additionally, the use of cryptocurrency by bad actors soared to new heights in 2022, with North Korean-affiliated hackers stealing over $1 billion in cryptoassets and DeFi protocols suffering losses exceeding $3 billion.[3] ICBA is alarmed that criminals and bad actors are, with relative ease, increasingly using cryptocurrencies to facilitate ransomware, money laundering, sanctions evasion, and other criminal activities.

ICBA also has serious concerns about the potential for disintermediation of traditional financial services by stablecoins and decentralized finance ("DeFi") - a result which will negatively impact community banks and disrupt the nation's regulated financial system. Prudential regulators have expressed similar concerns. For example, Marty Gruenberg, Chair of the Federal Deposit Insurance Corporation ("FDIC"), warned last October that nonbank stablecoins may disintermediate community banks, and he emphasized that threat "is an issue that should also be carefully explored and considered."[4] Acting Comptroller of the Currency Michael Hsu has also warned that a lack of interoperability within a stablecoin operating on multiple blockchains and a lack of interoperability across different stablecoins will lead to a highly fragmented payment system reminiscent of Pre-Civil War banking.[5]

As the government considers how to develop its agenda for digital assets, ICBA and its members call on the OSTP to prioritize research on the current and potential impacts from digital assets on community banks and the populations they serve. Community banks are the bedrock for the nation's financial system and economy. If community banks become disintermediated by a digital dollar or other digital assets, the consequences could be devasting to the banking system and the ability for Americans to access financial services. Moreover, given the outsized role that community banks play in providing financial services to small and rural communities, the potential disruptions by digital assets could have far-reaching economic and social costs. These potential consequences deserve significant attention by the OSTP and the research community to understand how the proliferation of digital assets and supervisory frameworks applied to or excluding digital assets may exacerbate an already uneven playing field between well-regulated community banks and entities that, by design and intent, prefer to be less regulated or unregulated.

---

[3] White House, National Economic Council, "The Administration's Roadmap to Mitigate Cryptocurrencies' Risks," by Brian Deese, Arati Prabhakar, and Jake Sullivan (January 27, 2023), https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/; Josh Smith, Reuters, "Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups – report" (February 6, 2023), https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01/.

[4] Federal Deposit Insurance Corporation, FDIC Chairman Martin J. Gruenberg, "Remarks by FDIC Acting Chairman Martin J. Gruenberg at the Brookings Institution on the Prudential Regulation of Crypto-Assets," October 20, 2022, https://www.fdic.gov/news/speeches/2022/spoct2022.html.

[5] Office of the Comptroller of the Currency, Acting Comptroller of the Currency Michael J. Hsu, Remarks Before the Institute of International Economic Law at Georgetown University Law Center, "Thoughts on Stablecoin Architecture," April 8, 2022, https://www.occ.treas.gov/news-issuances/speeches/2022/pub-speech-2022-37.pdf/.

Executive Summary

Turbulence in the crypto markets last year, especially the catastrophic failure of the algorithmic stablecoin TerraUSD and the sudden collapse of FTX, are evidence of the risks presented by digital assets, including scams, misrepresentations to consumers, and a growing potential for these digital assets to contaminate the financial stability of the traditional banking sector. As explained in more detail below, ICBA's position on digital assets can be summarized by the following principles:

1. Community bankers are opposed to the United States issuing a digital dollar or Central Bank Digital Currency ("CBDC"). The risks far outweigh the uncertain and unproven benefits cited by CBDC advocates. A CBDC threatens to disintermediate community banks, thus raising the risk of serious economic consequences. It is imperative that the federal government conduct thorough research into the potential for CBDC to disintermediate community banks and negatively impact the communities they serve.

2. Nonbank stablecoins, especially global stablecoins, also pose risks to community banks and their customers. These specific risks have not been fully explored in academic or government research; therefore, ICBA and its members urge the OSTP to support research efforts on the specific impacts that community banks may face if stablecoins become widely adopted for payments and contribute to the growth of decentralized financial services.

3. Digital assets present numerous significant threats, including financial crimes and risks to financial stability. Illicit activities fueled by cryptoassets, like ransomware, have affected community bank customers. ICBA and its members encourage the OSTP to prioritize research efforts to understand how bad actors use cryptoassets and to develop strategies or technologies to mitigate these risks.

Additionally, we encourage the OSTP to incorporate the following recommendations as it develops a National Digital Assets Research and Development Agenda:

- Conduct research to assess the full range of potential economic and social consequences that could result from a digital dollar disintermediating community banks.

- Focus research on the specific impacts to community banks and their communities if nonbank stablecoins continue to become more widely used for payments and support the expansion of decentralized finance ("DeFi").

- Perform additional research on blockchain technology, as well as other potential regulatory or legal solutions that could help mitigate the myriad threats of ransomware, sanctions evasions, and other financial crimes facilitated by digital assets.

Since bitcoin launched in 2009, the digital assets economy has exploded in growth - there are currently more than 20,000 different types of cryptoassets traded across hundreds of centralized and decentralized exchanges. The value of the crypto economy surged in 2021, reaching an all-time high of $3 trillion in total value, before it crashed in 2022 following a series of significant failures of crypto lenders, stablecoins, and other crypto projects. The impact of this precipitous downfall cannot be emphasized enough—investors lost hundreds of millions of dollars' worth of uninsured assets, and it is unlikely many will ever recover their accounts. Additionally troublesome is the fact that crypto-assets are widely used and leveraged by hackers and, as such, can be used to inflict real harm to American communities. The Colonial Pipeline cyberattack in 2021 that disabled critical infrastructure and triggered severe gas shortages on the east coast serves as a stark warning about the dangers presented by ransomware.[6]

ICBA Comments

Goals, sectors, or applications that could be improved with digital assets and related technologies

Advocates of digital assets have claimed that blockchain has the potential to revolutionize payments and bring financial services to un/underbanked Americans. However, that potential has not yet been realized and it remains uncertain whether the technology will ever meet that potential.

By contrast, other traditional technologies, such as real-time gross settlement systems, have a well-established track record of enhancing financial services and supporting innovation. ICBA recognizes there is a real need for faster payment capabilities, and we strongly support the development and implementation of FedNow, the new instant payment system created by the Federal Reserve that will launch later this year. As noted by Federal Reserve Governor Miki Bowman last year, "FedNow addresses the issues that some have raised about the need for a CBDC."[7] To that end, we implore the OSTP to leverage years-long government research and investments in FedNow by ensuring the OSTP's agenda is focused on understanding how instant payments facilitated by the Federal Reserve can address many of the issues that digital assets advocates now claim only a central bank digital currency can solve.

The vast potential of FedNow, a carefully developed and implemented platform, to improve payments for Americans should not be left to wither on the vine in favor of a central bank digital currency, a concept that is in nascent stages of understanding. Instead, the OSTP should take this

[6] Joe Carroll, Andres Guerra Luz, and Jill R. Shah, *Bloomberg*, "Gas Stations Run Dry as Pipeline Races to Recover From Hacking" (May 8, 2021), https://www.bloomberg.com/news/articles/2021-05-09/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline.
[7] Michelle Bowman, Federal Reserve Board of Governors, "Technology, Innovation, and Financial Services," Remarks at the VenCent Fintech Conference, Little Rock, Arkansas, August 17, 2022, https://www.federalreserve.gov/newsevents/speech/bowman20220817a.htm.

opportunity to consider how instant payment systems like FedNow can evolve to support additional needs in the future, particularly with respect to cross-border payments. In 2020, the G20 endorsed a plan to improve cross-border payments by finding ways to lower costs and increase transparency, and the Financial Stability Board ("FSB") now serves as the lead coordinator for these efforts.[8] The OSTP should consider how additional research into the challenges of cross-border payments can complement the FSB's ongoing work. For example, the OSTP could partner with the prudential regulators on research into specific technological, operational, or regulatory hurdles with which community banks must contend to offer cross-border payments to their customers. Finding solutions to these issues could allow community banks to provide enhanced payment services to their customers, meet a growing demand for faster and more efficient remittance payments, and support international commerce.

Goals, sectors, or applications where digital assets introduces risks or harms

<u>Central Bank Digital Currency ("CBDC")</u>

Community banks act as the nation's financial bedrock, with more than 4000 chartered banks serving towns and cities across the country. Community banks represent approximately 99% of all banks in the United States, and more significantly, provide a critical lifeline to underserved and rural communities. In fact, there are 2,276 community banks located in 1400 counties with populations under 50,000.[9] In other words, there are approximately 1.6 banks in the counties with fewer than 50,000 people, meaning that community banks are the only provider of financial services for millions of Americans.[10]

The facts stated above serve as vital context for our concerns about the potential for a CBDC to disintermediate community banks and inflict tremendous economic harm. That is why ICBA and its members believe understanding the wide-ranging consequences of a CBDC is of the upmost importance. ICBA and community bankers remain adamantly opposed to a CBDC because banks will be unable to lend against customer deposits stored as CBDC, thus disrupting community banks' ability to meet their credit needs of their community needs. These are serious concerns that merit extensive and dedicated government and academic research.

Therefore, ICBA strongly encourages the OSTP to research the specific risks that a digital dollar can pose to community banks and consumers. For example, the OSTP could sponsor research to consider what may happen to credit creation and small business development if a U.S. CBDC leads to significant declines in deposits at community banks. This question is vitally important and must be thoroughly examined before any decision is made to launch a CBDC. Main street still matters in the 21st century, and we implore the OSTP to carefully analyze the potential for a

[8] Financial Stability Board, "G20 Roadmap for Enhancing Cross-border Payments: Consolidated progress report for 2022," (October 10, 2022), https://www.fsb.org/wp-content/uploads/P101022-1.pdf.
[9] *Banking Strategist*, "Community Banks: Number by State and Asset Size," https://www.bankingstrategist.com/community-banks-number-by-state-and-asset-size.
[10] Ibid.

CBDC to disintermediate community banks and leave a trail of significant economic and social consequences in its wake.

Stablecoins

Unfortunately, few studies have investigated the specific repercussions for the community banks and the customers they serve. Therefore, ICBA and its members encourage the OSTP to consider research opportunities that will examine such consequences.

As one example, the OSTP could research how community banks may be affected by the rise of one or more global stablecoins and analyze the numerous impacts that could result from banks losing deposits to stablecoins. The OSTP could also sponsor more research into the financial stability threats posed by stablecoins, such as the possibility of a global stablecoin rapidly collapsing due to a cyberattack, a loss of user confidence, or other catastrophic event.

Cryptocurrencies and Crypto Entities

ICBA has repeatedly warned regulators and lawmakers about the risks of cryptocurrencies, and unfortunately many of those concerns were realized last year. Following a series of high-profile collapses of algorithmic stablecoins, cryptocurrency lenders, and cryptocurrency exchanges, millions of users remain unable to access their accounts or with assets that quickly plummeted in values. Some of these entities even falsely claimed to protect user assets with deposit insurance through the FDIC.[11] The impacts of these failures and misrepresentations continue to affect consumers today. ICBA and its members support research not only on the impacts of cryptocurrencies, but also on the ways in which volatility in the crypto markets may spill over onto Main Street and threaten the financial system.

ICBA and its members urge the OSTP to support ongoing research into the potential for DeFi to pose risks to consumers, the financial system, and U.S. national security. The risks of DeFi have been the recent focus of numerous regulatory bodies and organizations, including the Federal Reserve and the Bank for International Settlements.[12] However, there remain more opportunities to analyze the interconnectedness in DeFi and learn how it can spread volatility throughout the crypto ecosystem and possibly the traditional financial system.

[11] Federal Deposit Insurance Corporation, Financial Institution Letter, FIL-35-2022, "Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies," July 29, 2022, https://www.fdic.gov/news/financial-institution-letters/2022/fil22035.html.

[12] Federal Reserve Bank of Atlanta Policy Hub, Center for Financial Innovation and Stability, "Decentralized Finance (DeFi): Transformative Potential and Associated Risks," by Francesca Carapella, Edward Dumas, Jacob Gerszten, Nathan Swem, and Larry D. Wall, No. 14-2022, October 2022, https://www.atlantafed.org/research/publications/policy-hub/2022/10/18/14--decentralized-finance-defi--transformative-potential-and-associated-risks; Bank for International Settlements, Monetary and Economic Department, "Cryptocurrencies and Decentralized Finance," BIS Working Papers, No. 1061, by Igor Makarov and Antoinette Schoar, December 2022, https://www.bis.org/publ/work1061.htm.

Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

In addition to research efforts focused on the financial stability risks presented by CBDC and stablecoins, the OSTP should also support more research on digital assets and financial crimes. Ransomware, sanctions evasion, and many other illicit activities now involve payments in cryptocurrencies. While the government took significant steps last year to curtail the use of Tornado Cash, a mixer notorious for aiding North Korean hackers, there are still many threats posed by crypto mixers and anonymity-enhanced cryptocurrencies, such as Monero.[13] We encourage the OSTP to support research into technical, legal, and regulatory solutions to help private industry, law enforcement, national security organizations, and other government agencies address the rising threat of crypto crime.

Opportunities to advance responsible innovation in the broader digital assets ecosystem

ICBA and its members support responsible innovation in financial services; however, digital assets are neither the only source of innovation nor the only solution to deliver faster payments. Community banks, through decades of innovation and coordination with federal regulators, have made great strides towards expanding banking services to the un/underbanked. In fact, according to the latest FDIC survey, approximately 96% of all American households have access to a bank account.[14] This milestone was accomplished not through a CBDC or stablecoin, but rather from the persistent and responsible efforts of community banks to find new ways to meet the demands of their customers and communities.

As new systems like FedNow come online, community banks will have even more opportunities to leverage new technologies to develop and implement innovative solutions to meet the needs of the 21st century economy. To that end, we again encourage the OSTP to widen its research focus to consider how other technologies, particularly instant payment systems, can advance responsible innovation in financial services.

Conclusion

ICBA appreciates the opportunity to comment on the unique ways digital assets initiatives may impact community banks. Any National Digital Assets Research and Development Agenda must support efforts to protect the nation's financial system from unsound risks and criminal activity and recognize the vital role that community banks have in supporting communities, consumers, and small businesses across America.

---

[13] United States Department of the Treasury, Press Release, "U.S. Sanctions Notorious Virtual Currency Mixer Tornado Cash," (August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.
[14] Federal Deposit Insurance Corporation, "2021 FDIC National Survey of Unbanked and Underbanked Households" (November 14, 2022), https://www fdic.gov/analysis/household-survey/index.html.

We look forward to working with the OSTP and with the Administration as it considers the future of digital assets and develops policies that will enable community banks and their customers to benefit from advances in financial technology without sacrificing the health of the broader economy.

If you have questions or require additional information about ICBA's statements, please contact me at [redacted] or by email at [redacted]

Sincerely,

/s/

Brian Laverdure, AAP
Vice President, Payments and Technology Policy

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Inca Digital Federal

INCA
DIGITAL
FEDERAL

Industry Member
Veteran-Owned Small Business
DARPA SBIR Phase II Awardee
Dual-Use Technology Provider

Inca's Response to White House OSTP Call for Comment

AUTHORS:

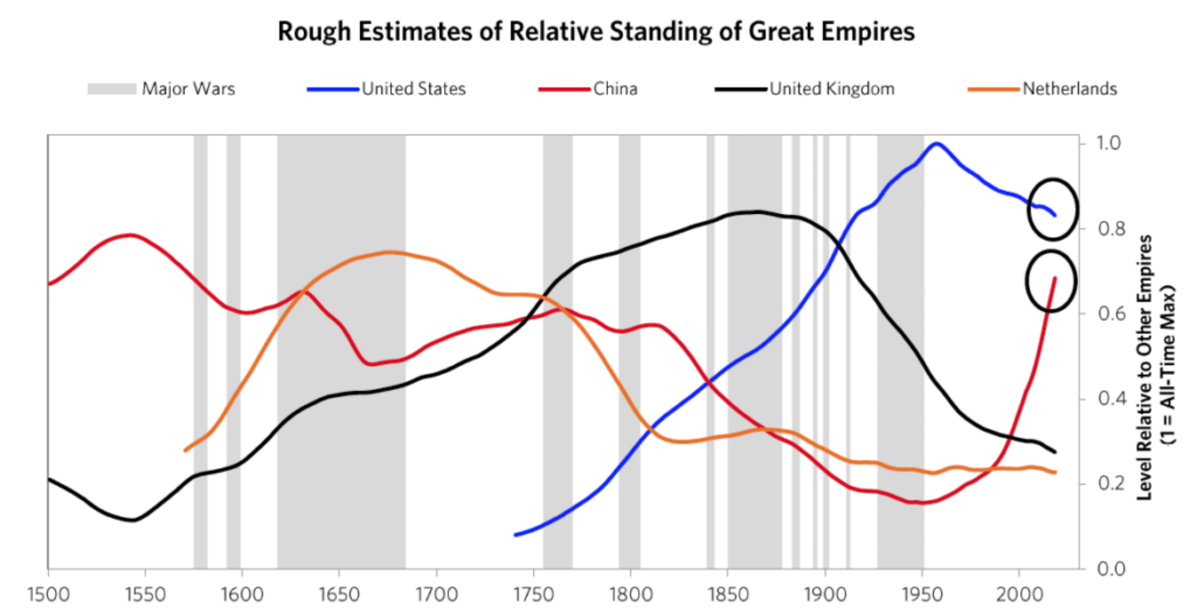
Anita Nikolich
Cameron Smith
Jules Hirschkorn
Eric O'Connor

Topic 1

Responsible innovation in digital assets could provide significant benefits for the American people. Digital assets are enabling new ways to move value through the online world, and their underlying technology is facilitating change across industries. In the private sector, companies are using DLT to synchronize databases with limited trust, enable new types of record keeping, build new infrastructures for managing digital identity, and provide novel financial services to consumers. In the public sector, the United States is exploring whether a CBDC could provide a trustworthy infrastructure to facilitate transactions in a highly digitized world. While the United States explores these potentials, countries such as China, Russia, and Venezuela have begun developing and implementing CBDCs, India just announced reaching a milestone of 50,000 users for the Digital Rupee (e₹) or eINR or E-Rupee. Across the board, applications of digital assets are benefitting from advances in foundational and translational research, spanning topics from cryptography to the social, behavioral, and economic sciences.

Topic 2

Rapidly rising geopolitical competition is challenging the most foundational aspects of existing global power structures. In particular, the rise in adoption of cryptocurrencies presents some unique challenges. Emerging great powers, such as Russia and China, are actively using cryptocurrency and digital asset infrastructure to subvert and exploit financial relationships in such a way that directly threatens the stability of existing financial paradigms and America's longstanding geopolitical relationships. Understanding the emerging cryptocurrency ecosystem at a granular level is a national security imperative as a means to counter Russian and Chinese economic warfare. Inca Digital has multiple ongoing efforts in data analytics to assist in this effort, including a project with the Defense Advanced Research Projects Agency. However, research and development (R&D) in this space has often been conducted in a fragmented manner, with limited consideration for the broader implications, applications, and downside risks for the underlying innovations. This is particularly concerning because there are many examples of how digital assets introduce new national security threat vectors.



Source: Ray Dalio - The Changing World Order

Since the introduction of the Bretton Woods system in 1944, the United States has been the global reserve currency. Bretton Woods required countries to guarantee convertibility of their currencies into U.S. dollars to within 1% of fixed parity rates, with the dollar convertible to gold bullion for foreign governments and central banks. This provided the basis of modern American economic power, with diminishing returns to our military superiority. In recent years, authoritarian regimes and those who disagree with the policies of advanced economies have endeavored to undermine this global order which has built unprecedented prosperity, lifting millions if not billions out of extreme poverty. Countries such as China and Russia look to create their own vision of a global world order which puts the needs of individuals on the back burner for the prosperity of the collective few. Inca Digital sits in a unique position in industry, as a veteran owned small business, bringing years of service and dedication to protecting the interests of the United States and its allies. The introduction of cryptocurrencies and digital assets has created a new vector of threat for these adversaries. Looking forward to the digitization of the economy, the underlying layer will be the movement of information and value. If we do not lay the proper groundwork, as we did, to industrialize the United States, the economic position we currently maintain will continue to erode from under us.

Topic 3

Two critical components of any national strategy with respect to digital assets are (a) developing an ability to identify material developments within the digital asset landscape, and (b) fostering innovation and development in the United States.

First, by analogy, traditional equity markets have established markets and indices that allow regulators and policymakers to monitor the most relevant activity. The New York Stock Exchange, The NASDAQ Stock Market, the London Stock Exchange, the Tokyo Stock Exchange among others are known entities with historically known trading and price attributes. Anomalies in trading volumes and money flows emanating from those markets can be easily monitored and identified. This is also true for global futures markets, as well as global currency and sovereign debt markets. Eurodollars, Bunds, Yen, and Yuan all trade on markets with closely tracked histories. While explanations often elude policymakers, anomalous trading or money movements are nearly always noticed as there are familiar historical patterns and relationships that are monitored by thousands of market participants.

In contrast, digital assets are traded globally on thousands of markets, few of which have anything near traditional market surveillance. The rapid introduction of products coupled with the potential for trading volumes in various assets to rapidly migrate to either new assets or exchanges makes this difficult. Further, most academics and researchers have not yet dedicated the time to the study of digital assets, inhibiting their ability to intellectually organize the various assets and trading venues within the space. As a result, agreed upon relevant metrics that would flag material changes in market dynamics are yet to be developed. Changes in money flows geographically or among assets are not readily identified because policymakers lack a "mental model" or map of the current landscape.

Second, digital assets also present an opportunity for national security. They can reduce the wealth gap by cutting global transaction costs. They allow people, globally and regardless of socioeconomic status, control over their own money. They can transform international aid and development, foster trade and drive a new sector of small businesses in the U.S. Digital Assets can reduce fraud and inflationary instability in global markets. Fostering digital asset innovation will increase U.S. competitiveness globally, and reduce the risk that closed systems - such as China's CBDC - take hold around the world.

Topic 4

The Federal Government should help ensure that the potential of digital assets is realized in sectors where it provides value, while taking steps to ensure that this realization is achieved with the appropriate guardrails. To ensure the continued leadership of America and to ensure responsible innovation is achieved - a clear understanding and proactive mitigation of the downside risks associated with increasing adoption of digital assets needs to be formed.

From Inca Digital's perspective, a key component to advancing the development of digital assets while also protecting communities and U.S. national interests from risks and harms that digital assets might present is effective market surveillance and risk management - via data analytics. While much is made of blockchain forensics from companies such as Chainalysis, there are many other data sets that are equally important to understanding what is happening in the digital asset ecosystem. This is not to disparage blockchain forensics at all. However, other datasets in the ecosystem are equally important: to include orderbook data, data from open source repositories such as GitHub, and data from social media. More should be done to foster not just crypto-native companies, but also companies that provide data analytics to ensure stable, effective, and fair markets.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Input Output Global, Inc. (IOG)

March 3, 2023

Office of Science and Technology Policy (OSTP)
Eisenhower Executive Office Building
[redacted]

Re: Comments on Digital Asset Research and Development

To Whom it May Concern at the OSTP,

On behalf of the government relations and policy team at Input Output Global, Inc. (IOG),[1] we would like to thank the OSTP on behalf of the Fast Track Action Committee (FTAC) on Digital Assets Research and Development of the Subcommittee on Networking and Information Technology Research and Development (NITRD) of the National Science and Technology Council, the National Science Foundation, and the NITRD National Coordination Office for the opportunity to provide comments to help identify priorities for research and development related to digital assets, including various underlying technologies such as blockchain, distributed ledgers, decentralized finance, smart contracts, and related issues such as cybersecurity and privacy (e.g., cryptographic foundations and quantum resistance), programmability, and sustainability as they relate to digital assets.

Below, please find our responses to some of the topics and questions posed by your office in the Request for Information Notice:

1. Goals, sectors, or applications that could be improved with digital assets and related technologies: Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered. This includes explanations of the current limitations in how those goals, sectors, and applications are currently advanced with limited use of digital assets and related technologies, and how increased or better use of digital assets could provide a specific advantage over existing approaches in advancing these objectives. Where relevant, respondents are encouraged to justify how digital assets provide unique value for advancing that goal, sector, or application compared to the use of traditional databases or other technologies (e.g., as outlined in National Institute of Standards and Technology Internal Report 8202,Figure 6).

Identity and Verifiable Credentials

In April 2021, IOG partnered with the Ethiopian Ministry of Education to implement a national blockchain-based student and teacher ID and attainment recording system to digitally verify

[1]Input Output Global, Inc. (IOG) is a Wyoming incorporated software development company, pre-eminent in the research and engineering of blockchain technology. While best known for the development of the Cardano blockchain, the company has also created a self-sovereign identity software solution, self-hosted wallets, and web3 tools. More information about Input Output Global can be found here: https://iog.io/

grades, remotely monitor school performance, and boost education and employment nationwide. The use of a blockchain, like Cardano, will allow for accurate tracking of individual grades, behavior, attendance, and educational attainment across all kindergartens, elementary schools, and general secondary schools.

The project is leveraging IOG's self-sovereign identity software solution, Atala PRISM, which is built on Cardano and offers core infrastructure for issuing DIDs (decentralized identifiers) and verifiable credentials. Atala PRISM will enable authorities to create tamper-proof records of educational performance across 3,500 schools, 5 million students, and 750,000 teachers to pinpoint the locations and causes of educational under-achievement and allocate educational resources effectively. This will provide all students with blockchain-verified digital qualifications to reduce fraudulent university and job applications, and increase social mobility by allowing employers to verify all applicants' grades without third-party agencies.

The Ethiopian government is providing 5 million teachers and students with tablets and a dedicated internet network, giving all students instant access to their academic records. Student IDs will be paired with data from learning management systems and harnessed by machine learning algorithms to drive personalized tuition, a dynamic curriculum, and data-driven policies and funding. Lastly, students will receive cards with near field communication (NFC) chips that will contain their educational credentials, which means the data will be available even if a student doesn't have a mobile phone or other device to connect to the system. This will open up higher education and employment opportunities for the 80% of Ethiopia's population living in rural regions and those facing civil unrest.

Last year, Ethiopian education authorities chose nearly 2 dozen public schools and began rolling out digital IDs for students and teachers and over 100,000 IDs have been issued thus far. This project will improve the administrative process for students, teachers, and overseeing bodies for near seamless interactions, increase the trustworthiness of student academic credentials internally and across borders by reducing the risk of fraud, and enable data-driven policy-making.

Connecting the Unconnected

In November 2021, IOG partnered with World Mobile Group Ltd. to democratize access to digital services and provide remote internet infrastructure in Africa. World Mobile's mesh network model leveraging the Cardano blockchain enables scalable, shared infrastructure, security, transparency, and self-sovereignty. This can lower the costs and the practical barrier for people to access connectivity, financial services, and education. The sharing economy gives every participant of the network a mutual stake in its success. It is enabled by a decentralized network where participants are rewarded proportionately for their contributions to the network.

Traditional mobile operators deliver connectivity where it is profitable for them to offer their services at a large scale, and some collect and sell your browsing data. World Mobile aims to deliver a secure and private mobile network run by the people, for the people.

World Mobile's AirNodes are the access layer of the network and provide last-mile connectivity for the voice, text, and data services used by World Mobile customers and communicate with the rest of the network (EarthNodes and AetherNodes) using the Internode API. Essentially, they replace the traditional last-mile access run by mobile operators. Instead of a big telco tower, AirNodes are hybrid mesh devices run by anyone who wants to provide connectivity in their area. This translates to less expensive internet access at approximately 1/3 of major telco rates in the region.

World Mobile is currently serving over 3,000 customers across 5 pilot sites in Zanzibar. This year, World Mobile will expand to 30 sites, with each node serving up to 700 people, in Zanzibar and beyond to Kenya and Tanzania.

RealFi – Banking the Unbanked

Pricing credit is about trying to assess and mitigate the risk of defaulting. Traditional consumer finance and credit reduces risk by understanding how borrowers behave – how much they spend, their income, and so on. A mature credit scoring system is key to delivering credit in developed economies, but it is even more critical in emerging markets. The reason why banks refuse credit or loans in emerging markets is often that they don't have enough data about the person or organization intending to borrow. The systems are either less sophisticated or simply not there. It is impossible to create an accurate financial picture through a credit score.

However, it is possible to build up a credit score by querying proxies, linked to an identity. You could contact utility companies to check if the customer has always paid their bills, or check with a phone provider to see how often the prospective borrower topped up their mobile. An identity is out there, the problem is how to tie data to the identity. Once that is achieved, the data can be presented to a local bank, microfinance initiative – or a decentralized pool of capital provided by people across the world in a blockchain community.

We have now reached a point when we can enable this through innovations in crypto. All the necessary financial information can be stored and relayed in a verifiable manner through an Atala PRISM ID. The monetary building bricks of DeFi can be used to structure these loans and hedge the currency risk, while scalable payment rails provided by the Cardano blockchain and various layer 2 solutions will make it possible to transfer capital across the world without friction.

RealFi, real finance targeted at the people who really need new ways to access finance (creating that real value often missing from DeFi), is an ecosystem of products that remove the frictions between crypto liquidity and real world economic activities to offer access to cheaper and faster credit and financial products.

The Cardano blockchain adds the final piece of the financial puzzle by unlocking real economic value at the end of the transaction chain: personal identity. Identity is central to everything. Once someone has an economic identity, a world of opportunity and inclusivity opens up. Real opportunity comes with access to essential services that were hitherto out of reach, and real finance, such as loans to open a business or maintain an existing one. But access to finance is only part of a larger picture. Without access to insurance, education, and health services, people would still be exposed to huge risks. RealFi, through the power of blockchain and a digital identity platform like Atala PRISM, offers a comprehensive solution to this quandary.

4. R&D that should be prioritized for digital assets: Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present. This includes topics for technical research, topics for research in the social sciences and across disciplinary boundaries, and opportunities for hardware and software development. This also includes information about emerging areas that could enable new opportunities to leverage digital assets, as well as information about technical limitations of digital assets and the associated business models and governance arrangements they often rely upon. Respondents are encouraged to, where relevant, describe how the discussed R&D topic could be useful in helping a potential U.S. CBDC system align with the Policy Objectives for a U.S. CBDC System.Respondents are also encouraged to share how the discussed R&D topic could help advance U.S. competitiveness and leadership in the world.

The cryptographic techniques that form part of the necessary infrastructure of blockchain networks can come to be a vital pillar for the data integrity of secure communication. R&D should be prioritized at exploring how blockchain technology can be utilized for national security and protecting our country's digital infrastructure.

6. Other information that should inform the R&D Agenda: Information about any other topic, not covered above, that respondents believe is important to inform the development of the National Digital Assets R&D Agenda. This may include ideas for collaborations between the Federal Government and other entities, as well as proposals that may not yet be feasible with the current state of technology but might become feasible in the next decade.

Government agencies, in collaboration with industry actors, can introduce blockchain-related technical infrastructure and adopt blockchain technology to deliver public services. Embracing blockchain pilot projects to streamline government functions would send positive signals to businesses seeking to use blockchain. Ongoing engagement with the private sector is also crucial so that policymakers, regulators, federal agencies and their staffs understand the technology, emerging innovations, their evolution, and the applications these technologies can play in society.

The focus on digital assets, as opposed to blockchain technology, means people can not see the forest from the trees. Blockchain technology, with its unique features (such as transparency, disintermediation, collaboration, immutability, and cryptographic security), can positively impact many aspects of society that are not related to securities or commodities. The same technology that would enable a rancher to register a brand could be reused for land deeds, a credit score, or issuing a non-fungible token (NFT) to represent a musical composition, assuring its artist of receiving fair compensation. From trade finance, to customs and certification processes, transportation and logistics, insurance claim settlements, environmental, social governance (ESG) disclosure compliance and government procurement— possible applications of blockchain technology encompass a diverse set of areas that can transform global commerce.

Sincerely,

[redacted]

Rachel Epstein, Esq.
Head of Government Affairs
Input Output Global, Inc.
[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

IPwe, Inc.

IPwe
Innovation Matters.
Manage It Better.

VIA EMAIL – DARD-FTAC-RFI@nitrd.gov **March 3, 2023**

To:

The White House Office of Science and
Technology Policy (OSTP)

Fast Track Action Committee (FTAC) on
Digital Assets Research and Development
of the Subcommittee on Networking and Information
Technology Research and Development (NITRD)of the National
Science and Technology Council

National Science Foundation (NSF)

NITRD National Coordination Office (NCO)

Re: RFI Response: Digital Assets R&D Agenda

Dear Members of OSTP and Members of Related Committees, Foundations and Offices:

I appreciate the opportunity to provide this RFI response on your National Digital Asset R&D Agenda and your efforts to expand the understanding of the full breadth and potential for digital assets across all financial and other use cases.

Introduction, Background and RWAs:

My name is Leann Pinto, and I am the President and Chief Executive Officer of IPwe, Inc. I, on behalf of IPwe, welcome your invitation to comment on digital assets, specifically with respect to Digital Assets Information Request No. 1. "*Goals, sectors or applications that could be improved with digital assets and related technologies,*" focusing on "where digital assets [can] provide significant value to the public, and examples of where benefits are already being delivered."

By way of background and prior to joining IPwe, I have had the benefit of working in pharma as a junior executive, as a lawyer for major firms in intellectual property, and at one of the largest tech corporations in the world. While I am becoming recognized as an authority on non-fungible tokens or ("NFTs"),[1] in particular dynamic patent NFTs, my interest in this topic, as well as my understanding is enhanced by my experience in business and law.

[1] *See*, https://www.uspto.gov/ip-policy/patent-policy/roundtable-patents-and-non-fungible-tokens; https://www.forbes.com/sites/jeffgapusan/2023/01/30/intangibles-and-nfts-can-creators-make-beliebers-of-companies/?sh=4ba6572e147a; https://www.forbes.com/sites/jeffgapusan/2023/02/15/birkin-bags-make-the-case-for-tokenizing-ip/

My focus in these comments will not be on "cryptocurrencies" or the related tokens or coins, including "CBDC," as those terms are defined in the RFI. Although these are fascinating applications of blockchain technology, this is only one subset of "digital assets," and which has heretofore been greatly misunderstood and overhyped, making these areas ripe for regulatory oversight. Instead, I will briefly comment on NFTs—a more useful and important type of "digital assets" that is also misunderstood—and how these can efficiently and elegantly improve understanding, management, and utilization of Real-World Assets ("RWAs"), in particular, "intangible assets."

Intangible assets, as used in accounting literature, refer to what is generally known as intellectual property ("IP") in all its forms, including patents, trademarks, copyrights, goodwill, trade secrets, and know-how, among others. It is currently estimated that now intangible assets comprise approximately about 90% of the market value reflected in the S&P 500, equating to over $21 trillion.[2]

<u>Digitization of Intangible Assets</u>:

While working at IBM in a senior role responsible for licensing IP, I developed an interest in blockchain technology. At that time, IBM was working with some of the largest corporations in the world and guiding them through the blockchain labyrinth. I had the good fortune of participating in many meetings with blockchain thought leaders that grasped, sooner than most of us, the potential for non-cryptocurrency digital asset applications of blockchain for enterprise, ranging from financial, to supply chain, to asset management and other applications. During this time, I became acquainted with Erich Spangenberg, the founder of IPwe, as they were working closely with IBM to develop non-cryptocurrency blockchain technology and applications to better manage IP.[3]

Since its inception in late 2018, IPwe has been focused on using blockchain and artificial intelligence (AI) to better manage intangible assets, with an initial focus on patents and trade secrets. At its core, IPwe believes innovation matters and that there are significant benefits—both for the owners but also for society overall—to be realized by managing it better, especially as we enter the web3 world. While our primary mission is more effective management and expanding commercial opportunity for innovation, a critical component of how we do this is by the creation of digital assets in the form of NFTs to store public verified and secure private data on an asset by asset (*e.g.*, patent by patent) basis. The current practice is to maintain this information in multiple disparate databases—if it is maintained at all—which massively complicates the understanding, management, and effective utilization of these critical assets. As opposed to cryptocurrencies or digital art, IPwe is focused on creating a secure, yet readily accessible, digital asset solution for storage of critical business information around the RWA in the intangible form.

[2] https://www.franklintempleton.com/articles/strategist-views/deep-waves-the-quiet-undertow-of-intangible-assets; https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-value-ip-rights-and-reputation-included/.
[3] https://www.ibm.com/case-studies/ipwe/

While we work with over 1,000 Small and Medium Enterprises (SMEs), IPwe also works with some of the largest corporations in the world.[4] While "cryptocurrency" applications continue to dominate the public discussion, fueled by uncertainty, stories of bad actors (*e.g.*, FTX) and a lack of understanding of the technology, most companies have made the decision to avoid crypto applications altogether until the regulatory environment is much clearer. Blockchain technology has multiple applications beyond cryptocurrencies and related tokens. My purpose in writing is to encourage you to expand the dialogue around blockchain and to evaluate and ultimately encourage blockchain applications and digital assets utilization for enterprise beyond "cryptocurrencies."

With an acknowledged bias, allow me to highlight a few elements of why blockchain, and in particular digital assets NFTs, are useful to more effectively manage RWA and promote innovation.

- <u>Verified Information</u>: Currently, there is a lot of information available in our Google/Bing/ChatGPT world, but the source and veracity of this "information" is difficult to ascertain. Unlike a blockchain application where the origin of a particular digital asset can be traced back to a specific block, the same is not true for other external applications and "information." This is referred to as the "Oracle Problem," which equates to a simple limitation that is the essence of blockchain and why this technology is extremely secure and reliable—external information to the blockchain is unverified. While this cannot be eliminated, a record of who input the "information" can be created, whether that "information" was able to be confirmed through cross-references to other public sources, and whether the "information" is likely reliable. This is referred to as "Verified Information." Blockchain technology—and NFTs in particular—is uniquely fit for purpose to create such digital asset record of "Verified Information." Just like title records in real property, Verified Information stored on an NFT digital asset is transparent and its reliability can be more easily tested. for trustworthy businesses to operate efficiently, Verified Information will become critical.
- <u>Centralized Information Management</u>: By its nature, IP from its inception throughout its lifecycle is typically managed by many different people and groups, all with their own, separate databases—with significant information lost along the way as these "hand-offs" occur. The path a patent follows is illustrative of the challenge: The creator who conceives of the innovation is involved at the earliest stages, but often there is a hand-off to another person or group that assesses that innovation and determines it should be patented. Once this assessment is completed, the innovation is typically handed-off to another person or group that drafts the application and prosecutes the patent, interacting with the various patent offices around the world, and most likely, multiple outside legal service providers. Once the patent(s) issue and the prosecution phase is completed, there is most often another group that takes responsibility for maintaining the patent assets, and hence, another hand-off. But then after patent issuance, the utilization rate of the innovation is estimated to be 5%.[5] The time from conception to patent issuance is typically measured in years. The information that is lost during this time is an important contributor to these dismal utilization rates. Capturing this information (data) during each phase and storing it in a secure centralized location is a significant benefit that digital asset NFTs are well-suited to handle.

[4] *See*, https://www.prnewswire.com/news-releases/clarivate-partners-with-ipwe-to-enhance-ai-and-blockchain-patent-solutions-301679350.html; https://newsroom.ibm.com/2021-04-20-IPwe-and-IBM-Seek-to-Transform-Corporate-Patents-With-Next-Generation-NFTs-Using-IBM-Blockchain

[5] https://www.forbes.com/sites/danielfisher/2014/06/18/13633/?sh=332341226f1c

IPwe
Innovation Matters.
Manage It Better.

- Digital Asset Class: By creation of digital assets for RWA, and in particular for IP, an entirely new asset class can be unlocked for developers, inventors, creators, and companies to truly achieve their innovation potential. I have seen first-hand how difficult it can be to transact in the IP space, particularly patents. The extremely low utilization rates mentioned above reflect the antiquated, inefficient, and untrusted practices that are *de rigeour* for large patent holders and single inventors alike. By providing a secure, transparent and verified source of data and information in a digital asset NFT for IP RWAs, society will finally be able to efficiently achieve its potential and enable all members to innovate collaboratively.

Why am I providing these comments to you?

In my role as President and CEO of IPwe, I see first-hand the actions that various governments are taking to encourage the creation of digital assets for data storage, and particularly the digitization of RWAs. China is well ahead of the US—Japan is not far behind—in encouraging the digitization of RWAs, in particular IP assets. While addressing cryptocurrency applications is important, I hope that the members will also consider the potential applications of digital assets for blockchain beyond cryptocurrencies and encourage corporations to broaden their understanding of the capabilities of blockchain to fundamentally improve the understanding, management, and utilization of RWAs.

I appreciate your time and consideration. If you require any further information, please do not hesitate to contact me at [redacted]

Sincerely,

[redacted]

Leann M. Pinto
President & CEO
IPwe, Inc.

From: James A. Eugene
To: DARD-FTAC-RFI
Subject: RFI Response: Digital Assets R&D Agenda (James Eugene)
Date: Friday, January 27, 2023 10:22:27 PM

Hello, my name is James Eugene

Here are a few fundamental principles that could be used to regulate CBDCs in a way that would be generally well-received:

1. Security: Ensure that the technology behind the CBDC is secure and able to protect consumers' personal and financial information.
2. Privacy: Provide robust privacy protections for consumers to keep their transactions confidential and protected from unauthorized access.
3. Accessibility: Make the CBDC easily accessible to all, regardless of income or location, so that everyone has the opportunity to use and benefit from it.
4. Transparency: Ensure that the operations and decision-making processes behind the CBDC are transparent and accountable so that consumers and stakeholders have confidence in the system.
5. User-friendliness: Design the CBDC to be user-friendly and intuitive so that even those with limited technical knowledge can easily use and understand it.
6. Inclusivity: Ensure that the CBDC is inclusive and does not discriminate against certain groups or individuals, such as those in underbanked communities.
7. Decentralization: Consider implementing a decentralized or semi-decentralized design for the CBDCs to make the system more democratic and resilient.

By following these principles, policymakers and regulators can create a CBDC that is trusted and widely used, providing benefits to people worldwide.

PUNISHMENT

Penalties for scammers and hackers who steal CBDCs should be severe and deterrent in nature to ensure the safety and security of the digital currency system. Here are a few potential approaches to penalizing these criminals:

1. Criminal Prosecution: Scammers and hackers who steal CBDCs can be prosecuted under relevant criminal laws and face penalties such as imprisonment, fines, and asset forfeiture.
2. Civil Litigation: Victims of CBDC theft can pursue civil lawsuits against the perpetrators and seek damages for their losses.
3. Regulatory Sanctions: Regulators can impose penalties on individuals and organizations that engage in CBDC-related fraud or hacking, such as fines, restrictions on their ability to operate in the market, and revoking of licenses.
4. International Cooperation: In cases where the perpetrators operate across borders, international cooperation between law enforcement and regulatory agencies can be leveraged to bring them to justice.
5. Technological Countermeasures: To prevent and deter future thefts, it may also be necessary to invest in advanced security and anti-fraud technologies to detect and prevent these types of crimes.

If CBDCs are hacked, and people's funds are stolen or lost, it could erode confidence in the government and the digital currency system. A loss of confidence could lead to a decline in the adoption and use of CBDCs, which would hurt the economy and the financial system as a whole.

Therefore, the government must take appropriate measures to ensure the security and stability of CBDCs, such as implementing strong cybersecurity measures, conducting regular audits and risk assessments, and having contingency plans in place to respond to potential security incidents.

Moreover, the government should be transparent and communicate effectively with the public about the measures it is taking to protect CBDCs and respond to security incidents to help build and maintain trust in the digital currency system.

Overall, the government must prioritize the security of CBDCs and take all necessary steps to prevent hacking and other types of fraud, maintain the public's trust in the digital currency system and ensure its long-term viability. If the government does not take proper measures to prevent scammers, frauds, and hackers, people will turn to cryptocurrencies despite their volatility and look solely toward battle tested and proven stablecoins which do not lose their peg.

TAX

To tax CBDCs in a way that would be fair and acceptable to individuals and families across different income levels, policymakers should consider the following principles:

1. Progressivity: A progressive tax system, where the tax rate increases as income increases, would ensure that those with higher incomes pay a larger share of their income in taxes.
2. Simplicity: The tax system for CBDCs should be simple and easy to understand so that individuals and families can easily calculate and pay their taxes.
3. Transparency: The rules and procedures for taxing CBDCs should be clear and transparent so that everyone knows what they are responsible for and can trust the system.
4. Equity: The tax system should be designed to be fair and equitable so that those with similar incomes are taxed similarly, regardless of their wealth or other factors.
5. Minimal Burden: The tax system should impose a minimal burden on individuals and families so that they are not unduly burdened by tax compliance or collection.
6. Avoid Double Taxation: Efforts should be made to avoid double taxation of CBDCs so that individuals and families are not unfairly taxed on the same income or assets multiple times.

COEXISTENCE

For CBDCs and cryptocurrencies to coexist and harmonize, a number of factors should be taken into consideration:

1. Regulatory Framework: Establishing a clear and consistent regulatory framework for CBDCs and cryptocurrencies will help ensure that they are subject to the same rules and oversight.
2. Interoperability: Developing technical standards and protocols to enable CBDCs and cryptocurrencies to interact and exchange value with each other will promote greater harmonization and cooperation between the two systems.
3. Consumer Protections: Ensuring that consumers have access to robust protections and dispute resolution mechanisms, regardless of whether they use CBDCs or cryptocurrencies, will help promote trust in the digital currency ecosystem.
4. Education and Outreach: Educating consumers, businesses, and regulators about the benefits and risks associated with CBDCs and cryptocurrencies will help to promote understanding and acceptance of these innovative technologies.
5. Collaboration and Partnership: Encouraging cooperation and partnerships between CBDC and cryptocurrency stakeholders, including governments, private sector companies, and civil society organizations, will help to build a more inclusive and effective digital currency ecosystem.

Governments should work with well known top cryptocurrencies for payment of services and goods. Crypto needs new regulation that will cause it to thrive under a new jurisdiction and NOT the SEC.

Cryptocurrencies, such as Bitcoin, Ethereum and Cardano should be treated as commodities because:

1. Decentralization: Like commodities, cryptocurrencies are decentralized and not issued by governments.
2. Limited supply: Most cryptocurrencies have a limited supply, similar to commodities.
3. Speculative investment: Cryptocurrencies are often bought and sold as speculative investments, similar to how commodities are traded.
4. Volatility: Cryptocurrency prices can be highly volatile, similar to the prices of

commodities.

Cryptocurrencies should be treated as digital commodities and should be viewed as another component of the internet. Crypto makes the internet more robust!

STABLECOINS

Governments can use stablecoins in a number of ways, including:

1. Digital Payment: Governments can use stablecoins as a digital payment system for government-to-government and government-to-citizen transactions, such as taxes, subsidies, and social welfare programs.
2. Financial Inclusion: By adopting stablecoins, governments can promote financial inclusion and provide access to financial services to underbanked and unbanked populations, who may not have access to traditional banking services.
3. Cross-Border Payments: Stablecoins can be used for cross-border payments, reducing the cost and time required for traditional cross-border transactions and making it easier for governments to transact with other countries.
4. Increased Transparency and Accountability: Stablecoins can increase transparency and accountability in government transactions, as all transactions are recorded on a secure, decentralized ledger, providing a permanent and immutable record of government activity.
5. Crisis Response: In times of crisis, such as natural disasters or economic turmoil, stablecoins can be used to quickly distribute funds to affected populations, providing a fast and efficient response to emergencies.

Overall, by leveraging the benefits of stablecoins, governments can improve the efficiency and effectiveness of their operations, while also promoting financial inclusion and increasing transparency and accountability.

I hope this was sufficient help,

Please get back to when you can

--
Peace

James A. Eugene

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Jamie Nestor

From: Jamie Nestor
To: DARD-FTAC-RFI
Subject: RE: RFI Response: Digital Assets R&D Agenda
Date: Friday, March 3, 2023 5:05:29 PM
Attachments: image002.png
image003.png

Please see corrected link to Trail of Bits Paper [redacted]

Thank you.

From: Nestor, Jamie Butcher (CID) (FBI)
Sent: Friday, March 3, 2023 5:00 PM
To: DARD-FTAC-RFI@nitrd.gov
Subject: RFI Response: Digital Assets R&D Agenda

Attention: Office of Science and Technology Policy (OSTP)
Re: RFI Response: Digital Assets R&D Agenda
In response to the second request for information: *2. Goals, sectors, or applications where digital assets introduces risks or harms: Information about goals, sectors, or applications where digital assets might introduce risks or harms, and examples of where risks or harms are already being manifested,* the FBI Virtual Assets Unit provides the following information:

I. Limited ability to recover funds lost to fraud or theft

a. The near instantaneous speed of transactions presents significant risk and reduces the ability to recover stolen/hacked/fraudulent funds, as compared to the traditional banking system which has time delays that assist in recovery. The traditional banking system allows for an effective Financial Fraud Kill Chain, which had a 74% success rate on business e-mail compromise (BEC) complaints, where initiated (involving domestic to domestic transactions), placing a hold on $329 million in 2021 according to the Internet Crime Complaint Center (IC3). See 2021 IC3 Annual Report.

b. In FY22, IC3 received 52,217 complaints related to cryptocurrency, with losses of $3.855 billion, more than double cryptocurrency related losses in 2021 ($1.6B). This exponential increase in losses is expected to continue.

II. Sanctions evasion

a. While both the inherent transparency of cryptocurrency and the compliance of cryptocurrency exchanges have demonstrated that sanctions enforcement is possible in the crypto world, many other exchanges facilitating the bulk of illicit activity are not compliant and easily allow sanctions evasion if their infrastructure remains untouched. For example, Garantex, which took in funds sent by ransomware addresses, saw its crypto transaction volume steadily increase post-designation. In the four months leading up through the April 2022 sanctioning of Garantex, the high-risk exchange averaged $620.8 million in monthly inflows. Post-sanctions, Garantex's inflows rose considerably, with an average of approximately $1.3 billion in monthly inflows through October. "This is most likely due to the fact that Garantex and most of its users are based in Russia. The Russian government has not enforced U.S. sanctions, leaving users not subject to U.S. jurisdiction with virtually no incentive to stop using Garantex. In fact, Garantex explicitly stated its intent to continue operating in social media posts immediately following the designation." Per 2022 Chainalysis report - [redacted]

III. Many exchanges lack Know Your Customer (KYC) requirements

a. The lack of availability of such data makes identifying the individuals responsible for committing a particular crime that much more difficult.

b. The boundaryless nature of virtual assets allow criminals to target victims around the globe, while insulating themselves from the threat of repercussions for their actions.

IV. The general public does not understand the technology enough to understand the associated risks to take appropriate precautions

a. Victims are lured into making investments through fake sites and apps with promises of unrealistic returns.

b. Victims are tricked into moving their money into "encrypted accounts" through crypto-currency kiosks that are under the control of malicious actors.

c. Individual's store their private keys in browsers or other places that are susceptible to compromise by malicious actors.

d. Individuals lose their private keys or seed phrase with no way of recovering assets.

V. Virtual asset service providers (VASPs) are subject to hacks, thefts and collapses

a. As of November 2022, there were more than 130 thefts from VASPs

VI. Blockchains are not actually as decentralized as believed due to centralized on and off ramps and are therefore potentially easier to disrupt than generally believed

a. [redacted]

b. You have to either (a) accept its immutability and trust that its programmers did not introduce a bug, or (b) permit upgradeable contracts or off-chain code that share the same trust issues as a centralized approach.

c. The number of entities sufficient to disrupt a blockchain is relatively low:

four for Bitcoin, two for Ethereum, and less than a dozen for most proof of stake (PoS) networks.

In response to the third request for information: *3. Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets,* the FBI Virtual Assets Unit provides the following information:

I.Research and development on a government run and funded blockchain analysis tool should be considered.

a. Currently there are several commercial blockchain analysis tools available for purchase. The use of these tools greatly enhances law enforcement's ability to investigate crimes, countering illicit financial activity and potentially recovering victim funds. The speed of transactions and the complexity of money laundering techniques used by some actors add to the value of the availability of such tools. The currently available tools can be cost prohibitive especially to smaller state and local law enforcement departments where funding is limited. The drastic increase in complaints related to virtual assets mean that no department is isolated from them and will need additional functionality to move forward with investigations.

b. While we recognize the development of such a tool may never reach the same level as the private sector solutions, having an option available is better than not. Open-source block explorers are helpful but do not lend themselves to the same level of attribution.

Jamie Butcher Nestor
SSA – Virtual Assets Unit (VAU)
[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Trail of Bits

Are Blockchains Decentralized?

Unintended Centralities in Distributed Ledgers

June 2022

Prepared by:

Evan Sultanik
Alexander Remie
Felipe Manzano
Trent Brunson
Sam Moelius
Eric Kilmer
Mike Myers
Talley Amir
Sonya Schriner

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 80+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at https://github.com/trailofbits/publications, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom.

Trail of Bits also operates a center of excellence for blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Cosmos, Ethereum 2.0, MakerDAO, Matic, Polkadot, Solana, Uniswap, Web3, and Zcash.

To keep up to date with our latest news and announcements, please follow @trailofbits on Twitter and explore our public repositories at https://github.com/trailofbits. To engage us directly, visit our "Contact" page at [redacted], or email us at [redacted]

Trail of Bits, Inc.
[redacted]
https://www.trailofbits.com
[redacted]

Table of Contents

Executive Summary

Over the past year, Trail of Bits was engaged by the Defense Advanced Research Projects Agency (DARPA) to investigate the extent to which blockchains are truly decentralized. We focused primarily on the two most popular blockchains: Bitcoin and Ethereum. We also investigated proof-of-stake (PoS) blockchains and Byzantine fault tolerant consensus protocols in general. This report provides a high-level summary of results from the academic literature, as well as our novel research on software centrality and the topology of the Bitcoin consensus network. For an excellent academic survey with a deeper technical discussion, we recommend the work of Sai, et al.[1]

Blockchains Are Decentralized, Right?

Distributed ledger technology (DLT)—and, specifically, *blockchains*—are used in a variety of contexts, such as digital currency, decentralized finance, and even electronic voting. While there are many different types of DLT, each built with fundamentally different design decisions, the overarching value proposition of DLT and blockchains is that they can operate securely without any centralized control. The cryptographic primitives that enable blockchains are, by this point, quite robust, and it is often taken for granted that these primitives enable blockchains to be *immutable* (not susceptible to change). This report gives examples of how that immutability can be broken *not* by exploiting cryptographic vulnerabilities but instead by subverting the properties of a blockchain's implementations, networking, and consensus protocol. We show that a subset of participants can garner excessive, centralized control over the entire system.

Sources of Centralization

This report covers several ways in which control of a DLT can be centralized:

- **Authoritative centrality:** What is the minimum number of entities necessary to disrupt the system? This number is called the *Nakamoto coefficient*, and the closer this value is to one, the more centralized the system. This is also often referred to as "Governance Centrality".

- **Consensus centrality:** Similar to authoritative centrality, to what extent is the source of consensus (e.g., proof-of-work [PoW]) centralized? Does a single entity (like a mining pool) control an undue amount of the network's hashing power?

- **Motivational centrality:** How are participants disincentivized from acting maliciously (e.g., posting malformed or incorrect data)? To what extent are these

[1] Sai et al., "Taxonomy of centralization in public blockchain systems: A systematic literature review," *Information Processing & Management*, Volume 58 Issue 4, (July 2021).

incentives centrally controlled? How, if at all, can the rights of a malicious participant be revoked?

- **Topological centrality:** How resistant is the consensus network to disruption? Is there a subset of nodes that form a vital bridge in the network, without which the network would become bifurcated?

- **Network centrality:** Are the nodes sufficiently geographically dispersed such that they are uniformly distributed across the internet? What would happen if a malicious internet service provider (ISP) or nation-state decided to block or filter all DLT traffic?

- **Software centrality:** To what extent is the safety of the DLT dependent on the security of the software on which it runs? Any bug in the software (either inadvertent or intentional) could invalidate the invariants of the DLT, e.g., breaking immutability. If there is ambiguity in the DLT's specification, two independently developed software clients might disagree, causing a fork in the blockchain. An upstream vulnerability in a dependency shared by the two clients can similarly affect their operation.

Key Findings and Takeaways

The following are the key findings of our research. They are explained in more detail in the remainder of the report.

- The challenge with using a blockchain is that one has to either (a) accept its immutability and trust that its programmers did not introduce a bug, or (b) permit upgradeable contracts or off-chain code that share the same trust issues as a centralized approach.

- Every widely used blockchain has a privileged set of entities that can modify the semantics of the blockchain to potentially change past transactions.

- The number of entities sufficient to disrupt a blockchain is relatively low: four for Bitcoin, two for Ethereum, and less than a dozen for most PoS networks.

- The vast majority of Bitcoin nodes appear to not participate in mining and node operators face no explicit penalty for dishonesty.

- The standard protocol for coordination within blockchain mining pools, Stratum, is unencrypted and, effectively, unauthenticated.

- When nodes have an out-of-date or incorrect view of the network, this lowers the percentage of the hashrate necessary to execute a standard 51% attack. Moreover, only the nodes operated by mining pools need to be degraded to carry out such an attack. For example, during the first half of 2021 the actual cost of a 51% attack on Bitcoin was closer to 49% of the hashrate.

- For a blockchain to be optimally distributed, there must be a so-called *Sybil cost*. There is currently no known way to implement Sybil costs in a permissionless blockchain like Bitcoin or Ethereum without employing a centralized trusted third party (TTP). Until a mechanism for enforcing Sybil costs without a TTP is discovered, it will be almost impossible for permissionless blockchains to achieve satisfactory decentralization.

- A dense, possibly non-scale-free, subnetwork of Bitcoin nodes appears to be largely responsible for reaching consensus and communicating with miners—the vast majority of nodes do not meaningfully contribute to the health of the network.

- Bitcoin traffic is unencrypted—any third party on the network route between nodes (e.g., ISPs, Wi-Fi access point operators, or governments) can observe and choose to drop any messages they wish.

- Of all Bitcoin traffic, 60% traverses just three ISPs.

- Tor is now the largest network provider in Bitcoin, routing traffic for about half of Bitcoin's nodes. Half of these nodes are routed through the Tor network, and the other half are reachable through .onion addresses. The next largest autonomous system (AS)—or network provider—is AS24940 from Germany, constituting only 10% of nodes. A malicious Tor exit node can modify or drop traffic similarly to an ISP.

- Of Bitcoin's nodes, 21% were running an old version of the Bitcoin Core client that is known to be vulnerable in June of 2021.

- The Ethereum ecosystem has a significant amount of code reuse: 90% of recently deployed Ethereum smart contracts are at least 56% similar to each other.

Contact Information

Administrative points of contact:

Dan Guido, [redacted]

Trent Brunson, PhD, [redacted]

Technical point of contact:

Evan Sultanik, PhD, [redacted]

Scrutinizing Blockchain Immutability

Every blockchain has a privileged set of entities that can modify the semantics of the blockchain to potentially change past transactions: namely, the authors and maintainers of the software. Many blockchains have a virtual machine (VM) built atop—or sometimes even integrated into—their consensus protocol. Bitcoin and its derivatives have a VM for interpreting transaction output scripts. Ethereum uses a VM for executing its smart contracts. Blockchains' VM semantics often evolve in response to both the demand for new features and the need for security mitigations. New VM opcodes are often added, and the costs of performing certain operations are regularly tweaked to prevent denial-of-service attacks.[2]

In some cases, the developers or maintainers of a blockchain intentionally modify its software to mutate the blockchain's state to revert or mitigate an attack—this was Ethereum's response to the 2016 DAO hack.[3] But in most other cases, changes to a blockchain are an unintentional or unexpected consequence of another change. For example, Ethereum's Constantinople hard fork reduced the gas costs of certain operations. However, some immutable contracts that were deployed before the hard fork relied on the old costs to prevent a certain class of attack called "reentrancy." Constantinople's semantic changes caused these once secure contracts to become vulnerable.[4] Fortunately, this issue was discovered manually, by chance, with just enough time before the fork for it to be delayed and later abandoned. In 2021, the Polkadot blockchain platform was temporarily crippled by node failures caused by an update to the Rust programming language compiler used to build the nodes.[5] In late August of 2021, a consensus issue related to changes in the most popular Ethereum client was exploited to cause a hard fork of the cryptocurrency.[6]

The data—and, more importantly, the code—deployed to a blockchain are not necessarily semantically immutable. Not only can the state of the blockchain be retroactively changed through modifications to the blockchain's software, but the semantics of individual transactions can change between when the transaction is initiated and when it is ultimately mined onto the blockchain thanks to software changes in the interim. Some blockchain platforms like Polkadot and Substrate also allow certain parameters and code to be updated through an on-chain governance process.

---

[2] Renlord Yang et al., "Empirically Analyzing Ethereum's Gas Mechanism," *IEEE EuroS&P*, 2019.
[3] David Siegel, "Understanding the DAO Attack," *CoinDesk*, June 25, 2016.
[4] Christine Kim and Nikhilesh De, "Ethereum's Constantinople Upgrade Faces Delay Due to Security Vulnerability," *CoinDesk*, January 15, 2019.
[5] Bastian Köcher, "A Polkadot Postmortem," *Polkadot* (blog), May 24, 2021.
[6] Turner Wright, "Bug in Ethereum Client Leads to Split — EVM-Compatible Chains at Risk," *Cointelegraph*, August 27, 2021.

The software itself does not necessarily need to change to affect the security properties of a DLT. For example, although Bitcoin is less than 15 years old, many of the foundational assumptions made when its protocol was designed have already become obsolete. When Bitcoin was originally conceived, Nakamoto assumed that each node in the consensus network would participate in mining. However, as the mining difficulty increases—thus decreasing the probability of getting a mining reward—"mining pools" (collectives that group both mining power and rewards) become increasingly popular as a means to garner a consistent profit. Today, the four most popular mining pools constitute over 51% of the hashrate of Bitcoin. Each mining pool operates its own, proprietary, centralized protocol and interacts with the public Bitcoin network only through a gateway node. In other words, there are really only a handful of nodes that participate in the consensus network on behalf of the majority of the network's hashrate. Controlling those nodes provides the means to, at a minimum, deny service to their constituent hashrate. This breaks the original assumption that all Bitcoin nodes will have a financial incentive (via mining) to remain honest. **If a node operator's self-interest is to be dishonest, then there is no explicit penalty for doing so**. Moreover, the number of *entities* necessary to execute a 51% attack on Bitcoin was reduced from 51% of the entire network (which we estimate at approximately 59,000 nodes) to only the four most popular mining pool nodes[7] (less than 0.004% of the network).

Finally, any blockchain that supports Turing-complete[8] on-chain execution (e.g., Ethereum, Hyperledger, and Tezos) cannot enforce semantic immutability. This is because such blockchains cannot prevent contracts from being upgradeable (a Turing Machine is capable of simulating any other Turing Machine,[9] allowing for upgradeability via interpreted inputs even if the on-chain code is immutable). For example, Alice can submit a transaction to a contract and, before the transaction is mined, the contract could be upgraded to have completely different semantics. The transaction would be executed against the new contract. Upgradeable contract patterns have become incredibly popular in Ethereum as they allow developers to circumvent immutability to patch bugs after deployment. But they also allow developers to patch in backdoors that would allow them to abscond with a contract's assets. **The challenge with using a blockchain is that one has to either (a) accept its immutability and trust that the programmers did not introduce a bug, or (b) permit upgradeable contracts or off-chain code that share the same trust issues as a centralized approach.**

[7] https://www.blockchain.com/charts/pools

[8] Such blockchains are technically linear bounded automata due to gas constraints.

[9] *Stanford Encyclopedia of Philosophy,* s.v. "Turing Machines," first published September 24, 2018.

The Nakamoto Coefficient

Various metrics have been proposed to measure the centrality or fairness of a DLT, including the Gini coefficient and Lorenz curve, both borrowed from economic theory. However, the minimum *Nakamoto coefficient* is perhaps the most intuitive. The Nakamoto coefficient is the number of entities sufficient to attack the system.[10] A completely centralized system will have a Nakamoto coefficient of one. The lower the Nakamoto coefficient, the more centralized the system.

It is well known that Bitcoin is *economically* centralized: in 2020, 4.5% of Bitcoin holders controlled 85% of the currency.[11] But what about Bitcoin's *systemic* or *authoritative* centralization? As we saw in the last section, **Bitcoin's Nakamoto coefficient is four**, because taking control of the four largest mining pools would provide a hashrate sufficient to execute a 51% attack. In January of 2021, **the Nakamoto coefficient for Ethereum was only two.**[12] As of April 2022, it is three.[13]

Even though these Nakamoto coefficients are relatively low, some might argue that exploiting them to attack a blockchain would be prohibitively expensive. While this may be true for individuals, **the actors incentivized to perpetrate these attacks include operators of competing currencies and nation-states who have the requisite resources**. Perverse incentives can exist with blockchains in the same way that the relative values of fiat currencies can be manipulated.

PoS protocols are becoming increasingly popular consensus mechanisms that address some of the shortcomings (e.g., expensive computation) of PoW blockchains like Bitcoin, Ethereum, and their derivatives. Instead of solving computationally hard problems like PoW miners do to mine blocks, most PoS networks instead require its block validators to stake a certain amount of cryptocurrency as collateral in the event that they act dishonestly—their mining power is proportional to their stake. Some PoS chains like Algorand distribute cryptocurrency as rewards for good governance.[14] PoS blockchains employ complex protocols to ensure that transactions are validated and to police the validators. Most PoS blockchain's consensus protocols (Avalanche's Snowflake, Solana's Tower BFT, etc.) break down if the validators associated with at least one-third of the staked assets are malicious, effectively pausing the network. Therefore, the Nakamoto coefficient of most PoS

---

[10] Balaji S. Srinivasan, "Quantifying Decentralization," *news.earn.com*, July 27, 2017.
[11] Sami Ben Mariem et al., "All that Glitters Is Not Bitcoin — Unveiling the Centralized Nature of the BTC (IP) Network," *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, (February 19, 2020).
[12] Qinwei Lin et al., "Measuring Decentralization in Bitcoin and Ethereum Using Multiple Metrics and Granularities," *arXiv:2101.10699v2 [cs.CR]*, (February 2, 2021).
[13] https://miningpoolstats.stream/ethereum
[14] Algorand Governance, s.v. "More Committing Commitments," accessed April 27, 2022.

blockchains is equal to the smallest number of validators that have collectively staked at least a third of all of the staked assets.

The following are the Nakamoto coefficients for popular PoS blockchains as of August 25, 2021:

Blockchain	Nakamoto Coefficient	Total # of Validators	Staked Value	Source
Avalanche	25	1,041	$11B	https://explorer.avax.network/validators
Solana	19	876	$37B	https://solana.com/validators
Eth2[15]	12	219,182	$22B	https://www.nansen.ai/
THORChain	11	38	$0.5B	https://thorchain.net/#/nodes
Terra	8	130	$12B	https://stake.id/#/
Cosmos	6	125	$4B	https://www.mintscan.io/cosmos/validators
BSC[16]	5	21	$7B	https://bscscan.com/validatorset
Fantom	3	46	$1B	https://ftmscan.com/validators
Polygon	2	100	$3B	https://wallet.matic.network/staking/

[15] The total number of validators is an upper bound. According to Nansen, the four biggest depositors have more than a third of the stake, and those depositors have 12 nodes.
[16] The number of validators necessary to reach one third of the stake is seven, but three are controlled by the same entity: Binance.

Consensus Centrality: Mining Pool Vulnerabilities

An increasing number of consensus protocol operations are being delegated to a small number of entities that typically run their own centralized software and protocols with little-to-no on-chain governance—in the case of PoW blockchains, these entities are the mining pools, and in the case of PoS blockchains, these entities are staked validators. In the previous section, we discussed how these entities present a significant target to disrupt the stability of a blockchain. In this section, we discuss how such entities' off-chain governance structures further increase the attack surface of a blockchain.

While there is evidence that risk-sharing entities such as mining pools and staked validators decrease the *economic* centralization of a blockchain, it is well known that they exist as *technological* single points of failure and are therefore rich targets for denial-of-service attacks.[17] **The safety of a blockchain depends on the security of the software and protocols of its off-chain governance or consensus mechanisms.**

Today, mining pool operators communicate with their participants using Stratum: an ad hoc JSON remote procedure call (RPC) protocol that organically evolved over the past decade with no official standardization. The protocol permits the mining pool operator to create "jobs" for each mining participant, each of which requires the participant to brute-force search through a unique subset of the search space of possible valid blocks.

The Stratum protocol is not encrypted. All jobs assigned to miners, all work results from miners, and even the initial authentication are transmitted in plaintext. The Stratum developers may have made this design decision because the Stratum protocol is implemented in the firmware of most hardware miners, which may not have the resources to implement SSL or TLS. Moreover, the Stratum developers may not have anticipated that attackers could exploit this design to authenticate as another user. It was later discovered that an eavesdropper such as a nation-state, ISP, or local network participant can use this transmitted information to estimate the hashrate and payouts of a miner in the pool. A malicious attacker-in-the-middle can actually manipulate Stratum messages to steal CPU cycles and payouts from mining pool participants.[18] These vulnerabilities have been known for years, and were initially addressed by adding forms of authentication to the Stratum protocol. However, none of the proposals to transition to a more secure protocol have been widely adopted.

Until 2018, authentication in the Stratum protocol did not even require a password. Attackers realized that they could deny service to mining participants by authenticating

---

[17] Lin William Cong, Zhiguo He, and Jiasun Li, "Decentralized Mining in Centralized Pools," *SSRN Electronic Journal* (January 2018).

[18] Ruben Recabarren and Bogdan Carbunar, "Hardening Stratum, the Bitcoin Pool Mining Protocol," *PETS* 3 (March 2017): 1–18.

with their usernames (which were enumerable from the mining pool website) and submitting invalid work.[19] After a miner submits a sufficient number of invalid blocks, mining pools would block the account of the participant, ignoring all further work and preventing future payouts. This was patched by requiring a password with authentication and using IP-based rather than account-based ban lists.

We have discovered that, today, all of the mining pools we tested either assign a hard-coded password for all accounts or simply do not validate the password provided during authentication. For example, all ViaBTC accounts appear to be assigned the password "123." Poolin seems not to validate authentication credentials at all. Slushpool explicitly instructs its users to ignore the password field as, "It is a legacy Stratum protocol parameter that has no use nowadays."[20] We discovered this by registering multiple accounts with the mining pools, and examining their server code, when available. These three mining pools alone account for roughly 25% of the Bitcoin hashrate.

The job of each miner is to find a nonce value that, when appended to the block header chosen by the mining pool, hashes to a value below a certain threshold set by the blockchain's current difficulty. A certain portion of the header is specific to the job/miner in order to prevent duplicate work across the jobs. The strategy by which mining pools choose both the base header for each job and the division of the search space between jobs (and, therefore, between individual miners) is not a part of the Stratum protocol; it is proprietary to the mining pool. ViaBTC is open source, so we can inspect how it works. ViaBTC creates a custom "coinbase" for each miner: the address to which rewards are deposited on success. This is what prevents a miner from absconding with a successfully mined block—the reward address, controlled by ViaBTC, is already baked into the header. ViaBTC also maintains a global, 32-bit job counter that it adds to the header, minimizing the search space overlap between jobs. The size of the search space for each job is 2^{96} bits out of 2^{256} bits, and it is unlikely that an attacker could overflow the job counter through repeated Stratum job requests, so it is still unlikely that jobs will have much overlap. However, **the mining pool server will continue to accept and perform computations to validate bogus work submitted by improperly authenticated miners, potentially leading to a denial of service.**

---

[19] Mohiuddin Ahmed et al., "A Poisoning Attack against Cryptocurrency Mining Pools," *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, eds. Joaquin Garcia-Alfaro et al. (Cham: Spring International Publishing, 2017), 140–154.
[20] Slushpool Bitcoin mining setup guide, s.v. "Which worker name/password should I choose?", accessed April 27, 2022.

Sybil and Eclipse Attacks: The "Other" 51%

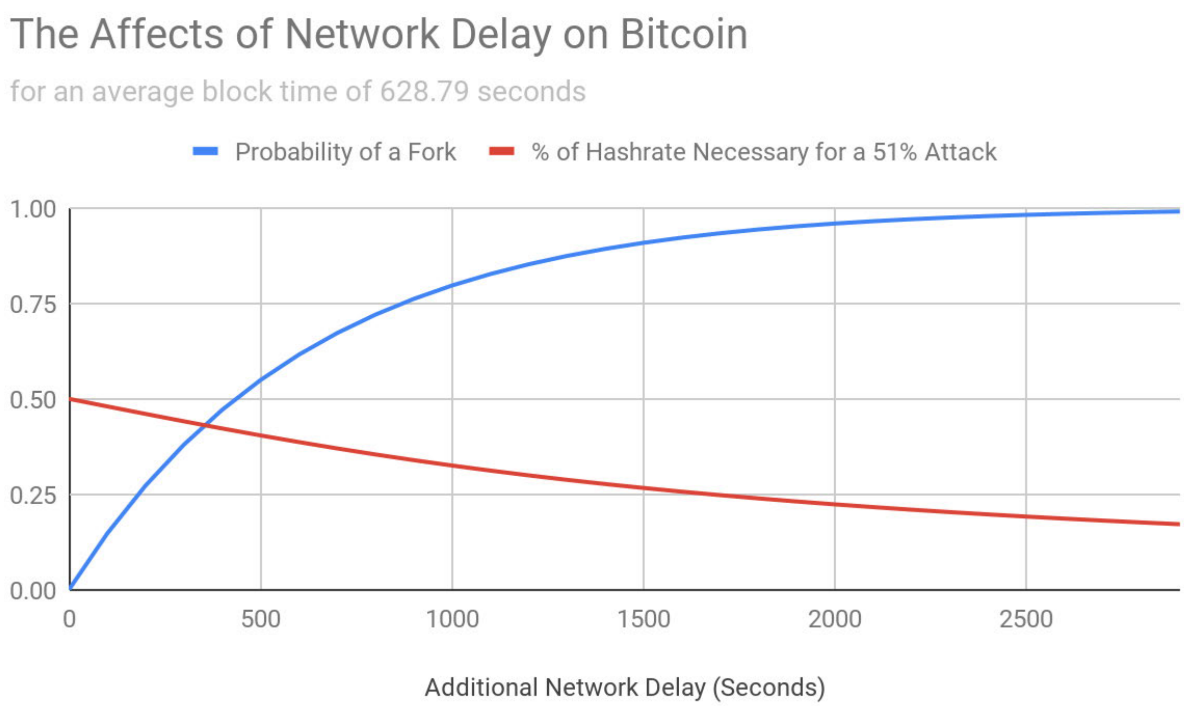
The discourse on attacks against PoW blockchains typically centers around the 51% attack: the very real threat that if a single entity controls at least 51% of the hashrate of the network, then that entity can modify the blockchain in otherwise prohibited ways.

It turns out that there are other forms of the 51% attack that affect all types of blockchains and distributed systems in general. What if the blockchain's consensus network were flooded with new, malicious nodes controlled by a single party? After all, deploying a new node requires only one inexpensive cloud server instance—no specialized mining hardware is necessary. This is called a *Sybil attack*. Such attacks can be used to affect the topology of the network in order to gain influence.

Sybil attacks can also be used to execute an *eclipse attack*: the denial of service to specific nodes in order to gain influence.[21] If one can cause nodes to have a sufficiently out-of-date or incorrect view of the network, this increases the probability of a blockchain fork: when two miners produce and broadcast valid but distinct blocks with the same parent block.[22] The longer the fork's branches become, the lower the percentage of the hashrate necessary for an attacker to execute a standard 51% attack.[23] This is because, eventually, one of the two branches will become the canonical head of the blockchain and the other branch will become a so-called "ommer" (previously called "uncle") blocks. Any transactions mined in ommer blocks will be invalidated, as if they had never been mined. The reason why forks reduce the cost of a standard 51% attack is because any hashrate expended toward extending a branch of the fork that will eventually become ommers is effectively wasted, reducing the effective global computational efficiency of the blockchain. Moreover, only the nodes directly connected to miners need to be degraded to carry out such an attack.[24]

---

[21] Atul Singh et al., "Defending against Eclipse Attacks on Overlay Networks," *EW 11: Proceedings of the 11th workshop on ACM SIGOPS European workshop* (September 2004).
[22] Christian Decker and Roger Wattenhofer, "Information Propagation in the Bitcoin Network," *IEEE P2P 2013 Proceedings* (2013).
[23] Dembo et al., "Everything is a Race and Nakamoto Always Wins," *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (November 2020)
[24] Ittay Eyal and Emin Gün Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," 2018.



The probability of a fork is calculated from Equation (3) of (Decker & Wattenhofer, 2013):

$$Pr[F \geq 1] = 1 - (1 - \lambda)^{\Delta},$$

where λ is the total mining rate (i.e., the inverse average block time) and Δ is the average network delay. The percentage of hashrate necessary to execute a standard 51% attack (also known as the “attack threshold”) is a consequence of Equation (2) of (Dembo et al., 2020):

$$\beta < \frac{1-\beta}{1+(1-\beta)\lambda\Delta}$$

$$\Downarrow$$

$$\beta < \frac{\lambda\Delta+2}{2\lambda\Delta} - \frac{1}{2}\sqrt{\frac{\lambda^2\Delta^2+4}{\lambda^2\Delta^2}}, \text{ assuming } \lambda\Delta > 0.$$

From our calculations based on data collected between January and June 2021, the effective computational power of the Bitcoin network was only 98.68% of its theoretical maximum power, due to the natural latency of the network. In other words, miners were operating on out-of-date information 1.32% of the time, thereby wasting their time. This means that **the actual cost of a 51% attack on Bitcoin was closer to 49% of the hashrate.** Therefore, contrary to established lore, it does not actually take 51% of the network’s hashing power to mount a successful 51% attack, even when all actors are assumed honest. With the accidental or nefarious introduction of further latency, the hashrate needed can plummet. With just a few minutes of delay, the takeover threshold drops to 40%, and with less than an hour it can be as low as 20%. All this should be taken in the context that just four mining pools already control more than 51% of the hashing power.

In July 2021, Grundmann and Baumstark were able to observe a Sybil attack on the public Bitcoin nodes.[25] The authors neither concluded nor speculated on the purpose of the attack; however, the attack did have the effect of significantly reducing the connectivity of the public Bitcoin network. Our analysis shows that this Sybil attack could have enabled an eclipse attack.

A recent impossibility result for the decentralization of permissionless blockchains like Bitcoin and Ethereum was discovered by Kwon et al.[26] It indicates that for a blockchain to be optimally distributed, there must be a so-called *Sybil cost*. That is, the cost of a single participant operating multiple nodes must be greater than the cost of operating one node. Unfortunately, Kwon et al. conclude that **there is currently no known way to implement Sybil costs in a permissionless blockchain like Bitcoin or Ethereum *without* employing a centralized trusted third party (TTP)**. Until a mechanism for enforcing Sybil costs without a TTP is discovered, it will be almost impossible for permissionless blockchains to achieve satisfactory decentralization.

[25] Matthias Grundmann, Max Baumstark, and Hannes Hartenstein, "Estimating the Node Degree of Public Peers and Detecting Sybil Peers Based on Address Messages in the Bitcoin P2P Network," 2021.
[26] Yujin Kwon et al., "Impossibility of Full Decentralization in Permissionless Blockchains," *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (October 2019).

Distributed Organization and the Power Law

Casual observers often assume that DLTs' peer-to-peer networks are "scale-free".[27] Roughly, a network is scale-free if the fraction of nodes with degree k is k^{-c}, for some constant c. This is a reasonable assumption, since many other natural phenomena such as social networks self-organize in this way. Scale-free properties in peer-to-peer networks are desirable since they provide a good balance between minimizing propagation delays and network connections, allowing the network to reach consensus faster with fewer interconnections.[28] After all, the purpose of the network is to reach consensus on the current state of the blockchain and to disseminate new, unmined transactions to other nodes. The faster this information spreads through the network, the harder it is to exploit information delay by executing an eclipse attack as described in the last section.

Are popular blockchain networks *actually* scale-free? It turns out that there is very little empirical evidence for this. While some blockchains like Ethereum use peer discovery protocols that have theoretical guarantees on consistency,[29] Bitcoin and its derivatives use a custom protocol about which relatively little has been written. The Bitcoin protocol does not provide a means for directly observing the peers of a node, although a node's peers can be indirectly estimated under certain rare conditions.[30]

Bitcoin's network topology is dictated by its peer discovery and connection algorithm, which is a part of the client's implementation and not the protocol itself. Bitcoin Core—by far the most popular Bitcoin client implementation—has hard-coded constants for various parameters that affect peering and, therefore, the network topology. These constants are not officially documented anywhere else, yet drastically affect the topology of the consensus network. The only way to examine those constants (or even know they exist, for that matter) is to interrogate the source code. Therefore, **the only comprehensive reference for the behavior of Bitcoin nodes is the source code of its most popular client.**

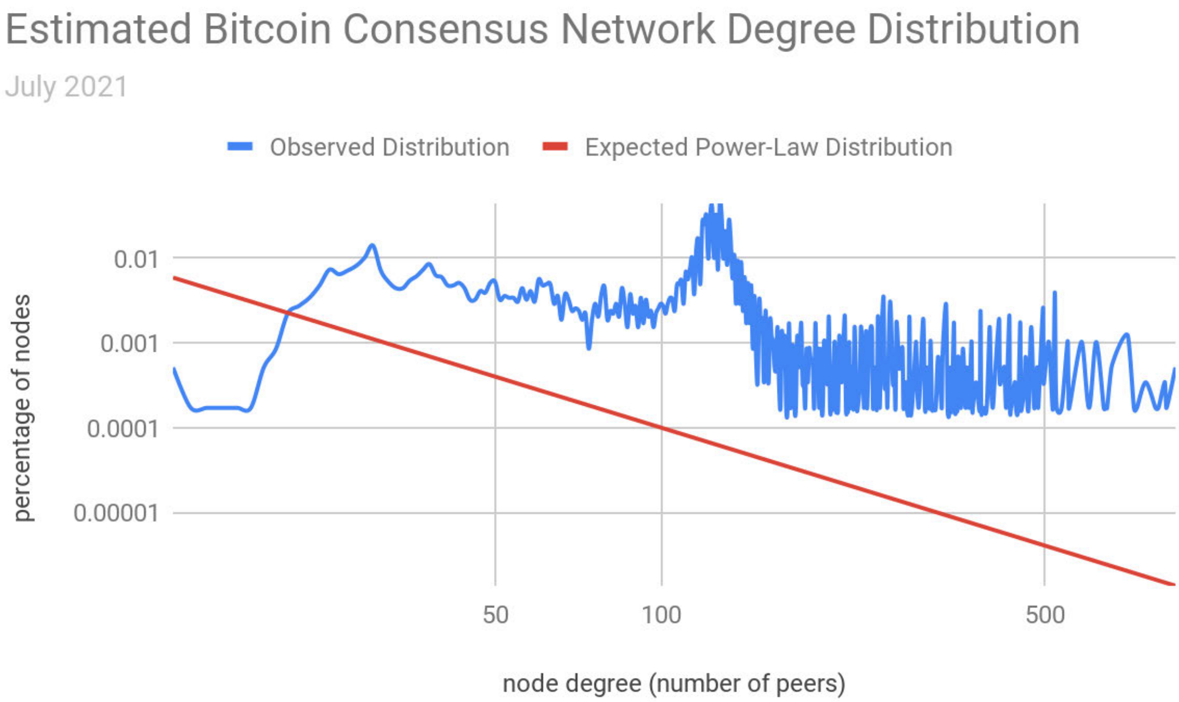
The cap on the number of known peer addresses that are shared with other peers is hard-coded to 23% or 1,000, whichever is smaller. Bitcoin Core does not enable *network address translation* (NAT) traversal or *Universal Plug and Play* (UPnP) by default, so if a

[27] Victoriano Izquierdo, "Centralized or Decentralized? Free Scale Networks!," *Medium*, August 19, 2017.
[28] Cohen and Havlin, "Scale-Free Networks Are Ultrasmall," *Physical Review Letters*, Volume 90 Issue 5, (February 7, 2003).
[29] Petar Maymounkov and David Mazières, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," 2002.
[30] Matthias Grundmann, Max Baumstark, and Hannes Hartenstein, "Estimating the Node Degree of Public Peers and Detecting Sybil Peers Based on Address Messages in the Bitcoin P2P Network," 2021.

Bitcoin node is run without a public IP address (e.g., on a home network or behind a firewall), it will not be able to receive incoming connections from other peers. These “non-public” Bitcoin nodes are able to make only outgoing connections, which are capped at eight. The “public” Bitcoin nodes that *do* accept incoming connections cap their peer count at 125. The Bitcoin client implementation also attempts to maximize the diversity of its peers by limiting the similarity of its peers' IP addresses.[31] Therefore, while the public nodes do interconnect with each other using a modified form of preferential attachment[32]—and therefore should have scale-free properties—the non-public nodes act as approximately regular-degree spokes around the hub of public nodes.

We know that the diameter of almost every random scale-free graph is very small:[33] $\log n \div \log \log n$, which for Bitcoin would place its diameter at five. The Bitcoin Core client has a hard-coded delay of two minutes before it gossips new verified blocks to a peer. Therefore, if Bitcoin were scale-free, we would expect an average block propagation delay of 10 minutes. However, we regularly observe block propagation delays of less than 10 minutes, suggesting that the graph is not in fact scale-free. Our crawls of the Bitcoin network suggest that the diameter is closer to four. This evidence supports our supposition that **a dense (possibly non-scale-free) subnetwork of public nodes is largely responsible for reaching consensus and communicating with miners.** This hypothesis is supported by empirical estimates of the degree distribution.

[31] Bitcoin Core will initiate at most only one peer connection to an IP address in each 16-bit CIDR block.
[32] Albert-Laszlo Barabási and Reka Albert, “Emergence of Scaling in Random Networks,” *Science* 286, no. 509 (1999).
[33] Béla Bollobás and Oliver Riordan, “The Diameter of a Scale-Free Random Graph,” *Combinatorica* 24, no. 1 (2004): 5–34.



There is a peak in the degree distribution at 125 peers, since this is the default cap for the Bitcoin Core client. Nodes with more peers are either running a different or modified Bitcoin client.

By crawling the Bitcoin network and querying nodes for known peers, we can estimate the number of public Bitcoin nodes (i.e., nodes actively accepting incoming connections). From crawling the Bitcoin network throughout 2021, we estimate that the public Bitcoin nodes constitute only 6–11% of the total number of nodes. Therefore, **the vast majority of Bitcoin nodes do not meaningfully contribute to the health of the Bitcoin network**. We have extended the Barabási–Albert random graph model to capture the behavior of Bitcoin peering. This model suggests that at the current size of the Bitcoin network, at least 10% of nodes must be public to ensure that new nodes are able to maximize their number of peers (and, therefore, maximize the health and connectivity of the network). As the total number of nodes increases, this bound approaches 40%.

Network Centrality

In the previous section, we investigated how a DLT's network of nodes can affect centralization. But what about the actual underlying network infrastructure? For at least the past five years, **60% of all Bitcoin traffic has traversed just three ISPs.**[34] As of July 2021, about half of all public Bitcoin nodes were operating from IP addresses in German, French, and US ASes, the top four of which are hosting providers (Hetzner, OVH, Digital Ocean, and Amazon AWS). The country hosting the most nodes is the United States (roughly one-third), followed by Germany (one-quarter), France (10%), The Netherlands (5%), and China (3%). Moreover, at the same time, approximately half of all Bitcoin traffic was routed through Tor.[35] This is yet another potential surface on which to execute an eclipse attack, since the ISPs and hosting providers have the ability to arbitrarily degrade or deny service to any node. Traditional Border Gateway Protocol (BGP) routing attacks have also been identified as threats.[36]

The underlying network infrastructure is particularly important for Bitcoin and its derivatives, since all Bitcoin protocol traffic is unencrypted. Unencrypted traffic is fine for transactional and block data, since they are cryptographically signed and, therefore, impervious to tampering. However, **any third party on the network route between nodes (e.g., ISPs, Wi-Fi access point operators, or governments) can observe and choose to drop any messages they wish**. Say Alice wants to transfer ₿1 to Bob. She creates a transaction for the transfer, digitally signs it, and submits it to a node for propagation throughout the network. The transaction is not yet confirmed; it is in a limbo called the *mempool.* Alice's node will gossip the transaction to its peers until the message eventually reaches a node associated with a miner (or, more likely, a mining pool). The miner can then choose to include the transaction in a block. Once a block with Alice's transaction is mined, it is passed back a node to be gossiped back through the rest of the network. At any point in this process, a malicious node, miner, or *intermediary on the network* can choose to forgo gossiping the transaction before it is mined. If a mining pool's nodes are not sufficiently connected to the dense subnetwork of public nodes described in the previous section, then this sort of attack is easier.

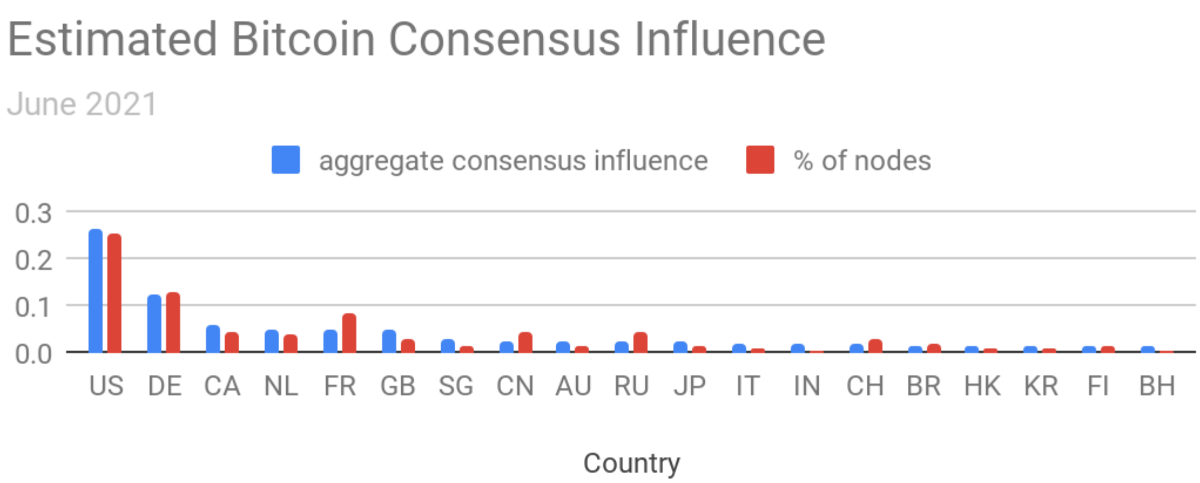
The Bitcoin protocol also allows nodes to be run as Tor hidden services. In fact, **Tor is now more popular than any other AS—or network provider—in Bitcoin, routing traffic for about 20% of Bitcoin nodes.** The next largest AS is AS24940 from Germany, constituting

---

[34] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," *IEEE Symposium on Security and Privacy* (2017).
[35] Osato Avan-Nomayo, "Bitcoin network node count sets new all-time high," *Cointelegraph*, July 15, 2021.
[36] Muoi Tran et al., "A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network," *IEEE Symposium on Security and Privacy* (2020).

only 10% of nodes. This is concerning[37] because a malicious Tor exit node can modify or drop traffic similar to an ISP, as described above. Over the past year, a malicious actor (widely believed to be from Russia) used a Sybil attack to gain control of up to 40% of Tor exit nodes. The attacker used the nodes to rewrite Bitcoin traffic.[38]

We propose a new metric that captures the amount of influence a node has on the consensus of the entire network based on its topological position: *consensus influence*, equal to the node's *eigencentrality*.[39] A node's consensus influence is a function of the consensus influence of its peers; nodes with more influential peers are themselves more influential. The higher this value, the more influence a node has on consensus. Another property of this definition is that the higher a node's consensus influence, the more gossip protocol messages that will pass through it. This metric can be calculated using the principal eigenvector of the network's adjacency matrix. As expected, **the two countries with the highest percentage of non-Tor nodes, the United States and Germany, have the highest aggregate consensus influence in Bitcoin.**

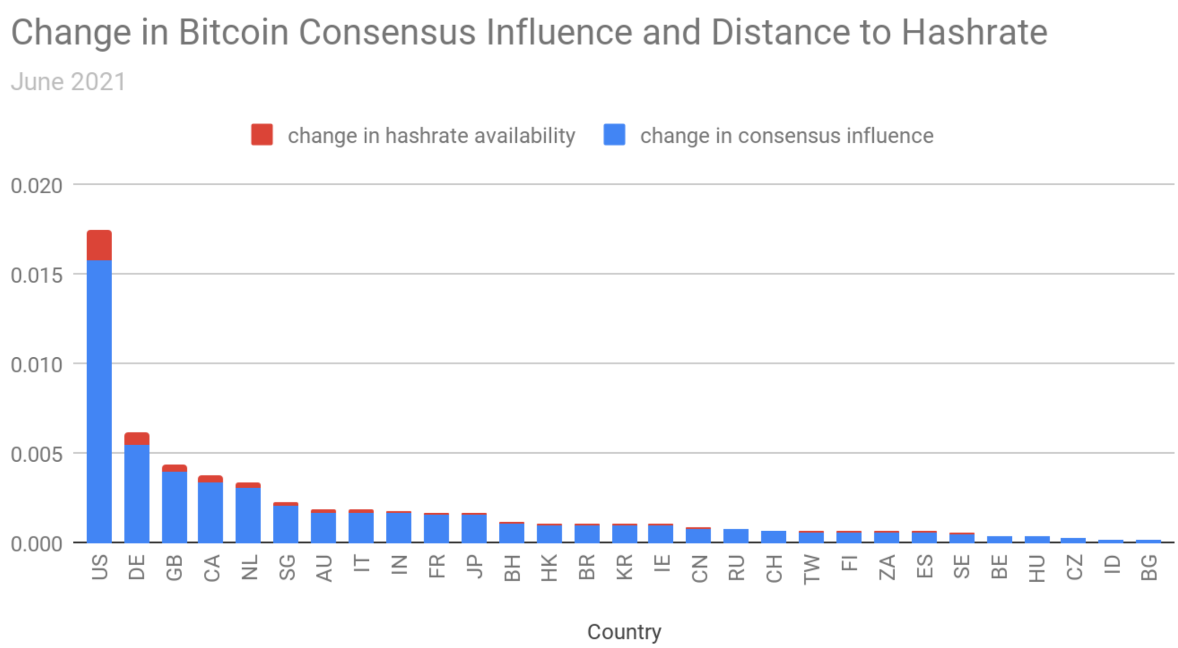


Consensus influence must be estimated for Bitcoin using a combination of crawl data and a probabilistic model of the topology since Bitcoin clients do not explicitly reveal their peers.

We would like to quantify the extent to which a country that unilaterally blocked all Bitcoin traffic could affect the system. We can calculate this effect on node consensus versus the effect on "hashrate availability", which we define as the estimated network delay between a node in the consensus network and all of the miners in the network, normalized by their hashrate. The lower the hashrate availability of a node, the quicker its messages will be

[37] Alex Biryukov and Ivan Pustogarov, "Bitcoin over Tor Isn't a Good Idea," *IEEE Symposium on Security and Privacy* (2015).
[38] Nusenu, "Tracking One Year of Malicious Tor Exit Relay Activities (Part II)," *Medium*, May 8, 2021.
[39] Mohammed J. Zaki and Wagner Meira, Jr. (2014). *Data Mining and Analysis: Fundamental Concepts and Algorithms*. Cambridge University Press. ISBN 9780521766333.

transmitted to and from the miners. We first estimate the global distribution aggregate consensus influence, as in the previous chart. Next, for each country, we remove that country and calculate the new distribution of consensus influence among the remaining countries. We quantify the change by comparing the distributions' relative entropy (Kullback–Leibler divergence). This is depicted as the blue bars in the following chart. We repeat this process calculating instead the change in hashrate availability, depicted as the red bars in the chart. Larger blue bars indicate countries whose removal would have the most significant effect on the resulting consensus network topology. Larger red bars indicate countries whose removal would have the most significant effect on the other countries' communications access to hashrate.



Software Centrality

As discussed earlier, it is vital that all DLT nodes operate on the same latest version of software, otherwise, consensus errors can occur and lead to a blockchain fork. Software differentials and vulnerabilities regularly cause consensus errors. For example, on August 24, 2021, a bug in an older version of the popular Ethereum client Geth was hastily patched.[40] However, participants in the Flexpool, BTC.com, and Binance mining pools continued to use older, unpatched versions of the software. On August 27, 2021, the inconsistent patching led to a consensus error that forked the Ethereum blockchain.[41] On October 25, 2021, a vulnerability in all prior versions of Geth was discovered that permitted a carefully crafted peer-to-peer message to inflict a denial-of-service attack on the receiving node.[42] From our crawls of the Bitcoin network, we observe that **21% of Bitcoin nodes are running an old version of the Bitcoin Core client that is known to be vulnerable.**

While software bugs can lead to consensus errors, we demonstrated that overt software changes can also modify the state of the blockchain. Therefore, the core developers and maintainers of blockchain software are a centralized point of trust in the system, susceptible to targeted attack. There are currently four active contributors with access to modify the Bitcoin Core codebase,[43] the compromise of any of whom would allow for arbitrary modification of the codebase. Recently, the lead developer of the $8 billion Polygon network, Jordi Baylina, was recently targeted in an attack with the Pegasus malware,[44] which could have been used to steal his wallet or deployment credentials.

The blockchain client implementation is not alone in its importance—the entire ecosystem of blockchain software poses a risk of consensus errors and differentials. For example, cryptocurrency traders must decide whether to use a non-custodial wallet (i.e., to manage and store their own credentials in a local digital wallet) versus escrowing their credentials in a centralized custodial exchange. The majority of users appear to do the latter. This choice is not simply about the convenience of delegating management to a third party; it is about whether one trusts a centralized third party versus one's own security hygiene and the developers of one's non-custodial wallet.

---

[40] Christine Kim, "Ethereum's Most Popular Software Client Issues Hotfix to High Severity Bug," *CoinDesk*, August 24, 2021.
[41] Joanna Ossinger, "Ethereum Weathers Bug that Underlines Possible Blockchain Risks," *Bloomberg*, August 30, 2021.
[42] Martin Holst Swende, "CVE-2021-41173: DoS via maliciously crafted P2P message," `ethereum/go-ethereum`, *GitHub*, October 25, 2021.
[43] Brandy Betz, "2 Prominent Bitcoin Core Contributors Step Away From Their Roles," *CoinDesk,* December 10, 2021.
[44] John Scott-Railton et al., "Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," *The Citizen Lab*, April 18, 2022.

We generated software bills of materials (SBOMs) and dependency graphs for the major clients for Bitcoin, Bitcoin Cash, Bitcoin Gold, Ethereum, Zcash, Iota, Dash, Dogecoin, Monero, and Litecoin. We then compared two dependency graphs based on the clients' normalized edit distance.

	Bitcoin	Dash	Bitcoin Cash	Dogecoin	BTCGPU	Litecoin	Monero	Zcash	IOTA	Geth
Bitcoin	1.00	1.00	0.99	0.99	0.99	0.99	0.95	0.92	0.90	0.90
Dash	1.00	1.00	0.99	0.99	0.99	0.99	0.95	0.92	0.90	0.90
Bitcoin Cash	0.99	0.99	1.00	0.99	0.99	0.99	0.95	0.92	0.90	0.88
Dogecoin	0.99	0.99	0.99	1.00	1.00	1.00	0.95	0.93	0.90	0.89
BTCGPU	0.99	0.99	0.99	1.00	1.00	1.00	0.95	0.93	0.90	0.89
Litecoin	0.99	0.99	0.99	1.00	1.00	1.00	0.95	0.93	0.90	0.89
Monero	0.95	0.95	0.95	0.95	0.95	0.95	1.00	0.92	0.91	0.92
Zcash	0.92	0.92	0.92	0.93	0.93	0.93	0.92	1.00	0.94	0.88
IOTA	0.90	0.90	0.90	0.90	0.90	0.90	0.91	0.94	1.00	0.91
Geth	0.90	0.90	0.88	0.89	0.89	0.89	0.92	0.88	0.91	1.00

Our edit distance metric is calculated by comparing the relative depths of all shared dependencies in their dependency graphs. If the depth of a shared dependency is different between two dependency trees, then we say that they have an edit distance of the inverse of the minimum depth minus the inverse of the maximum depth. For all nodes that are in one dependency graph but not the other, the edit distance is the inverse of the depth of the node. We then normalize the total edit distance by the sum of the inverse depths of all dependencies in each graph. A value of 0.0 means that the graphs are completely different and a value of 1.0 means that the graphs are identical.

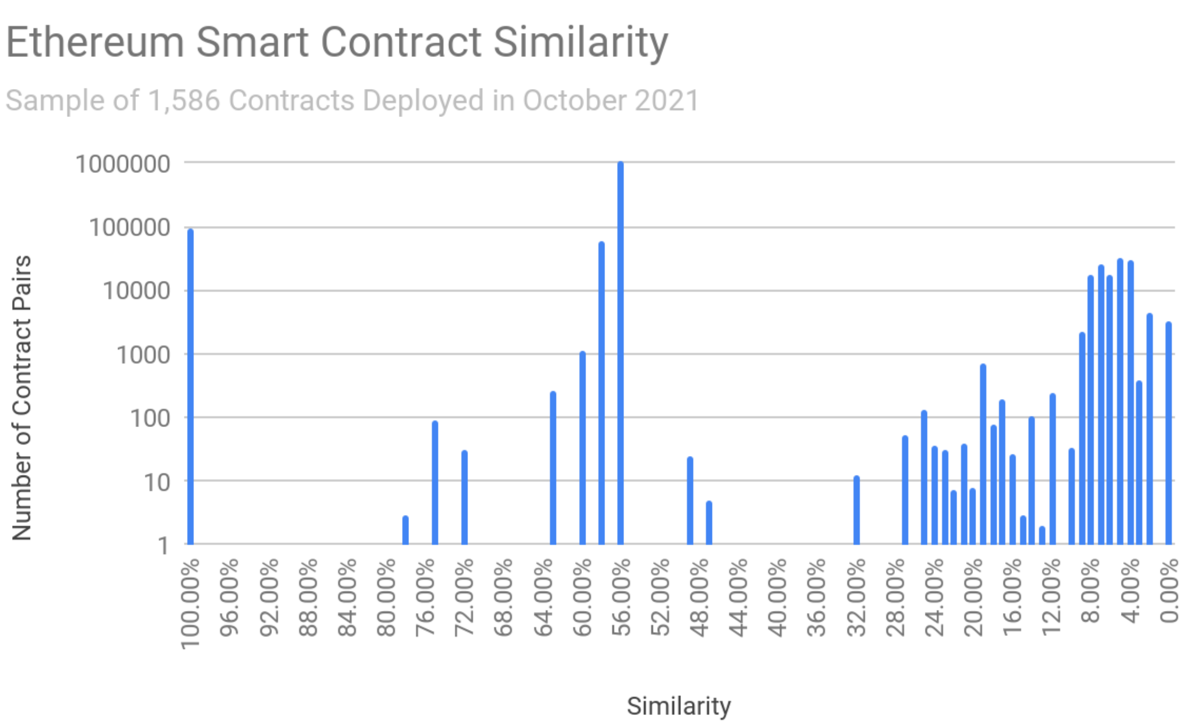
As expected, Bitcoin forks and derivatives remain nearly identical to Bitcoin. Surprisingly, Monero, Zcash, and Geth—which were all independently developed—are also very similar to Bitcoin.

As mining pools are increasingly necessary for PoW mining to be profitable, the centralization and security of their associated infrastructure are increasingly important. The most popular Bitcoin mining pool, AntPool, distributes client software to its miners in the form of black-box, closed-source Windows binaries. **To the best of our knowledge, there has never been a third-party security assessment of these tools.** ViaBTC, one of the top four Bitcoin mining pools, has open-sourced its client code. The system is complex, is written in C, and includes many historically difficult-to-implement components in a language like C. For example, it includes handwritten parsers that process external web requests. **Any remote code execution vulnerability in a mining pool client would allow**

an attacker to either deny service to the mining pool (i.e., reducing the overall hashrate) or redirect the hashrate toward a 51% attack.

On-chain software is also susceptible to code reuse and vulnerabilities. For example, the Ethereum smart contract ecosystem makes heavy use of code reuse and sharing to implement common features that are not natively available in the common language frameworks. Most contracts use the OpenZeppelin library for things like mathematical operations with overflow/underflow detection and standard token API implementations.

We sampled 1,586 smart contracts deployed to the Ethereum blockchain in October 2021, and compared their bytecode similarity, using Levenshtein distance as a metric. One would expect such a metric to *underestimate* the similarity between contracts, since it compares low-level bytecode that has already been transformed, organized, and optimized by the compiler, rather than the original high-level source code. This metric was chosen both to act as a lower bound on similarity and to enable comparison between contracts for which we do not have the original source code. **We discovered that 90% of the Ethereum smart contracts were at least 56% similar to each other.** About 7% were completely identical.



Ethereum contract bytecode contains embedded metadata such as hashes of the original source code as well as compilation configuration details. For example, this hash will vary if a single source code file is compiled twice with different indentations. These hashes *were* *not* stripped from the binaries before performing the above comparison, nor were any constant operands (e.g., hard-coded contract addresses). This means that the true *semantic* similarity between the contracts could be much higher than pictured. This is because two codebases that vendor or copy/paste similar library code (e.g., OpenZeppelin or SafeMath, which are very popular) will be more similar if the hashes are ignored.

Conclusions

In this report, we identified several scenarios in which blockchain immutability is called into question not by exploiting cryptographic vulnerabilities but instead by subverting the properties of a blockchain's implementation, networking, or consensus protocol. A subset of a blockchain's participants can garner excessive, centralized control over the entire system. The majority of Bitcoin nodes have significant incentives to behave dishonestly, and in fact, there is no known way to create *any* permissionless blockchain that is impervious to malicious nodes *without* having a TTP. We provided updated data on the Nakamoto coefficient for numerous blockchains and proposed a new metric for blockchain centrality based on nodes' topological influence on consensus. A minority of network service providers—including Tor—are responsible for routing the majority of blockchain traffic. This is particularly concerning for Bitcoin because all protocol traffic is unencrypted and, therefore, susceptible to attacker-in-the-middle attacks. Finally, software diversity in blockchains is a difficult problem in terms of both upstream dependencies and patching.

Acknowledgements

This report was written by Trail of Bits based upon work supported by DARPA under Contract No. HR001120C0084 (Distribution Statement A, Approved for Public Release: Distribution Unlimited). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA. Many thanks to Molly White, Josselin Feist, and Artem Dinaburg for their helpful feedback.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Jurat Blockchains

JURAT

March 3, 2023

Via email to DARD-FTAC-RFI@nitrd.gov

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

Re: RFI Response: Digital Assets R&D Agenda

Dear Deputy General Counsel Wallace:

I write as the C.E.O. of Jurat Blockchains, a U.S.-based research and development company creating technologies to support the rule of law and enable due process in blockchain transactions.

Founded in 2020, our company is a collaboration between blockchain engineers and seasoned attorneys who share a passion for consumer protection and a deep concern about the larger lawlessness problems confronting regulators and mainstream commercial adopters. Our products make blockchains governable by regulators and other officials while strictly maintaining the norms and benefits of decentralization for all users.

As an early entrant in the blockchain law enforcement space, Jurat has a unique perspective to share regarding Topics 2 (research opportunities that could be introduced to support efforts to mitigate risks from digital assets), Topic 3 (R&D priorities that can protect U.S. national interests) and Topic 3 (setting standards to help advance democratic values in the use and governance of digital assets).

[redacted]

A. Research opportunities and priorities for on-chain legal enforcement

Technologies that facilitate on-chain enforcement of the law will be increasingly vital to the commercial and security interests of the United States as blockchain ascends. The mass of commerce driving our economy is predicated on laws, often complex and evolving, which rely on governments and courts for their enforceability. If blockchain is to attract mainstream commerce and become its backbone, which is a core goal for the industry, blockchains must provide the certainty of effective law enforcement that commerce already enjoys and which our economy demands. Similarly, absent effective law enforcement, blockchain technology is easily perverted into a tool that threatens core American ideals and American safety. For example, this threat is already obvious from the fact that North Korean hackers are using ransomware to extort bitcoin from American companies and citizens which it then uses to finance its development of weapons of mass destruction.[1] In short, the United States should prioritize R&D into technologies that can interweave American ideals into decentralized protocols so that they remain beneficial instead of being weaponized against our interests and freedoms.

A recently filed federal court case, The JuratBTC Blockchain v. Andreyev, et al., 1:23-cv-00779 (N.D.Ill.), demonstrates the potential for on-chain enforcement technologies to advance U.S. interests in the next generation of blockchains.

In that case, individual miners operating the JuratBTC blockchain brought suit against 16 international criminals sanctioned by the Office of Foreign Asset Control pursuant to Executive Orders. The defendants included the cryptocurrency mixer Blender.IO[2] (used by the notorious cyber-crime organization Lazarus Group), Anton Andreyev[3] (a Russian hacker who worked to interfere in American elections), and Jiadong Lee, aka "Blackjack1987"[4] (a member of a crime ring that laundered over $100mm in cryptocurrency stolen by North Korean hackers), among others. The miners (myself among them) sought to freeze these Defendants' accounts so that their blockchain would remain compliant with the U.S. sanctions laws. The miners were able to do so because the JuratBTC blockchain (a bitcoin fork) incorporates Jurat-developed technologies that connect courts with blockchains.

---

[1] E.g. https://home.treasury.gov/news/press-releases/jy0768 (U.S. Treasury sanctions against the BTC wallets of the Lazarus Group) (last checked 3/2/23).

[2] Id.

[3] https://home.treasury.gov/news/press-releases/sm1118 (last checked 3/2/23).

[4] https://home.treasury.gov/news/press-releases/sm924 (last checked 3/2/23).

[redacted]

On February 21, 2023, the federal court entered a temporary restraining order (TRO) to freeze the accounts of these 16 sanctioned individuals.[5] The JuratBTC nodes accessed the court's order via the U.S. PACER docketing system and then autonomously implemented the court's ruling by blocking the cryptocurrency in the sanctioned accounts.

This on-chain enforcement process remained decentralized at each step. No central authority controlled the blockchain. Rather, citizens applied to the courts to enforce the law and the decision was made in accordance with U.S. constitutional due process protections for users of the blockchain. Similarly, the court was not empowered to control the blockchain (no government official has direct control, nor is there an official key). The nodes themselves accessed the PACER system to review the court's order, with each node satisfying itself that the action (freezing the funds) was legally authorized before processing the transaction. No intermediary was needed nor involved as the nodes used a Jurat-developed protocol to understand the exact transaction that the court had ordered.[6]

The result is historic. It represents the first time that a public blockchain has been able to comply with the requirements of U.S. laws and block sanctioned accounts. The same accounts on the Bitcoin blockchain were emptied by these 16 sanctioned individuals as the Bitcoin miners not only accepted their transactions but also adopted (and continue to accept) the ledger reflecting them. The Bitcoin miners thereby enabled the evasion of sanctions by these international criminals.

In this case, the JuratBTC miners are the ones who invoked the court (acting out of a civic mindset to support law enforcement and to protect themselves from becoming involved in sanctions evasion). Nevertheless, it is also true that the same sort of action can be taken by the government officials who are charged with enforcing laws and regulations, using their usual procedures. For example, police routinely resort to courts to obtain warrants to seize items involved in criminal activity. The same procedure can result in an effective judicial warrant to seize digital assets on-chain. Likewise, regulators could obtain an injunction against a smart contract like Tornado Cash, effectively shutting down its operation.[7] This injunctive enforcement tool can be used in a more targeted fashion than sanctioning all accounts that

[5] See The JuratBTC Blockchain v. Andreyev, et al., 1:23-cv-00779 (N.D.Ill.), Dkt. No. 9, available at https://jurat.io/wp-content/uploads/2023/02/9.TRO-Signed.pdf (last checked 3/2/23).

[6] The technology for enforcing court orders without intermediaries is discussed in the Jurat Whitepaper (available at www.jurat.io/whitepaper) and summarized on the Jurat website (https://jurat.io/technology/) and in a light paper (https://drive.google.com/file/d/18c59SrBAV5J3olAByt2qqVmdS_ORR7n3/view).

[7] To some proponents, any method for officials to exert authority over digital assets would violate the norms of decentralization. But the position lacks justification. Persons expressing this concern also own

[redacted]

interact with a smart contract, and therefore protects liberty on-chain consistent with the public's legitimate law enforcement interests.

It is important to note that the same technology for providing due process and law enforcement on-chain also protects consumers and supports mainstream commerce to adopt the blockchain and automated smart contracts. Not only can court orders be entered to freeze transactions but they can also effectuate transfers between blockchain accounts, for example, by awarding damages, returning stolen property, or restoring lost property to the holder of the account. Court orders can also trigger contract calls to effectuate contract remedies and, where appropriate, reform smart contracts to better reflect the intent of the contracting parties. For a more fulsome discussion of how on-chain enforcement can support the mainstream adoption of digital assets and smart contracts while preserving decentralization see the Jurat Whitepaper, supra note 6, at pages 4-8.

B. Advancing democratic values in the use and development of digital assets

I also wish to note the importance of incorporating due process protection technologies like Jurat into the payment rails underlying any Central Bank Digital Currency (CBDC). There is great potential for CBDC to cement the U.S.'s position as a world economic leader and also to augment our commercial banks' efforts towards financial inclusion. However, CBDC also holds a great risk for abuse of power by government officials and by private financial interests should banks become the locus of CBDC issuance. The ability for a government to observe, promote (or nudge) and prohibit economic activity on a person-by-person basis has never existed in a free society. The potential for such power to fuel totalitarianism is far too great to be left unchecked.

Accordingly, should the U.S. place the power of the dollar into a CBDC, no government official or private bank should ever have direct control over any citizen's holdings or expenditures. Courts must always be in the loop to ensure due process and protect each citizen's freedoms. This is true not only for prohibitions on an individual's use of funds but, also, the provision of funds (such as in economic development and poverty elimination programs). Economic freedom is fundamental to every other freedom we enjoy as U.S. citizens, just as economic compulsion can be misused to discourage the exercise of free speech and religion, and to inflict undue punishments against disfavored individuals and organizations. Courts are

houses, cars and bank accounts, all of which the government leaves alone. Due process is an excellent protector of property rights, so limiting on-chain enforcement to valid court orders will keep digital property as sacrosanct as physical property.

[redacted]

the institution that humans have developed to ensure rule of law. They are the only organ that stands between the government's inestimable powers and the individual citizen.

To conclude, some of the "guardrails" that the Whitehouse seeks to discover for blockchain technology already exist in the U.S. Constitution and our courts have been researching and developing procedural safeguards for centuries. Our judicial system knows how to protect our liberties and resolve disputes in a manner that enforces U.S. policies, supports beneficial economic development and ensures justice to individual citizens. U.S. R&D efforts should focus on the best methods to incorporate the judicial system at the protocol level into the next generation of blockchains.

Sincerely,

[redacted]

Mike Kanovitz
CEO Jurat Blockchains

[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Knox Networks

Office of Science and Technology Policy (OSTP)
Response to "Request for Information: Digital Assets Research and Development"

Responses Submitted on behalf of the Organization:	Knox Networks
Organization Type:	Industry
Members writing this Response:	Parul Sharma, [redacted]

1. *Goals, sectors, or applications that could be* ***improved with digital assets and related technologies****:* Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered. This includes explanations of the current limitations in how those goals, sectors, and applications are currently advanced with limited use of digital assets and related technologies, and how increased or better use of digital assets could provide a specific advantage over existing approaches in advancing these objectives. Where relevant, respondents are encouraged to justify how digital assets provide unique value for advancing that goal, sector, or application compared to the use of traditional databases or other technologies (*e.g.,* as outlined in *National Institute of Standards and Technology Internal Report 8202,* Figure 6).

   Response:

   Goals of Digital Asset Adoption by the U.S.
   As the reserve currency of the world and a global economic leader, U.S. policymakers need to have a central role in establishing the norms of international commerce. A significant area of initial focus should be the development of a government backed digital asset. In so doing, the U.S. can address the major obstacles to mass adoption: lack of standards in interoperability, privacy and scalability. Properly deployed, the U.S. backed digital asset will embed in its design solutions for mass adoption: interoperability, privacy and scalability while compatible with the two-tier banking system. Delay in developing its own government backed digital asset will allow nations with other models to innovate ahead of the United States, and become the de facto standard-setter,potentially leading to outcomes that disfavor U.S. policy priorities and chill the U.S.-based private sector. Instead, the United States should play a decisive, timely, and leading role in this area, focusing on interoperability, privacy, security, and scalability of any government backed digital asset, that still preserves a two-tier banking system.

   1. The Importance of Interoperability
      In a global economy, it is crucial to develop an interoperable model compatible with other solutions that may have varying degrees of privacy, governance standards, or security precautions. One of the core tenets of money is its ability to be used as a medium of exchange, and easier integration with platforms. Therefore, the U.S. government should work closely with emerging U.S.-based private sector leaders, various international organizations, trade blocs, currency unions, and regulators to establish global standards and interoperability definitions for all government backed digital asset systems. Importantly, the United States should focus on encouraging the use of financial standards (e.g. ISO-20022) that allow for interoperability between various payment networks.

   2. The Importance of a Privacy Protection Standards
      Another factor slowing the mass adoption of digital assets is the perceived lack of consumer protection and privacy for data related to digital asset transactions. A solution with programmable money should allow consumers to own their data/hold their PII separately in their wallets and share it in a secure manner upon consent. Programmable money should be pseudonymous, entirely separate from the consumer's data. Analytics can be extracted at the bill level and prove helpful in tracking net-value volume flows between participants, calculating holding periods for each digital dollar, and generating information for suspicious activity reports, among other use

cases. This solution still captures the PII and any KYC requirements necessary to satisfy existing legal obligations on financial institutions, but done in a privacy-enabled way through encryption techniques such as zero-knowledge proofs.

3. The Importance of Scalability
   Scalability is another concern when thinking about mass adoption of digital assets, especially considering current distributed ledger technology networks which face transaction bottlenecks due to their replicated nature. For example, current transaction rates do not scale to accommodate retail payments of the U.S. economy. Proposed improvements to the payments system focus on widespread promotion of faster database processing. For example, FedNOW promises improvements to faster processing with its improvements to FedWire, but relies on legacy ways to think about batched ownership of currency and increasing the throughput of just one data source. In contrast to the kind of improvements offered by FedNOW, file-based programmable money **– non-blockchain technology that can be used for digital assets –** captures ownership and transfer data. More specifically, file-based programmable money allows each dollar bill in circulation to be its own ledger, a cryptographic proof with embedded settlement and transaction history. Furthermore, the file-based programmable money would be backed by reserves necessary for the relevant regulatory regime (e.g., bank deposits, etc.).

4. The Importance of Compatibility with the Two-Tiered System
   One last, but certainly not least, factor of facilitating the mass adoption of digital assets would be to have the solution work within the two-tier banking system. Using the two-tiered nature of the banking system as it is today and leveraging commercial banks to be participants in operating the system allows for greater efficiencies in transaction throughputs and more efficient distributions of capital into the economy. Radical departures from the existing financial system are unlikely to generate mass adoption. Indeed, encouraging mass adoption to a platform that evolves from the current financial system is easier from a regulatory and efficiency standpoint, but still offers the potential for reaping the benefits digital assets provide, such as opportunities for participation in the digital economy and increased financial inclusion.

Digital Assets Provide the Potential for New Financial Products and Services
The potential for financial products and services under a file-based programmable money system is tremendous. File-based programmable money could enable more efficient and transparent real-time payments on a global scale, with reduced settlement fees for single or dual-currency exchanges and more limited foreign exchange risk. Corporations could also manage holdings more easily when moving funds across borders, improving liquidity and limiting exposure. This technology also allows for more transparency and auditability with transactions, which could help in combating fraud and corruption.

In addition, file-based programmable money can be used for a variety of financial products, including treasury securities and repurchase agreements. If this technology is used by established clearinghouses, it could have the potential to drastically reduce settlement times for securities transactions, even allowing post-trade events to take place in near real-time. Because this type of technology keeps a running record of ownership history, it could also drastically reduce the chance of settlement breaks or data discrepancies on a trade, which often result in costly, manual reconciliation.

The Importance of Cash Like Properties In Digital Assets
When we think about current mass adoption of currency, cash has proven to be the main choice across different regulatory and financial regimes. Some current digital asset technologies contain risks that prevent it from providing the benefits of cash. Given this, it is important that there is a digital equivalent to what cash represents to current financial systems and their consumers. For example, any government backed digital asset should have offline capabilities and be designed to achieve similar features as

physical cash with as minimal drawbacks as possible. Because physical cash can be used offline, so should government backed digital assets.

While offline transactions open risks of double spending in the system, a solution such as file-based programmable money can provide sufficient mechanisms to guard against those liabilities within the financial system, and bad actors can be sanctioned and prosecuted. Further, the victims of fraud or point of sale purchasers seeking recourse should be able to avail themselves of the same or similar protections afforded to today's card users who may be unsatisfied with purchases. A similar framework of consumer protections would be necessary and likely need to be attached at the financial intermediary level - the consumer wallet level and regulated by a federal entity such as the Consumer Financial Protection Bureau, Financial Criminal Enforcement Network (FinCEN), or the FDIC. But more importantly, the offline capabilities of a system should enable resilience to network outages (e.g. natural disasters) where connectivity is unavailable. There are various strategies that can be used to guard against exponential liabilities in an offline situation, including limiting the number of transactions that can be done offline.

Financial Inclusion and the Impact of Digital Assets on Vulnerable Populations

Digital assets such as file-based programmable money can help bridge the gap that exists between millions of underbanked and unbanked individuals in the U.S. and access to proper financial services. It is critical that digital assets be designed with the most underserved communities in mind from the get-go to avoid recreating the same problems that exist in the current financial system. Underserved communities will benefit from all of the services that digital assets provide, but will especially benefit from a digital asset solution that prioritizes (1) the ability to transact without a bank account, (2) the protection of privacy and identity, and (3) the ability to transact payments while offline.

First, file-based programmable money allows users to transact without a bank account. Nevertheless, the technology also allows for proper Anti-Money Laundering/Know Your Customer checks. A non-account-based file-based programmable money system could allow individuals to hold government backed digital assets on mobile devices without the prerequisite of a bank account. Any consumer who is un- or under-banked could have access to well-regulated financial products and services from the traditional banking sector, while still allowing for accountless-usage to reduce hurdles. At the same time however, the design is also compatible with having a bank account – thus, capturing a wide number of users.

Second, using file based programmable money technology allows the use of an embedded digital identity solution that captures personally identifiable information (PII) that are needed to satisfy AML/KYC requirements. This information could be captured in a privacy enabled way (through encryption techniques such as zero-knowledge proofs). This system design preserves the anonymity of using cash, where consumers can act pseudonymously, and potentially selectively reveal information only as required. This way, consumers can own their data on their own devices, and when they share that data, it is done so with minimal exposure.

Third, file-based programmable money also offers an offline solution via peer-to-peer transfers for end users. This helps improve the reliability of the payments system for the most vulnerable communities which may not live in areas with reliable internet connection. This wallet based system would allow for reduced friction between consumers and small businesses in P2P and P2B payments. The offline features of file-based programmable money enable point-of-sale (PoS) transactions despite events when a connection to the internet is lost. This is vital for situations such as a natural disaster, which might otherwise restrict the transfer of value between consumer and merchant. Offline transactions can be transacted using devices available on the market today.

2. *Goals, sectors, or applications where digital assets introduce risks or harms:*
   Information about goals, sectors, or applications where digital assets might introduce risks or harms, and examples of where risks or harms are already being manifested. This includes explanations of direct or indirect impacts on users of digital assets, communities or sectors in which digital assets might circulate or be integrated into services, and non-users (*e.g.,* communities, environment) that may be exposed to risks or harms of digital assets (*e.g.,* ransomware attacks, higher electricity costs, pollution). Where relevant, respondents are encouraged to justify how digital assets are introducing new risks or harms in advancing the underlying goal, sector, or application compared to the use of traditional databases or other technologies.

   Response:

   Digital assets, like all major technologies, may introduce risks and harms to both direct and indirect users of the system. It is important to understand these potential risks to better mitigate them in future system design, in particular for a potential US CBDC.

   In the current digital assets landscape, retail and even institutional users are likely to be most familiar with blockchain-based cryptocurrencies such as Bitcoin or DogeCoin. Many of the concerns that people have regarding digital assets, rightly or wrongly, are colored extensively by the problems that are generally prevalent in, but not exclusive to, cryptocurrencies. As we have seen from the past year, there have been a number of high-profile crypto exchanges and "stablecoins" that have failed to adequately represent themselves and their risks to investors, and have often served as a haven for fraudsters, illicit financing, and ransomware payments.

   Most cryptocurrencies are run on a public distributed ledger technology (DLT). Public DLTs, and especially the Proof-of-Work (POW) consensus mechanism, rightly draws criticism for its extensive environmental impact, with Bitcoin consuming more electricity than Argentina annually. And unlike in a traditional database, there is generally no single administrator in the system that can unilaterally control the actors with a public DLT, leading to a limited number of options for KYC/AML/Sanctions checks on users and thereby potentially allowing for illicit financing.

   Private DLTs, unlike their public counterparts, are networks with trusted verifiers and intermediaries. They can skip most of the concerns around energy consumption because there is no required consensus mechanism, and their use cases are more in-line with traditional databases. Despite this similarity, private DLTs still generally hit scalability issues when transactions per second (TPS) exceed a few thousand, which starts to cause issues in use cases beyond wholesale applications. A potential retail CBDC, especially one in an economy as big as the US, would need to be able to solve the scalability problem, and central banks are already running into performance issues during tests.

   With these problems identified, digital assets also bring a variety of new features to the table, such as smart contracts and improved auditability, that are improvements over the traditional database. Ideally, the problems of current DLT systems should be addressed and their benefits brought over to a CBDC system, but even CBDCs have their concerns.

   Perhaps the most obvious concern many have for a CBDC is that of privacy, or lack thereof. CBDCs should be designed to mirror the current use of cash, and should ideally disaggregate transaction data from user identification data requirements where possible while still allowing for adequate KYC/AML checks. There are a number of countries around the world, most notably China, which are currently piloting a CBDC, and may use that additional information to monitor the activities of its citizens more closely. This may lead to further entrenchment of existing discriminatory practices to political or other dissidents, and even less maliciously may lead to the rise of a "nanny state." Many criticisms of CBDC are geared against fighting this reality, and adequate safeguards will need to be put in place for the US and other economies's CBDCs.

There is also a real concern that a CBDC may introduce additional risk into the banking system by allowing for a central point of failure for payment. A number of the countries who have begun pilot launches of a CBDC, including Nigeria and the Eastern Caribbean Currency Union, have run into non-insignificant hurdles with their system launches. In the case of the ECCU, their entire payment system was offline for several weeks, which would be a paralyzing force to a national economy had it been the primary form of payment. There has always been the risk of a currency impacting perceptions and capabilities of the wider economy, but CBDCs introduce significantly more surface area for something to go wrong in comparison to paper banknotes.

3. *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets:*
This might include information about R&D that helps companies build more environmentally-sustainable digital assets, assist law enforcement in countering illicit financial activity using digital assets, and enable regulators to protect consumers from fraud. This includes opportunities to innovate for equity and privacy with R&D that could help underserved communities harness the benefits of digital assets while being protected from their risks, such as via improvements to digital assets to allow them to better remain accessible, reliable, and secure even when connectivity and end-user device quality are limited.

Response:

Following are the efforts with which federal research can mitigate risks from digital assets:
   1. Choose a digital assets ecosystem that is interoperable, scalable and efficient:
   All of the potential benefits of a CBDC could be better achieved through programmable money (digital cash) technology in an intermediated CBDC model versus through Distributed Ledger Technology.
   2. Choose a digital asset ecosystem that is secure and enables privacy:
   For the CBDC to be operational, it is essential to solve the problems associated with double-spend and double-credit attacks, enable offline payment capabilities and create a barrier to illicit finance. By selecting a digital asset ecosystem that has the above mentioned features and has the capacity to add more features in the future can ensure key requirements are developed to enable regulators to combat financial fraud and to assist law enforcement agencies in countering illicit financial activity using digital assets.
   3. Choose a digital asset ecosystem that can serve a diverse demographic inclusive of the unbanked population:
   The primary benefits of cash are its value as a widely accessible means of non-account-based payment, which programmable money can achieve. A CBDC should extend the benefits of a bearer instrument, a non-account-based system, by allowing for large and small transactions to be facilitated for people of all socioeconomic backgrounds, across borders, and at all times. A CBDC should also enable proactive monetary analytics of the modern economy and its participants. For a CBDC to be suitable for global economic use, solving the problems associated with offline capabilities, and non-custodial wallets while creating a barrier for illicit finance are essential.

4. *R&D that should be prioritized for digital assets:*
Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present. This includes topics for technical research, topics for research in the social sciences and across disciplinary boundaries, and opportunities for hardware and software development. This also includes information about emerging areas that could enable new opportunities to

leverage digital assets, as well as information about technical limitations of digital assets and the associated business models and governance arrangements they often rely upon. Respondents are encouraged to, where relevant, describe how the discussed R&D topic could be useful in helping a potential U.S. CBDC system align with the *Policy Objectives for a U.S. CBDC System.* Respondents are also encouraged to share how the discussed R&D topic could help advance U.S. competitiveness and leadership in the world.

<u>*Response:*</u>

Refer to answers to questions 1 and 6.

5. *Opportunities to advance responsible innovation in the broader digital assets ecosystem:*
Information about opportunities for the United States to advance responsible innovation in the broader digital assets ecosystem, in areas that are adjacent to R&D. This may include programs that could support increased education and workforce training related to digital assets, standards setting efforts that could help advance democratic values in the use and governance of digital assets, and supply chain opportunities to maintain access to the necessary hardware for emerging digital assets.

<u>*Response:*</u>

The US should collaborate with like-minded democracies and allies to help ensure that CBDC requirements are built to align with democratic values. This should include global standards on how CBDCs should be designed to comply with international sanctions and protect due process and the rule-of-law for individuals holding CBDC. In addition, by utilizing the US's standing as the leader of both the free and financial world, the US should help contribute to a common and open standard, thereby democratizing the payments ecosystem. This should serve as a public bulwark against countries which may seek to increase surveillance on their populations via CBDCs.

One of the potential barriers to smoother adoption of digital assets could be lack of clarity on the rules, regulations and standards that may apply to digital assets. The sooner the federal government can articulate such regulations, in a manner that can be incrementally extended in phases, it would enable a more phased and de-risked adoption. These rules should also ensure that the previously mentioned principles of scalability, privacy, security, and interoperability are clearly defined and met.

By ensuring that the CBDC ecosystem compliments the two tier banking system, the central bank can leverage the existing banks and payment interface providers workforce to ensure they are trained on the new technology and standard. Much like the regulatory practices followed by banks on security standards set today (e.g., KYC, AML, etc.). The CBDC ecosystem will also benefit from having banks and their workforce play an active role in ensuring the established CBDC standards are met.

Other than the above the support of increased education and workforce, training will also be required, to ensure smooth operation of the CBDC ecosystems. In particular, communication around these topics to the general public can help alleviate concerns and correct any knowledge-gaps among the population. <u>Unfortunately, CBDC has unfortunately become a topic of misinformation in certain areas of the public, and the government must be proactive in both alleviating the real concerns around CBDC and dispelling the false rumors that surround CBDC</u>.

6. *Other information that should inform the R&D Agenda:*
Information about any other topic, not covered above, that respondents believe is important to inform the development of the National Digital Assets R&D Agenda. This may include ideas for collaborations

between the Federal Government and other entities, as well as proposals that may not yet be feasible with the current state of technology but might become feasible in the next decade**.**

Response:

There are a variety of potential collaborators and emerging technologies which may impact the National Digital Assets R&D Agenda.

For collaborations, it is recommended that the US champion its position as the global leader in finance for implementing standards and promoting interoperability of different payments systems. Projects like the Bank for International Settlements' Project mBridge with China, Thailand, the UAE, and Hong Kong demonstrate the need for international interoperability and desire for buy-in from major economies.

The US should work in collaboration with the world's major economies, especially allies within the G7/EU/USMCA, to minimize the discrepancies between payment systems that would cause friction points for users and business. This includes major financial players within these regions, including their central banks and large private financial institutions. A small-scale example of what this collaboration might look like could be seen through the P27 Nordic Payments initiative, which looks to support a Nordic-wide shared payments infrastructure while still utilizing multiple currencies and while crossing many political boundaries.

In addition, the Agenda could also consider working with major technology players in the payments space for streamlining their payment systems to be interoperable with a potential US CBDC and recommendations for capabilities to improve financial inclusivity. This might include features such as accessibility features and offline payments design, which may be necessary in areas with lesser infrastructure and/or currently experiencing infrastructural outages.

The most important looming technological development is that of commercially viable quantum computing, which may make many current encryption algorithms obsolete. The advent of quantum will pose a challenge to any CBDC, and it will therefore be imperative to set standards and recommendations for flexibility with encryption schemes. This would allow for quantum-resistant encryption algorithms to be swapped in place of current algorithms when quantum computing starts being used outside of labs.

Zero-Knowledge (ZK) Proofs are another technology that is still in the early adoption phase but may be critical in the future of country-wide digital asset systems. ZK proofs are able to prove the validity of information without ever having to reveal the information (e.g. proving to an employer an SSN is valid without having to give the number itself). Currently, ZK proofs are limited in terms of scalability, but further research may be able to get ZK proofs viable for large scale retail use cases.

Combining ZK proofs with concepts such as Self-Sovereign Identity (SSI) allow for an incredibly powerful yet privacy-preserving modern identity solution that could actually *enhance* user privacy over current systems. A simple example of this privacy enhancement could be seen when getting your driver's license checked at the bar - the bar only needs to know the answer to the "is this person over 21?" rather than currently showing all of the data on a driver's license. SSIs, along with related technologies of Verifiable Credentials (VC) and Decentralized Identifiers (DIDs), would allow for user data to integrate with both government and private identification schemas and store their information on their device without unnecessarily needing to expose their data.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Leonard Gricci

From: Lee Gricci
To: DARD-FTAC-RFI
Subject: RFI Response: Digital Assets R&D Agenda
Date: Sunday, January 29, 2023 12:43:21 PM

Dear Members,

This YouTube video (Empowering community-driven governance on Cardano - YouTube) is essential upfront learning as you move forward in the regulatory process for cryptographic and blockchain technologies. "IOG CEO & Founder **Charles Hoskinson** sat down with IOG's Chief Legal Officer **Joel Telpner** to discuss the next steps in the creation of the MBO, particularly around the drafting of a new constitution."

Please consider inviting these two thought leaders as you build out your regulatory framework for the cryptographic and blockchain ecosystem.

Respectfully submitted,

Leonard Gricci
Member of The Public

Sent from Mail for Windows

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Lukka, Inc. ("Lukka")

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

March 3, 2023

Via electronic submission to: DARD-FTAC-RFI@nitrd.gov

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
Executive Office of the President
[redacted]

Re: Request for Information; Digital Assets Research and Development Agenda

Dear Ms. Wallace:

Lukka, Inc. ("Lukka") appreciates the opportunity to respond to the "Request for Information; Digital Assets Research and Development" published by The White House Office of Science and Technology Policy ("OSTP") on January 26, 2023. We support OSTP's belief that responsible innovation and comprehensive research and development are necessary to the ecosystem, and are writing to provide input on how the use of well-designed and authenticated data solutions can aid consumer protection, and improve regulators and policymaker's understanding of the crypto asset ecosystem.

Introduction

Founded in 2014, Lukka serves the most risk mature businesses and governments in the world with institutional grade data and data-based risk management solutions. Lukka bridges the gap between the complexities of blockchain data and traditional regulatory and business needs. Our customers include both Traditional and Crypto-Asset Exchanges and Trading desks, Government Tax Authorities and Regulators, CPA and Accounting Firms, Fund and Financial Auditors, Fund Administrators, Miners, Protocols, individuals, and any other organizations interacting with crypto-assets. Lukka is a global data company, headquartered in Naples, Florida, with offices in New York, Singapore, Switzerland, and team members located around the world.

Lukka has the most comprehensive crypto-asset and exchange coverage in the industry. This depth of coverage ensures there are no information gaps, in assets or marketplaces, that could limit regulatory efforts. Lukka Reference Data is an extensive set of security masters from exchanges and other sources across the crypto ecosystem that standardized crypto-asset names, tickers, trading pairs, spot and derivatives, unique and custom assets such as non-fungible tokens ("NFTs"), and more.

Lukka's core offerings include:

- Enterprise Data Management Suite: a comprehensive set of web-based software and data capabilities built to simplify crypto middle and back-office financial data management, gain/loss calculations, and custom reporting.
- Enterprise Data Products: institutional-quality crypto asset and pricing data solutions to support the unique needs of organizations adopting blockchain data into their core functions.
- The Lukka Digital Asset Classification Standard ("LDACS"): a detailed and comprehensive structure consisting of a five-tier hierarchical taxonomy to improve transparency and efficiency in assessing and analyzing over 90,000 crypto assets, currently.

Our products undergo annual AICPA SOC audits to ensure the highest technology risk standards, and are built with institutional standards that focus on data quality, accuracy & completeness, and managing technology risk. As a result, Lukka is trusted worldwide by top crypto industry participants, including traditional financial institutions, trading platforms, governments, accounting and tax firms, and leading investors.

Lukka has proudly supported the Internal Revenue Service ("IRS") since 2017, where our experts have assisted IRS-Criminal Investigation by performing analysis of virtual currency data sets to reconstruct taxable income calculations. In one instance, this work involved analyzing ~30,000 trades and transfers representing ~65 different crypto-assets across 3 source exchanges. Lukka interacted with IRS exam and counsel teams for purposes of ingesting the data, receiving direction on technical tax issues raised (e.g., airdrops), addressing data gaps, and communicating the results.

Responsible Innovation

As discussed in the Request for Information, OSTP correctly identifies the necessity of research and development in the digital asset and blockchain ecosystem as precursor to responsible innovation. To allow this nearly 16 year old technology to continue to redefine a multitude of industries, while meeting the standards of the regulators, and simultaneously gaining mass market acceptance, it is imperative that solutions built specifically for blockchain and digital assets are responsibly developed by the industry and relied upon by governments.

The backbone of blockchain and crypto is its data - the unimpeachable recordings of transactional histories spread across public networks that anyone can view. But due to the nature of digital assets and the marketplace, it is difficult to keep track of and understand all of that data. Some of the intricacies of this ecosystem bring challenges to participants and regulators alike. For example:

- There are hundreds of unsupervised crypto trading platforms around the world.
- Trading platforms operate 24/7 without standardized ticker symbols, file formats, or valuation processes.
- Crypto transactions occur in extreme fractional quantities and may be traded for one another without fiat currency.
- While the majority of transactions are recorded on a blockchain, there is a significant portion of transactions that occur off-chain.

The complexity of the system results in unique data characteristics that are not compatible with traditional fintech software and infrastructure.

To understand and execute protocols based on large data sets like this requires infrastructure, education, constant maintenance, and years of experience. Lukka's standardized and enriched Reference Data covers 450,000+ assets, 165,000+ derivatives, 120,000+ trading pairs, and 1,000+ ecosystem entities such as exchanges, Over the Counter (OTC) desks, and pricing sources including decentralized exchanges (DEX) & decentralized finance (DeFi). Lukka Reference Data is integrated into Lukka Enterprise Data Management, so this process is fully automated for tax authorities and regulators.

Data management must be a central part of research and development as OSTP collaborates with other federal agencies to develop priorities related to digital assets. Working with those who are not only innovators and experts in the area, but who also play a part in bringing responsibility to the industry, would be an additional means for achieving the stated goal of responsible innovation.

Topic Number 3 - Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

Safeguards for consumers and investors are necessary for sustainable growth and long-term investment. Instituting regulations that require disclosures pertaining to risks, conflicts of interest, leadership, and financials are essential for protecting consumers from potential fraud and mitigating those risks. While disclosures give consumers up-front protection, external audits and crypto asset classification and monitoring tools enable a long-term compliance mindset within the crypto ecosystem. Institutional-quality data solutions that provide crypto market participants with transparent and audit-ready valuations and reconciliations across hundreds of blockchains, thousands of tokens, and millions of transactions can protect against fraud. This functionality serves companies and governments with equal ease.

Data management tools can further assist institutions by delivering clarity to a multitude of complex crypto transactions, using tools like asset mapping, standardization, and data ingestion and extraction. A service provider that can ingest data via API or various file formats, automate analysis of large volumes of crypto data, and decrease the need for manual reviews of transactions, can then provide much-needed comprehensive quantitative analysis of crypto activity.

At Lukka, we are committed to the security, operability, and integrity of our solutions and our customers' data. We believe that there is a healthy intersection between the essential pillars of decentralization and autonomy in the crypto ecosystem, and the protection of consumers through traditional risk management practices like audits, disclosures, and regulatory compliance. Lukka provides solutions to both government and institutional customers so they are able to find this equilibrium.

Topic Number 5 - Opportunities to advance responsible innovation in the broader digital assets ecosystem

Based on our experience meeting the needs of global crypto market participants and regulators, we take the position that a robust crypto asset taxonomy is of maximum regulatory value. In the absence of a global consensus on such a taxonomy, it is worthwhile for regulators and policymakers to work together with the industry on a methodology that can be adapted to meet their national needs and concerns.

The advantages and use cases for the development and deployment of an appropriate taxonomy are numerous; including:

- To aid in the understanding of the traits and volume of specific crypto assets that are active in the local ecosystem;
- To support the monitoring of the risks and benefits associated with the crypto assets in the local environment, including any systemic financial and consumer protection risks as needed; and
- To assist in the mapping of crypto assets to traditional assets (financial or otherwise).

In general, after many years of working to organize, standardize, and normalize crypto transactions and traits, Lukka sees that the benefits of a well-designed taxonomy are greater than any related costs.

An existing token mapping system – the Lukka Digital Asset Classification System

Key to the advantages presented above is combining a well-designed taxonomy and mapping approach, with appropriate expertise that spans both crypto and traditional assets. LDACS is a detailed and comprehensive structure consisting of a five-tier hierarchical taxonomy with the purpose to improve transparency and efficiency in assessing and analyzing digital assets.

LDACS is designed to fulfill the global digital asset community's need for a complete and globally accepted taxonomy to classify digital assets.

Guidelines for Classification:

- Classification by Intended Use & Structure

  The classification of a digital asset is not always straightforward or immediately identifiable. In order to determine the intended use and structure of an asset, Lukka examines existing documentation and communications from the asset issuer that detail the intended use case(s) of the asset. These details are then compared holistically to Lukka's sector definitions. Following this comparison, any sector classifications that are deemed applicable are assigned to the asset.

- Source of information used for LDACS Classification

  The primary source of information used for classification will be the official communication by the issuer of the asset. Such communication includes (but does not have to be limited to): the whitepaper, one-pager, official website, blog, or social media accounts associated with the asset and its issuer. Lukka will look at all forms of official communication and documentation available that describe the use case or structure of the asset and ultimately take a holistic view in its classification.

  In instances where there appears to be no formal communication or documentation, but there is sufficient information from sources Lukka deems as reputable and appropriate to use, Lukka will utilize that information during the classification process on a best efforts basis.

- Selection of the Primary Classification

  In instances where there is only one intended use case for an asset (e.g. Bitcoin), that classification is selected as the Primary Classification. However, digital assets can facilitate more than one use case (eg, Wault Finance). Thus, for a given asset, it is possible to have multiple LDACS Classifications. In these more complex instances, Lukka will provide multiple classifications for the asset, but flag only one as the Primary Classification. The Primary Classification flag will ultimately be decided by what appears to be the most prevalent intended use case through a comprehensive examination of all available information as described in the previous section. Where multiple classifications exist, Lukka does not provide a hierarchy of use cases outside of a boolean classification.

- Ecosystem Support Assets Classification

  In the case of assets that perform a special function in a given cryptocurrency ecosystem but do not perform the primary function of the assets within that ecosystem, such as Governance Tokens, the Primary Classification of those assets will reflect the primary use case of the asset's ecosystem rather than the primary use case of the asset itself. For example, Ampleforth Governance Token is the Governance Token of the algorithmic stablecoin Ampleforth. Ampleforth Governance Token is an essential part of the Ampleforth ecosystem, but has no other use case outside of that ecosystem and is not itself a stablecoin. Thus, its Primary Classification designation would be Algorithmic Stablecoin.

Having a trusted token classification system upon which both the industry and regulators can rely on for responsible innovation would allow for a more complete governance of digital assets.

Conclusion

Lukka is committed to supporting regulators, standard-setters, and policy makers as they seek to both better understand the crypto ecosystem and design protections for their respective citizens and financial markets. We have unique insights across the various crypto assets and markets, and across many different types of market participants who are our customers. So, we would close by offering to participate in any ongoing discussions, and to provide any educational materials or research tools, as needed.

Thank you for your time and consideration of our feedback. We would be pleased to discuss any of these comments at your convenience.

Respectfully,

Brian M. Whitehurst
Head of Regulatory Affairs and Regulatory Counsel
Lukka, Inc.

Tom Dixon
Head of Public Sector
Lukka, Inc.

Suzanne Morsfield
Global Head of Accounting
Lukka, Inc.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Mark Abner

From: Mark Abner
To: DARD-FTAC-RFI
Subject: < RFI Response: Digital Assets R&D Agenda >
Date: Sunday, January 29, 2023 9:22:02 AM

To Whom It May Concern,
Thank you for the opportunity to comment for the Federal Register on policy efforts to grapple effectively with modern monetary technologies. I will also forward my comments to my congressional representatives. I vote in every single election, I vote 100% Democratic, I live in Minnesota, I own Bitcoin and believe in its bright future, and I think the following:

1). The government needs to define clearly and reign in some 20,000 unregistered securities. It needs to regulate in the manner that it already regulates penny stocks, which is what these tokens are. The software companies and teams ("foundations") behind the 20,000 unregistered securities can be forced to disclose risks and conform with US law or cease operations. Applying existing securities law more effectively to force disclosure will wipe out 95-99% of cryptocurrencies and, therefore, their risks.

On the other hand, Bitcoin is not a security. It is digital property. Forcing cryptocurrency projects to disclose risks similar to penny stock disclosures will simultaneously expose the federal government's specific limitations with regard to Bitcoin, the sole commodity in the sector, which is uniquely decentralized and globally adopted. There is no central team behind Bitcoin, so there is no one to regulate or disclose, forcing US law and regulators to adapt to its commodity properties.

2). The federal government should understand that Bitcoin's use of electricity is a security feature, not an environmental bug. Moore's Law is already ensuring that ASIC miners are becoming dramatically more efficient with each generation. Also, fierce competition is ensuring that Bitcoin miners seek out the cheapest electricity anywhere on earth, which usually means renewable, stranded and wasted electricity of all kinds, such as flare gas on oil pads, isolated hydro in former industrial areas, and excess wind and solar in West Texas, which cannot otherwise get to market. Bitcoin miners, uniquely, arrive at these remote locations and transmit their products to market with a simple internet connection, creating jobs and value and incentivizing more sustainable energy development. Bitcoin miners usually do not compete with more expensive, peak, household electricity use, because they cannot afford to.

We will look back critically in just a few years on the abundant foolishness of the current proof of work energy narrative, so let's not build a restrictive regulatory framework now to address concerns that are taking care of themselves. If the US wants to participate in and lead this global tech sector, the government must be farsighted enough to understand that the negative energy narrative around Bitcoin mining, much of it funded by competing token projects like Ripple's underwriting of Greenpeace anti-Bitcoin marketing campaigns, does not hold up to scrutiny and certainly will not hold up over time. Other nations understand the flawed energy narrative in the US and media and will attract this tech sector and its value creation away from the US by helping miners embrace and develop the abundant stranded, renewable, undeveloped energy sources in their countries. We need to be smart.

3). The Federal government should separate bad actors in the Bitcoin ecosystem from those who wish to comply with rules (if only the government would provide the rules.) Fidelity, BlackRock and other established institutions interested to provide Bitcoin services to their clients are proven responsible actors. Until the government can provide an effective playing field, the industry will remain offshore, risky and problematic.

4). The US government has, unfortunately, proven itself - repeatedly - as untrustworthy of the immense responsibility to issue a CBDC. Americans do not want coins that allow their government yet another way to spy electronically on their activities and to hand over the power to restrict financial transactions the government opposes, whether such spending is judged to be noncompliant with future political activism, spending that is noncompliant with abortion access, spending that is noncompliant with preferred climate or DEI beliefs, spending that benefits restricted countries, and so on unpredictably as the political winds change over time. In the hands of government, CBDCs will inevitably become our country's version of China's social credits system. If the Federal government proceeds to issue a CBDC, which is simply government spyware, prepare for fierce, protracted, organized, probably partisan, and very wealthy resistance.

Thank you for your consideration of my concerns.

Mark Abner
St. Paul, Minnesota
January 29, 2023

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Metallicus, Inc.

1. Digital assets and their turing-complete distributed ledger technologies (DLT) can provide significant benefits to the financial services, trade, law, hospitality, and energy sectors of the economy. DLT offers real-world benefits relating to improved network uptime and reliability, security, transparency, and efficiency through the automated execution of smart contracts. These characteristics can affect the largest sectors of our economy in significant ways. Fraud and criminal activity can be greatly reduced within international trade by mandating government ID verification and, biometrically and cryptographically secured release authorizations. Hospitality businesses can increase their customer loyalty and overall revenue streams by offering unique reward models that utilize smart contracting and non-fungible tokens. Energy usage can be tracked on a DLT atop which carbon credits can also be issued, awarded, and redeemed automatically through the use of smart contracts. Smart contracting can also greatly increase the efficiency with which legal contracts are executed, particularly in the insurance industry. Traditional technologies are not able to offer all of these benefits due to the security and reliability risks posed by centralized computing infrastructure. Distributed ledger technology combined with the composability of blockchain components and smart contracts is the fundamental technological breakthrough that allows for this level of efficiency, reliability and traceability. As of now, financial services are being challenged by these nascent technologies. Particularly, the rise of fully reserve-backed and regulated stablecoins has made remittance payments trivially easy, fast, and cheap when compared to using traditional cross border payments. The USA is the greatest generator of outbound remittance payments due to its robust economy, which attracts people from all over the world. By promoting the use of DLT for remittances, we can ensure that the loved ones of hard working Americans are receiving as much as possible, without the burden of high transaction fees. The positive global economic impact of this would be in the billions. Responsible tokenization of the US Dollar will ensure that the US Dollar remains the top global trade currency. Currently, the limiting factors for public adoption relate to the lack of network scalability and regulatory compliance, for the predominant chains Bitcoin and Ethereum. Distributed ledger usage incurs fees for the end user associated with each payment, which incentivizes the distributed security model. Ethereum transaction fees vary based on network congestion and can become prohibitive when demand for the network is high. These fees can be

minimized or eliminated through the use of advanced and highly scalable ledger technologies. The vast majority of DLTs also do not feature compliance tooling on-chain. DLTs should include KYC account verification and transaction monitoring in order to comply with OFAC sanctions and other regulatory rulings. Without these built in safeguards, we cannot responsibly encourage the adoption of DLT across the major sectors of our economy.

2. The absence of regulation and auditing of the digital assets and DLT industry has allowed the proliferation of fraudulent platforms ranging in size from small to extremely large, with customer losses mounting into the tens of billions. By introducing sensible legislation which protects consumers while fostering innovation, we can avoid these situations in the future. Such legislation should prohibit the rehypothecation of users' digital asset deposits by exchanges and brokerages and mandate that virtual asset service providers (VASPs) must provide a public and real-time view into the Assets and Liabilities of the organization. Digital Asset companies must be held to the same, or even greater risk management standards than traditional finance firms. Stablecoin regulations must mandate that stablecoins are fully reserve backed by US Dollars and/or US Treasuries, and must outlaw synthetic or algorithmic stablecoins which pose significant risks to the economy. The publicly searchable ledger, which has its benefits, also poses significant risks to consumers and businesses by eliminating privacy. We can safeguard privacy in financial services while remaining compliant with regulatory requirements through the use of trusted-setup ZK proofs (zero knowledge proofs). A trusted-setup allows regulators to have a viewing key for audit purposes. A DLT which allows regulated financial institutions to remain compliant and retain privacy while allowing instant settlement on a decentralized ledger would be critical towards making this technology viable for mass adoption. These ledgers must also be energy efficient in today's world of rising energy costs and environmental concerns. Fast and efficient Proof of Stake consensus mechanisms are highly favored over wasteful Proof of Work consensus, which is slow and costly to the environment. Traditional database technologies are able to provide scalability, compliance, privacy and are energy efficient, but by utilizing PET such as ZK proofs, on-chain compliance tooling, and Proof of Stake consensus, DLTs can achieve these standards we are accustomed to while harnessing the massive reliability, traceability, and efficiency gains of DLT.

3. The Federal Government has a significant R&D opportunity to form a close public-private sector partnership with Metallicus, Inc. Metallicus, Inc is building the aforementioned solutions in the regulated and compliant DLT space. These solutions are environmentally-sustainable, offer tools for law enforcement to counter illicit activity using digital assets, and enable regulators to protect consumers from fraud. The wallet solutions that are now built are based on the W3C open source standard called Webauthn which Apple, Google, and Microsoft are leveraging and have named FIDO. This solution stores users' private keys in the secure element of any readily available device, which is segregated from the device OS. It can only sign for a transaction when the assigned hardware or biometric key is present, therefore eliminating the majority of security risks around private keys. Users will not have to invest in expensive proprietary hardware to secure their digital assets easily. Metallicus, Inc are also working on solutions to make lost private keys a problem of the past. These solutions can make digital assets viable, including CBDCs. With the DLT, compliance and security technologies mentioned above, everything exists today for the USA to launch a CBDC tailored to the specifications of the Federal Reserve. By taking the lead on CBDC and stablecoin digital assets, the USA can remain the leader in the changing global economy.

4. The R&D of a US CBDC should take into context how the PRC is building the digital Yuan, and aim to improve upon it. While the Federal Reserve has the power to build any level of programmability into the privately controlled CBDC DLT network, it should avoid integrating social credit score systems and continue to encourage healthy saving habits of Americans by eliminating the negative interest rate policy built into the digital Yuan, for example, which forces Chinese citizens to spend their money instead of saving it. By enabling choice with a US CBDC, the USA can maintain its lead in the world as the bastion of freedom and maintain its reputation for having the strongest and most trusted capital markets. Another focus of R&D efforts should be the systemic upgrade of the bank settlement system. Interchange, ACH and SWIFT are in desperate need of an upgrade, and the DLT solutions detailed in this request for information are being built exactly with this purpose in mind. Banks and processors can settle transfers instantly, with compliance controls on-chain, privately, all by using fully USD reserve-backed stablecoins as the bearer instrument. The financial impact of fast settlement across the banking system would be significant.

5. The United States needs to participate in the creation of DLT standards to be used industry wide. This can increase the rate of innovation and economic growth that results from the broader adoption of digital assets. A common set of standards will reduce the friction between innovators, financial institutions, and consumers. The USA needs to continue to develop chip manufacturing domestically, to be able to provide the hardware necessary to secure these DLTs. The hardware does not have to be purpose-built, as the fastest and most resource-efficient DLTs do not require special proprietary hardware, such as the ASICs used in Bitcoin mining.

6.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Michael Jones, University of Cincinnati

Education and financial integration are the real solutions to crypto's setbacks

In response to a Notice of Request for Information,[1] we address

Topic 3: Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets, and

Topic 4: R&D that should be prioritized for digital assets:

The last several months have left a black eye on the crypto industry. Cryptocurrency exchanges are declaring bankruptcy, law enforcement agencies are filing criminal charges against industry insiders, and the casual observer is left to wonder when the next shoe will drop. FTX's former CEO, Sam Bankman-Fried, is in the limelight due to charges of defrauding US consumers out of billions of dollars. This year, President Biden's National Economic Council (NEC) criticized not just Bankman-Fried, but many other bad actors in the crypto industry who "mislead consumers, have conflicts of interest, fail to make adequate disclosures, or commit outright fraud."[2] In response, some NEC economists urged Congress to isolate the crypto industry and not "deepen the ties between cryptocurrencies and the broader financial system." Although the NEC has correctly diagnosed crypto's challenges, its proposal takes the industry in the wrong direction.

On the very same day that the NEC advocated for financial isolation, the Federal Reserve Board denied an application from Wyoming-based bank, Custodia, to become a member of the Federal Reserve system. The Federal Reserve justified its decision by saying that Custodia's issuance of crypto assets on public, decentralized networks presents significant safety and soundness risks. After Custodia's request for integration into the Federal Reserve system was denied, its CEO went to Twitter to defend itself by saying that the bank "actively sought federal regulation, going above and beyond all requirements that apply to traditional banks." Furthermore, the Securities and Exchange Commission (SEC) has also repeatedly denied applications from companies like Fidelity, VanEck, and Grayscale to launch bitcoin spot exchange traded funds (ETF). Grayscale is currently suing the SEC, stating that the regulatory agency is being unreasonable and illogical for denying financial integration to crypto investors who want more regulation.

---

[1] https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development

[2] https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks/

In a recent survey of University of Cincinnati Carl H. Lindner College of Business students, UC's Kautz-Uible Cryptoeconomics Lab found that 40% of male students hold cryptocurrency, and more than 10% of them have lost access to their funds from scams, theft by cryptocurrency exchanges like FTX, or by losing account identification credentials. Rather than financial isolation, the government should be opening up and integrating digital asset purchase and custody markets to institutions that are subject to more stringent controls found in the broader financial system.

Despite media attention, the outbreak of fraudulent behavior is not unique to crypto. Earlier this year JP Morgan appeared to be a victim of fraud when it acquired a startup, student financial aid company called Frank for $175 million. Frank's founder, Charlie Javice, allegedly made-up millions of user accounts in order to inflate the market value of the company. In the recent past, one can find plenty of examples of financial fraud from companies including Enron, Worldcom, Wells Fargo, and Madoff Investment Securities. New characters in the age-old play of greed are now the stage as crypto.

Fortunately, federal prosecutors have quickly moved to accept guilty pleas under existing laws from some in FTX's leadership, and multiple state regulators are investigating the crypto lending company, Celsius, for securities fraud and financial mismanagement. These regulatory agencies though do not have the resources or complete information to proactively prevent fraud before it happens. They frequently rely on credible complaints from individual investors for their investigations. The presence of a greater number of investors, not fewer investors, will result in more oversight and accountability in the crypto industry.

If US agencies are going to reject those crypto organizations who want certain levels of oversight and regulation, then the least the government can do is provide resources to increase the level of crypto education and literacy. In the same survey mentioned above, the Kautz-Uible Cryptoeconomics Lab recently asked UC students to self-assess their overall level of financial knowledge and crypto knowledge. Not surprisingly, this young group expressed rather low levels of knowledge in both domains. Just over 30% of students indicated an above average level of financial knowledge, but less than 10% reported an above average level of crypto knowledge.

Those who are crypto literate will know how to obtain and store cryptocurrency safely, and they will also know how to assess risk to make appropriate investments. The state of Ohio recently required all students who graduate from its high schools to earn one-half of a financial literacy credit.[3] Economists recognize that financial literacy is such a critical skill for life and career success that Ohio passed a law to require its schools to teach the subject. It is time that every state also takes crypto literacy seriously. With a significant percentage of this young population being denied access to regulatory guardrails for their crypto holdings, the University of Cincinnati is dedicated to leading the way in crypto literacy. We urge the Office of Science and Technology Policy to invest in R&D to advance crypto literacy research and educational programming.

Sincerely,

Michael Jones, PhD, Director of the Kautz-Uible Cryptoeconomics Lab
Jack Luu, Digital Futures Fellow
Binny Samuel, PhD, Associate Professor, Lindner College of Business

Respondent type: Academic Institution

[3] https://education.ohio.gov/Topics/Learning-in-Ohio/Financial-Literacy/Financial-Literacy-in-High-School

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Thesis by Michael Rowen

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY

by

Michael S. Rowen

December 2022

Thesis Advisor: Leo J. Blanken
Second Reader: Nicholas Dew

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE				*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis		
4. TITLE AND SUBTITLE SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY				**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael S. Rowen				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) [redacted]				**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) [redacted]				**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.				**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Concepts to harness positive opportunities inside the cryptocurrency ecosystem to advance national security objectives have yet to be fully explored in government organizations. This thesis, focuses on cryptocurrency as a subset of digital assets and attempts to answer the question: Is there utility for cryptocurrency in U.S. special operations (USSOF) and could it support broader U.S. national security strategies? A whole-of-government approach for the responsible development of digital assets should include Department of Defense (DOD) and USSOF perspectives. The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace. The DOD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams with the intent to develop new operational concepts. USSOF should continue to expand public-private partnerships to improve awareness, capacity, and competency in the digital asset ecosystem and leverage blockchain research and development directives to inform innovative concepts for cryptocurrency in special operations.

14. SUBJECT TERMS cryptocurrency, special operations, SOF, Bitcoin, USSOCOM, USASOC, digital assets, financial technology			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY

Michael S. Rowen
Major, United States Army
BA, Western New England College, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED DESIGN FOR INNOVATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Leo J. Blanken
Advisor

Nicholas Dew
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Concepts to harness positive opportunities inside the cryptocurrency ecosystem to advance national security objectives have yet to be fully explored in government organizations. This thesis focuses on cryptocurrency as a subset of digital assets and attempts to answer the question: Is there utility for cryptocurrency in U.S. special operations (USSOF) and could it support broader U.S. national security strategies? A whole-of-government approach for the responsible development of digital assets should include Department of Defense (DOD) and USSOF perspectives. The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace. The DOD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams with the intent to develop new operational concepts. USSOF should continue to expand public-private partnerships to improve awareness, capacity, and competency in the digital asset ecosystem and leverage blockchain research and development directives to inform innovative concepts for cryptocurrency in special operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CBDC	Central Bank Digital Currency
CoW	Coalition of the Willing
CRADA	Cooperative Research and Development Agreement
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DARPA	Defense Advanced Research Projects Agency
DC:BB	Distributed Consensus: Blockchain and Beyond
DID	Decentralized Identification
DLT	Distributed Ledger Technology
DOC	Department of Commerce
DOD	Department of Defense
DOT	Department of Treasury
IPFS	Interplanetary File System
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
SOCOM	Special Operations Command
TSOC	Theater Special Operations Command
USASOC	United States Army Special Operations Command
USD	United States Dollar
USDC	United States Dollar Coin
USDT	United States Dollar Tether
USSOF	United States Special Operations Forces
VEO	Violent Extremist Organizations

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Emerging financial technologies have the potential to reveal gaps in national security strategies for the United States. The presidential executive order of March 2022 and the digital asset development framework of September 2022 represent initial steps to provide a comprehensive whole-of-government model in response to this gap. Methods to harness positive opportunities inside the cryptocurrency ecosystem to advance national security objectives, however, have yet to be fully explored in government organizations. This thesis, therefore, focuses on cryptocurrency as a subset of digital assets and attempts to answer the question: Is there utility for cryptocurrency in U.S. special operations (USSOF) and could it support broader U.S. national security strategies?

A. KEY FINDINGS

The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. Beyond financial settlements, cryptocurrency offers the ability to build private and secure applications on public blockchain infrastructure to deliver valuable non-standard communication or data management tools for military operations. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace.

A whole-of-government approach for the responsible development of digital assets should include Department of Defense (DOD) and USSOF perspectives. Including USSOF concepts for cryptocurrencies could help the United States to shape global cryptocurrency adoption with the intent of countering nefarious activity and modernizing security strategies while concurrently developing novel support mechanisms in moments of crisis and conflict.

Blockchain technology is widely accepted as a valuable innovation and forms one of the foundations to digital assets. A policy window is opening for DOD leaders

to stimulate innovation in emerging financial technology tactics by understanding the overlap between blockchain, digital assets, and global power dynamics. A blockchain research symposium held at NPS in September 2022 offered an opportunity to analyze the current state of blockchain adoption in the U.S. government and identify threats, opportunities, areas of friction and advocacy.

There is potential for a divergence in blockchain development and adoption between authoritarian regimes and democratic nations, underscoring the need to recognize the implications of blockchain technology in U.S. national security strategies. U.S. pacing threats view digital currency markets as an opportunity to gain hegemony with new central bank digital currencies and shape an alternative, digital financial system by exploiting early adopters and undermining the potential for public good from digital asset technologies. The United States is positioned to assist allies that are looking for regulatory clarity and policy guidance to establish global norms in line with U.S. values for blockchain and digital assets. Perspectives from USSOF operators trained and educated in cryptocurrency may offer an important feedback mechanism to U.S. policymakers.

B. RECOMMENDATIONS

- The DOD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams with the intent to develop new operational concepts.

- The U.S. government should continue to expand public-private partnerships to quickly improve awareness, capacity, and competency in the complex blockchain and digital asset ecosystem where DOD is too often overlooked in key stakeholder positions.

- USSOF should leverage the 2023 NDAA SEC 5913 "National Research and Development Strategy for Distributed Ledger Technology" to request additional resources for advancing education and experimentation with digital assets in U.S. special operations units. USSOF in conjunction with academic and private partnerships, should conduct surveys to help illuminate the level of adoption and literacy for digital assets which will drive training requirements and experimentation.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Dr. Leo Blanken and Dr. Nicholas Dew, for their guidance, leadership, and encouragement while pushing me to explore an emerging but contentious topic.

It was a privilege to work with everyone in the cryptocurrency and financial technology sector, I learned more than I could have imagined. I am so grateful for the community's eagerness to help and trust in my research to connect me with other key leaders. The blockchain symposium was only possible because of this wonderful and patriotic network of leaders who offered their time and expertise, I am truly thankful.

I would also like to thank my peers and other NPS faculty members who patiently listened to my rhetoric about cryptocurrencies and provided valuable recommendations and feedback.

Most importantly, I am grateful for my loving family who kept me balanced through this incredible experience and appreciated the time I dedicated to this subject. My wife, Keelan, and daughters, Blair, Alice, and Ruby are truly a blessing, their love and support trumps any achievement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE INTERSECTION OF CRYPTOCURRENCY AND NATIONAL SECURITY

The operational use of cryptocurrency for U.S. special operations forces (USSOF) has the potential to serve as a forcing function to discover emerging financial technology concepts in strategic competition and modernize partnerships. Digital asset proliferation may have impacts far beyond the financial environment and the U.S. national security enterprise must continue to assess adoption trends to adequately respond to shifts in geopolitics. Fortunately, the United States is making progress toward a digital asset strategy as evident in the March 2022 presidential executive order directing a call to action from U.S. stakeholders to provide recommendations for responsible development of digital assets.[1] Following the executive order, the U.S. released a digital asset development framework in September 2022, which was intended to provide a comprehensive whole-of-government model.[2] However, one government entity largely absent from the published digital asset framework is the U.S. defense department. This is an oversight: the U.S. may miss an opportunity to gain ground-truth insights to help shape the U.S. leadership position toward digital assets and positively influence global adoption trends.

Current U.S. research and development for digital assets is focused on the implications of central bank digital currencies, addressing consumer and investor protection, and countering illicit finance.[3] The U.S. defense enterprise's supporting role centers around countering threat finance such as the recent announcement from the

[1] Exec. Order No. 14067, "Executive Order on Ensuring Responsible Development of Digital Assets" (2022), https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

[2] The White House, "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets," The White House, September 16, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

[3] Darrell Duffie and Elizabeth Economy, "Digital Currencies: The U.S., China, And The World At A Crossroads," Working Group (Hoover Institute, 2022), https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads.

Pentagon for a Defense Advanced Research Projects Agency (DARPA) project to help authorities crack down on illicit uses of digital assets.[4] U.S. government organizations have yet to fully develop proven methods to explore the cryptocurrency ecosystem and harness positive opportunities for national security objectives.

Of all the subsets of digital assets, cryptocurrency is the most contentious and typically holds a negative connotation. However, USSOF are comfortable when surrounded by uncertainty and would likely embrace the opportunity to shine light on the murky world of cryptocurrencies to help understand both positive and negative use cases. The positive solutions for cryptocurrency in military operations are largely unknown and the untapped potential for programmable digital currency in the hands of creative special operations members may reveal more opportunities beyond countering illicit activity. Cryptocurrencies such as Bitcoin and Ethereum offer a novel medium of exchange for peer-to-peer communication, instantly transferring value around the world, or developing more applications beyond the original function, albeit with proper risk mitigation.

A comprehensive strategy will need to reach the diverse subsets of digital assets; central bank digital currency, cryptocurrencies, non-fungible tokens, and stablecoins which all demand time and attention to fully understand. This thesis is focused on cryptocurrency as a subset of digital assets and attempts to answer the question; is there utility for cryptocurrency in U.S. special operations and could it support broader U.S. national security strategies?

B. APPROACH

The approach taken for this research project intends to offer a wide range of concepts for cryptocurrencies but observed through the lens of a U.S. national security practitioner. Cryptocurrency is an emerging technology, and the fundamentals are not commonly understood among the general population. This led to the decision to offer a conceptual thesis focused on stating the relevance for cryptocurrency in U.S. special

[4] Tory Newmyer, "Pentagon Launches Effort to Assess Crypto's Threat to National Security," *Washington Post*, September 23, 2022, https://www.washingtonpost.com/business/2022/09/23/darpa-crypto-national-security/.

operations. The complicated nature of cryptocurrency and the underlying blockchain technology may leave some readers with more questions than answers. That result may still offer positive commentary within the U.S. national security enterprise and maintain cryptocurrency in the mind of practitioners. The research revealed that most resources and articles discussing the DOD and cryptocurrency are limited to countering illicit activity. This thesis intends to offer additional scenarios where special operations forces could harness the positive benefits surrounding a novel financial technology. This paper offers general concepts for how special operations could leverage the cryptocurrency ecosystem by citing examples of cryptocurrency and digital asset use cases around the world.

Of note, Chapter IV summarizes several key points from the planning and execution of a blockchain research symposium conducted on the Naval Postgraduate Schools campus from 12 to 13 September 2022. It is recommended for readers to reference the appendices for each panel concept sheet which offers the moderator questions and may offer more context to the key findings listed in Chapter IV. Please note that we did not develop a panel 5 concept sheet. The summary was co-authored with an NPS faculty member, LTC Michael "Kelly" McCoy who helped organize and lead the symposium. This event aggregated various national security practitioners and U.S. Defense Department leaders to debate the threats and opportunities for blockchain technology, cryptocurrencies, and the intersection of national security for two financial technology innovations.

A blockchain symposium was a deliberate approach used to support this thesis largely due to the contentious narrative surrounding cryptocurrency in U.S. national security circles. The author and faculty members from NPS, believed that starting with cryptocurrency's foundational technology, blockchain, offered a more acceptable model to introduce potential benefits of cryptocurrency. Overall, the blockchain symposium presented an opportunity to analyze the broader support and adoption potential of cryptocurrency in both the private and public sectors which may prove useful for future research and development.

C. LITERATURE REVIEW

1. The Narrative of Digital Assets in U.S. Government

The discussion within DOD circles regarding cryptocurrency centers on the negative implications from cryptocurrency in support to nefarious activity and possible counter-measure U.S. forces could take to reduce those threats. Violent extremist organizations (VEOs) and criminal organizations are leveraging cryptocurrency to remain undetected while transferring value, communicating, and laundering money. Nation states have embraced the cryptocurrency ecosystem to attempt sanctions avoidance and build a new network to transfer value or trade commodities. In the article *Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency*, the authors offer that "cryptocurrency transactions expand the international financial competitive space by creating an alternative to a fiat-based monetary system that skirts international financial mechanisms set to detect and intercept suspicious activities."[5] The negative repercussions for the United States and allies if an alternative international financial market without the U.S. dollar as the reserve currency are significant and expert analysis, research, and security strategies should continue to prevent those conditions. A gap in research still exists to determine where the responsible integration of cryptocurrency and other digital assets into the current U.S. led, international trade markets and security enterprise may benefit.

The DOD, and specifically financial management commands recently added a 40-hour digital asset training course and executive level cryptocurrency classes.[6] Comptrollers in the DOD typically apply counter threat financing doctrine which is often absent with cryptocurrency references or connects digital currency to illicit activity. The DOD's focus and experience for disrupting terror financing cells is likely driving most of the current literature on cryptocurrency but as digital asset literacy grows so too will the scope of research. The Fall 2022 issue of *Armed Forces Comptroller* is a positive adoption signal

[5] Sara Dudley et al., "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *Joint Force Quarterly*, no. 92 (2019): 60.

[6] Joint Knowledge Online, "New USSOCOM J35 Counter Threat Finance (CTF) Curriculum," Joint Chiefs of Staff, August 4, 2022, https://www.jcs.mil/JKO/Latest-News/JKO-Customer-Spotlights/Article/3115355/new-ussocom-j35-counter-threat-finance-ctf-curriculum/.

for financial technologies and the editions subtitle, *Operationalizing the Army's Universe of Transactions* presents several articles sharing methods to implement data analytics and dynamic value transfer systems.[7] Specifically, the article *Applying Financial Capabilities to Achieve Multi-Domain Effects* by COL Brian Smith, details a process the U.S. Army could implement for financial instruments to achieve tangible operational effects.[8]

Two reports from the Center for Naval Analyses (CNA), offer relevant cryptocurrency information for military organizations. Both reports were published in 2019 and authored by Megan McBride and Zack Gold who present in depth analysis and helpful background information.[9] The reports titled "Cryptocurrency: A Primer for Policy-Makers" and "Cryptocurrency: The Implications of Special Operations Forces" are recommended as an early reference to help understand the connection of cryptocurrency to military operations.[10]

In Figure 1, the CNA report on the implications for SOF presents a chart outlining potential challenges and opportunities for special operations units correlated to various levels of cryptocurrency adoption. This tool remains useful when applying the current state of cryptocurrency adoption and then incorporating analysis from McBride and Gold to build context for military specific research and development.

---

[7] Rich Brady and Bill Arnold, "Data Analytics: From Raw Data to Informed Decisions," *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022), https://asmconline.org/armed-forces-comptroller/.

[8] Brian A. Smith, "Applying Financial Capabilities to Achieve Multi-Domain Effects: Using Financial Capabilities Operationally Rather Than Transactionally," *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022): 54, https://asmconline.org/armed-forces-comptroller/.

[9] Megan McBride and Zack Gold, "Cryptocurrency: A Primer for Policy-Makers" (Arlington, VA: Center for Naval Analyses: Analysis and Solutions), accessed October 26, 2022, https://www.cna.org/reports/2019/08/cryptocurrency-primer-for-policymakers.

[10] Megan McBride and Zack Gold, "Cryptocurrency: Implications for Special Operations Forces" (Arlington, VA: Center for Naval Analyses: Analysis and Solutions, August 2019), https://www.cna.org/reports/2019/08/cryptocurrency-implications.

Likely futures of cryptocurrencies and potential implications for SOF

		Scenario 1: Increased adoption/ Stalled regulation	Scenario 2: Increased adoption/ Increased regulation	Scenario 3: Stalled adoption/ Increased regulation	Scenario 4: Stalled adoption/ Stalled regulation
Challenges	Fractured regulatory environment	↓	↔	↑	↔
	Evolution of technology (and nefarious behaviors)	↓	↔	↑	↔
	Lack of knowledge, training, and education	↓	↓	↓	↓
Opportunities	Exploitable existing technology	↑	↑	↔	↑
	Underdeveloped partnerships	↑	↑	↑	↑
	Malleable future environment	↔	↑	↑	↔
	Underexplored potential applications	↑	↔	↔	↑

Mid-term implications for SOF given its existing posture	
↓	Negative
↔	Neutral
↑	Positive

Source: CNA

Figure 1. Cryptocurrency Adoption and Implications Tool.[11]

In general, there is a consensus for continued collaboration to share methods for managing the emergence of cryptocurrency across U.S. government departments and agencies. The U.S. State Department published a success story and positive use case after cryptocurrency rewards helped to gather intelligence on cybercriminals.[12] Harnessing the benefits from alternative incentive structures provided by cryptocurrency may spark more creativity from other national security organizations. As other government agencies spread best practices for disrupting nefarious cryptocurrency it helps improve awareness of the capabilities and limitations for cryptocurrency. The book *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* includes multiple articles discussing blockchain, cryptocurrencies, and

[11] Source: McBride and Gold.

[12] Martin Leo Rivers, "Got Bitcoin, Will Buy Intel: U.S. Government Offers Cryptocurrency Bounty In Radical New Approach To Fighting Cybercrime," Forbes, accessed October 27, 2022, https://www forbes.com/sites/martinrivers/2021/07/18/got-bitcoin-will-buy-intel-us-government-offers-cryptocurrency-bounty-in-radical-new-approach-to-fighting-cybercrime/.

nation agnostics digital networks.[13] The thought leadership provided by forward leaning technologists and service members in these publications is vital to help steer research and development efforts in SOF. A 2020 report from the Cyber Defense Review offers a supporting argument for including SOF units in digital threat finance efforts at the operational level such as at the Theater Special Operations Commands (TSOC).[14] The author, Hugh Harsono, states that SOF is postured to increase support to digital threat finance operations and the application of SOF specific instruments and relationships, it could help U.S. national security objectives combating VEO finance capabilities.

At the Naval Postgraduate School there are several thesis' which research emerging financial technology with most highlighting Bitcoin in particular, such as Peter Denning's report titled *Bitcoins Maybe, Blockchains Likely*.[15] Most publications either connect threat finance to cryptocurrency and include various risk assessments or provide nuanced technical insight to the broader blockchain industry. For example, NPS's Systems Engineering Department offers a thesis paper detailing the protocols or security provenance for Ethereum's blockchain.[16] In general, the research framework is focused on methods to reduce undesired activity of cryptocurrency or ways to posture national security towards the disruptive nature of cryptocurrency and illicit applications such as the thesis titled *Cryptocurrency and State Sovereignty*.[17]

Another relevant NPS thesis discusses the social networks supporting Bitcoin and offers greater insight to Bitcoin utility for SOF, which directly impacted this thesis and inspired several operational concepts. The thesis titled, *Bitcoin: A Technology Influenced*

---

[13] Zachary S Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* (Livermore, CA: Center for Global Security Research, 2021). Pg 269

[14] Hugh Harsono, "Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain," *The Cyber Defense Review* 5, no. 3 (2020): 153–60, https://www-jstor-org.libproxy.nps.edu/stable/26954878.

[15] Peter J. Denning and Ted G. Lewis, "Bitcoins Maybe; Blockchains Likely," *Sigma XI-The Scientific Research Society*, December 2017.

[16] Vikram K. Kanth, "Blockchain for Use in Collaborative Intrusion Detection Systems" (master's thesis, Monterey, CA, Naval Postgraduate School, 2019).

[17] Ryan L. Frebowitz, "Cryptocurrency and State Sovereignty" (Monterey, CA, Naval Postgraduate School, 2018), https://calhoun nps.edu/handle/10945/59663.

Social Movement, by Green and Johnson presents cryptocurrency adoption in the context of global social movements and theory.[18] The thesis by Johnson and Green also provides a thought experiment which detailed a hypothetical use case incorporating a U.S. Army Civil Affairs team utilizing Bitcoin during key leader engagements and transactions.

The most recent NPS thesis, *Understanding Bitcoin and It's Utility for Special Operations Forces*, served as a starting point and helped steer this thesis approach.[19] The author, Michael Pero, focused on Bitcoin and offers a framework for continued research of Bitcoin in military operations. Pero's publication shares case studies on the history of money and Bitcoin's unique value proposition. The paper also references Bitcoin in resistance movements and posits that the U.S. could leverage the principles of cryptocurrency in future resistance movements which also inspired an expansion of that concept in Chapter III of this thesis.

Cryptocurrency presents many policy considerations, but these are beyond the scope of this thesis. It is difficult for anyone to fully grasp the complex nature of U.S. fiscal policy and regulation, but this paper recommends DOD leaders closely monitor publications or news releases from the U.S. Department of Treasury (DOT) and Commerce (DOC). Both departments are two key stakeholders leading the U.S. in responsible development of digital assets. The National Institute of Standards and Technology under the DOC published a blockchain technology overview. The Presidential executive order and whole-of-government framework charters the U.S. DOT and DOC to work across government to help drive innovation but maintain safeguards while advancing the frontier of digital assets. There are still outstanding legal questions, but the DOC's *Digital Asset Competitiveness Report* offers important background information with a balanced

---

[18] Jason D. Johnson, "Bitcoin: A Technology-Influenced Social Movement" (master's thesis, Monterey, CA, Naval Postgraduate School, 2019), https://calhoun nps.edu/handle/10945/63988.

[19] Michael C. Pero, "Understanding Bitcoin and It's Utility for Special Operations Forces" (Monterey, CA, Naval Postgraduate School, 2022), https://calhoun nps.edu/handle/10945/69701.

approach towards U.S. leadership in this emerging market while addressing a wide range of risks.[20]

The programmability of many cryptocurrency blockchains such as Ethereum and Bitcoin's Lightning Network may arguably reveal unforeseen opportunities in non-standard payment methods and communication capabilities. For the Ethereum blockchain in particular, one of the gold standard resources for developers is the book *Mastering Ethereum: Building Smart Contracts and DApps*.[21] This document was published in 2019 and offers methods to develop smart contracts on Ethereum blockchain, which helps expand the utility of the blockchain through computer programming and coding. As quoted in the first pages, the book is intended to "serve as both as a reference manual and as a cover-to-cover exploration of Ethereum."[22] Many of the arguments for the future utility of cryptocurrency lean heavily on the application development outlined in *Mastering Ethereum* with supporting evidence from the expanding cryptocurrency markets. The report titled *Weaponizing Blockchain* reveals how China, Russian, and the U.S. view military applications beyond explicit monetary transactions and the open-source nature of cryptography and distributed computing now levels the playing field for nation states and illicit networks.

It takes time to understand the array of digital asset threats and opportunities, which contributes to the United States reluctance to implement cryptocurrency into U.S. military operations. Sharing academic resources such as a technical summary for A *Taxonomy of Cryptocurrencies and Other Digital Assets* helps reduce the learning curve and establish a shared understanding of cryptocurrencies.[23] The number of academic resources continues to grow as mainstream adoption of certain digital assets increases, however there is still

[20] Department of Commerce, "Responsible Advancement of U.S. Competitiveness in Digital Assets," Digital Asset Competitiveness Report (Washington, D.C: U.S. Department of Commerce, September 2022), https://www.commerce.gov/files/digital-asset-competitiveness-report.

[21] Andreas M. Antonopoulos and Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, First edition (Sebastopol, CA: O'Reilly, 2019).

[22] Antonopoulos and Wood.

[23] Andria van der Merwe, "A Taxonomy of Cryptocurrencies and Other Digital Assets," *Review Business: St. Johns University*, no. 41 (2021): 30–43, https://www.stjohns.edu/sites/default/files/uploads/Review-of-Business-41%281%29-Jan-2021.pdf.

limited information published from a U.S. military perspective. An article published by *Strategy Bridge* in 2022 touches on the complicated nature of digital currency and policy hurdles for the United States when adapting regulations and standards to meet emerging digital currencies and how U.S. adversaries may leverage the technology.[24]

2. What Is Cryptocurrency?

The three main subsets of digital assets are cryptocurrencies, central bank digital currencies, and stablecoins with cryptocurrency holding the most volatility and speculation. Bitcoin became the first successful cryptocurrency after the whitepaper published in 2008 and remains the leader in global adoption compared to other alternative cryptocurrencies. The U.S. financial crisis in 2008 helped drive the early adopters of Bitcoin as many people lost trust for banks and centralized institutions. The introduction of Nakamoto's *Bitcoin Whitepaper* offers insight to the original intent of Bitcoin's protocol.

> …payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.[25]

This quote helps connect the relevance for special operations and Bitcoin if considering the mutual benefits to digital peer-to-peer connections. The ability to establish a private communications channel, without third-party intermediaries, transfer value, and trust through cryptography should pique the interest of special operations units.

The developers of Bitcoin are unknown, but the network protocol emerged as a novel way to conduct peer-to-peer transactions and remove third party entities to handle trust and accurate record keeping. Blockchain and cryptography underlie the technology

[24] Alyce Abdalla, "U.S. Strategy and the Future of Money: Advancing U.S. Interests During a Financial Transformation," The Strategy Bridge, August 2022, https://thestrategybridge.org/the-bridge/2022/8/29/us-strategy-and-the-future-of-money.

[25] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.Org*, October 2008, https://bitcoin.org/en/bitcoin-paper.

while advancements in computer processing power facilitated scaling through a global decentralized network. Individuals can download Bitcoin's open-source software, run a node on their home computer, and validate transactions, which codifies the information on the blockchain.[26] Bitcoin's innovative nature sparked organizational changes through a digitally native economy over the borderless internet without trusting a third party. The decentralized nature of Bitcoin helps the network avoid central points of failure or succumb to censorship from nation state firewalls. The resiliency and redundancy of the network is supported by distributed ledger technology (DLT) and people or "nodes" running the software which can update new or returning nodes with the transaction history.

A loose analogy is to imagine if individuals could run Visa's electronic payments network on their home computer, help validate every transaction occurring on the network, and also maintained a complete historical ledger. This analogy begins to reveal obstacles with Bitcoin's slow and cumbersome protocol as a medium of exchange which does hinder the ability to compete with cash payments as a means of currency. This factor, in combination with the open-source nature of Bitcoin and other cryptocurrency developer software, led to an emergence of alternative cryptocurrencies with a wide range of functionality. The viability of some cryptocurrencies is frequently debated as many are simply derivatives from other open-source documents and offer little value to customers.

In general, cryptocurrencies are categorized into different layers depending on which blockchain is used as the foundation and subsequent tokens to deliver new capabilities or applications. Typically, cryptocurrency blockchains offer specific tokens which are mined through various incentive structures to generate new coins and properly maintain network transactions.[27] Cryptocurrency is often used as the catch-all phrase but a more precise understanding places tokens as another category or layer, built on top of a cryptocurrency blockchain.[28] Developers even built a new layer, named the Lightning

[26] Kristen Busch, "Blockchain: Novel Provenance Applications" (Washington, D.C: Congressional Research Service, April 12, 2022), https://crsreports.congress.gov/product/pdf/R/R47064.

[27] Coinbase, "Crypto Basics - What Is Mining?," Coinbase Learn, 2022, https://www.coinbase.com/learn/crypto-basics/what-is-mining.

[28] "Cryptocurrencies vs. Tokens: Digital Assets," Gemini, accessed October 26, 2022, https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference.

Network, on top of Bitcoin's original protocol to help improve efficiency and promote application development for Bitcoin.

Many cryptocurrency companies offer helpful websites and free educational guides to increase understanding and confidence. For example, Chainalysis offers free online courses of instruction through their "Chainalysis Academy" website to choose specific areas to research.[29] The centralized exchange, Gemini, offers a particularly user friendly "cryptopedia" on their website which allows users read a concise summary for variety of digital asset terms.[30] Another trusted exchange, Coinbase, delivers a comprehensive guide to cryptocurrency basics, advanced terminology, and even Coinbase Institute which presents free reports to download and help increase awareness of the market.[31] Between both public and private research organizations, there is an abundance of resources on digital assets and are typically free to access online.

Centralized digital currencies and stablecoins are likely positioned as a critical bridge between the legacy financial system and emerging financial technology markets. Central bank digital currencies are a new form of digital money intended to supplement existing central bank reserves, according to The Federal Reserve Bank of Boston and Massachusetts Institute of Technology's digital currency initiative.[32] Stablecoins are like central bank digital currencies as the idea is to provide a stable value relative to a national currency. However, stablecoins have no leading authority or international standards for private stablecoin creation or oversight for assets in reserve which places added pressure for U.S. congressional action. Stablecoins and CBDC's help the digital currency markets manage volatility and diversify reserve pools if handled with proper oversight and regulation. It is reasonable to assume that future applications of digital assets by the DOD

[29] "Learn Cryptocurrency," Chainalysis Academy, accessed October 31, 2022, https://academy.chainalysis.com/page/learn-cryptocurrency.

[30] Gemini, "Crypto Glossary - Cryptopedia," Gemini Cryptopedia, 2022, https://www.gemini.com/learn/glossary.

[31] Coinbase Institute, "Coinbase Institute," accessed October 31, 2022, https://www.coinbase.com/institute.

[32] Federal Reserve Bank of Boston, "Project Hamilton Phase 1 Executive Summary," Federal Reserve Bank of Boston, February 3, 2022, https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx.

will require integration with approved stablecoins and potentially versions of a central bank digital currency.

3. Critiques of Cryptocurrency

The international community and the United States are struggling to catch up with cryptocurrency regulatory policy and standards. The global demand for digital assets is growing and government officials continue to push for varying levels of regulation.[33] Some concerns center around the official designation of digital assets to determine which cryptocurrencies are a security or commodity. Additional security minded concerns question how companies and governments can implement know-your-customer and anti-money laundering measures for cryptocurrency. These issues have been debated for years with dedicated research to help gauge the sensitivity and necessity to apply government clarity.[34] The alternative settlement layers of cryptocurrency offer methods outside of traditional financial systems and highlight concerns for the United States to enforce economic sanctions and project economic power.

Most cryptocurrencies have yet to be officially categorized or designated under specific U.S. regulatory offices or departments. Bitcoin, with no centralized company or owner is decentralized and considered a commodity with tax laws like gold, therefore falling under the U.S. commodities regulations. Many developing nations believe in the potential for a new asset class outside of national government issued currency and embraced Bitcoin as legal tender such as El Salvador in 2021.[35] Critics still argue El Salvador's decision to purchase large amounts of Bitcoin to hold in reserve is the wrong

[33] Tadas Limba, Andrius Stankevičius, and Antanas Andrulevičius, "Towards Sustainable Cryptocurrency: Risk Mitigations from a Perspective of National Security," *Journal of Security and Sustainability Issues*, December 19, 2019, https://repository mruni.eu/handle/007/16063.

[34] Victor Dostov and Pavel Shust, "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?," *Journal of Financial Crime* 21, no. 3 (January 1, 2014): 249–63, https://doi.org/10.1108/JFC-06-2013-0043.

[35] International Trade Administration, "El Salvador Adopts Bitcoin as Legal Tender," U.S. Department of Commerce, International Trade Adminstration, June 2021, https://www.trade.gov/market-intelligence/el-salvador-adopts-bitcoin-legal-tender.

decision and the price volatility is supporting evidence against nation state ownership of Bitcoin.

There are growing concerns surrounding the cryptocurrency market as risks for investors and consumers are evident when major corporations in the ecosystem collapse and exploit customers in the emerging and unregulated global markets. 2022 revealed several failures within the digital asset ecosystem and the vulnerabilities when a venture capital, hedge funds, and centralized trading exchanges conduct reckless or criminal business practices. The collapse of a private stablecoin triggered a cascade effect which exposed multiple centralized digital asset investment companies and harmed both institutions and retail investors. The cryptocurrency market collapse in 2022 revealed that traditional business principles still apply for cryptocurrency and flaws in human nature will continue to be an enemy of innovation. The company FTX was the third largest cryptocurrency trading exchange in the world when details of potentially fraudulent financial management systems were revealed to the public. The subsequent collapse of FTX is a major reason for skepticism with digital assets and private cryptocurrencies. The hyper-financialization and speculative investing practices of digital asset markets often cloud the innovative potential for many observers and government organizations believe the risk is too high to consider cryptocurrency applications.

Cryptocurrency payments offer the path of least resistance for criminals and drives the exploitive nature in the ecosystem. Criminals find use from cryptocurrency's instant and borderless transactions while other open-source software helps to quickly move funds between wallets. Ransomware cyber-attacks are growing since 2020 and typically demand payment in Bitcoin or other cryptocurrencies.[36] This overshadows the positive utility of cryptocurrency for the U.S. military as the current objectives are focused on targeting threat actors who embrace digital assets.

The impact of cryptocurrency on climate change and the debate surrounding associated energy demands also hinder the adoption for the U.S. government. The Bitcoin

[36] Leandro Berg, "RTF Report: Combatting Ransomware," Institute for Security and Technology (IST), accessed August 13, 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.

protocol operates on a proof-of-work blockchain process which requires computers to solve a complex algorithm to create new digital coins. Bitcoin miners often employ hundreds of computers solely dedicated to the mining process and use tremendous amounts of energy. Some nations have banned the practice of cryptocurrency mining and other institutions have paused adoption of cryptocurrency until a more sustainable mining option is available.[37] The U.S. Department of Defense could anticipate tough questions from politicians and constituents concerned about the negative impacts of higher energy consumption with more adoption of proof-of-work cryptocurrency.

4. Current Gap in Research

The idea for operational use of cryptocurrency in SOF units is a critical gap in research and reveals a seam for financial technology applications in national defense. The private sector is far more advanced in their infrastructure and broad ecosystem which scaled rapidly to support growing international demand. Ukraine's rapid adoption of cryptocurrency supports the opportunity for USSOF personnel to apply a suite of value toolbox with cryptocurrency and help lean forward with building proficiency in cryptocurrency to support future moments of crisis and infrastructure collapse.[38]

Sara Dudley's article in Strategic Latency Unleashed offers a comprehensive synopsis of cryptocurrency implications for U.S. national security yet remains SOF-centric with a rare insight for harnessing the benefits. Dudley states, "SOF forces employing disruptive tactics offer commanders nonkinetic solutions and means to affect both the full spectrum of conflict and broad-ranging adversaries. Utilizing latent cryptocurrency capabilities in both a defensive and offensive way represents a viable disruptive, nonkinetic capability SOF might bring to the competitive gray space short of armed conflict."[39] After

[37] Harald Vranken, "Sustainability of Bitcoin and Blockchains," *Current Opinion in Environmental Sustainability*, Sustainability governance, 28 (October 1, 2017): 1–9, https://doi.org/10.1016/j.cosust.2017.04.011.

[38] Danny Nelson and Anna Baydakova, "Ukraine Leads Global Crypto Adoption, Chainalysis Says in New Report," September 8, 2020, https://www.coindesk.com/markets/2020/09/08/ukraine-leads-global-crypto-adoption-chainalysis-says-in-new-report/.

[39] Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. 278.

acknowledging the potential of cryptocurrency use in SOF, leaders in the SOF community should push for more research and development to make sense of the cryptocurrency ecosystem and prioritizes where to start for the tactical end-user.

At minimum SOF units should improve education and local training in the digital asset ecosystem to allow for greater awareness on the battlefield and be capable of supporting alternative transaction methods if requested by critical partners and allies in the future. SOF may embrace cryptocurrencies inherent characteristics and begin overt testing with the top two cryptocurrencies, Bitcoin and Ethereum. Many special operations units operate with the grassroots individuals knowledgeable with cryptocurrency such as in Eastern Europe, Southeast Asia, and Africa. This raises the prospect that Special Operations Forces may be a primary tool for research and development into how to leverage the cryptocurrency ecosystem both in training environments and during deployments.

II. SOF AS THE INCUBATOR

A. THE CULTURE OF SOF AND INNOVATION

The Russian invasion of Ukraine serves as a catalyst for exploring the implications of cryptocurrency on the battlefield. As Eliot Cohen articulated in *Commandos and Politicians*, historically commando units are directed to assist in innovation by testing new concepts which are then shared with the broader national security enterprise.[40] Special operations units continue to serve as a laboratory to inject new ideas and technology into the force by applying rapid prototyping techniques which combine professional military education and cognitively flexible members and incubators.[41] Case studies on innovation in the military are well documented but one trait commonly referenced for successful diffusion is driven by organizational and leadership culture toward innovation, specifically referenced by scholar Stephen Rosen. "Winning the Next War" by Rosen proposes that innovation is often best accomplished during peacetime but does face significant barriers of adoption from conventional incentive structures and timelines.[42] By comparison, special operations organizations offer the most flexibility for career progression, funding, and typically provide senior leader support for mavericks and small teams championing new concepts. SOFWERX is one available "maker-space" or incubator resource for SOF to help source solutions through research and development. The unique authorities and acquisitions processes required to maintain a competitive edge in emerging technologies is acknowledged by SOF leadership and supported through DOD and the National Security Innovation Network.

Elite cross functional teams are often granted the time and space to test, measure and educate the force on novel use cases and recommendations for adoption. Elite unit

---

[40] Eliot A. Cohen, *Commandos and Politicians: Elite Military Units in Modern Democracies*, Harvard Studies in International Affairs, no. 40 (Cambridge, Mass.: Center for International Affairs, Harvard University, 1978).

[41] Leo Blanken, "Special Operations Forces as a Rapid Prototyping Laboratory," ed. Philip Swintek, *Center for Global Security Research*, January 2021, http://hdl.handle.net/10945/67924.

[42] Stephen Peter Rosen, *Winning the next War: Innovation and the Modern Military*, Cornell Studies in Security Affairs (Ithaca, NY London: Cornell University Press, 1994).

support to cyber operations is increasingly important as the necessity to mitigate risk and improve tactical fidelity through cyber technology is too large to ignore. Many special operations security practitioners understand that expanding irregular warfare capabilities and authorities may present opportunities to update doctrine or tactics. Special operations forces can access their international footprint and partnerships to experiment while providing feedback regarding digital asset adoption to assist U.S. policymakers.

In *Strategic Latency Unleashed*, Blanken and Swintek describe the benefits to prototyping and offer that "SOF forces are the most capable of weaving research activities into their operations. Through their careful selection and training processes and lean organizational design, SOF possess the cognitive and operational flexibility to integrate prototyping nimbly and responsibly. Through thoughtful planning that leverages a dedicated network of PME-based researchers and "customers," the joint force could fruitfully utilize SOF units as a global laboratory for innovation."[43] SOF could benefit from rapid experimentation and connection to commercial company developers to test mobile applications that navigate the digital asset ecosystem and create custom solutions for each region or tactical element.

As the first steps are taken through education, units must show a willingness to collaborate across government agencies and departments, which has become standard practice for many special operations units. For the U.S. special operations community to experiment responsibly with cryptocurrency, it is imperative to collaborate with the U.S. Department of Commerce, Department of Treasury, and The Office of Science and Technology Policy to follow cutting edge guidance and regulation while sharing educational tools or training opportunities. Approving new cryptocurrency instruments in the operator's toolbox can help the United States remain agile and reinforce its position as a preferred partner around the globe. SOF units understand the importance of building relationships and establishing trust through working groups with interagency partners will

---

[43] Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. 322.

help illuminate adversary activity while ensuring SOF tactical end-users maintain awareness of shifting policy for cryptocurrency.

A formal mechanism will be required to ensure feedback is shared effectively. The Theater Special Operations Commands (TSOC) are forward deployed subordinate to each Geographic Combatant Command (GCC) and could facilitate intelligence reports and deployment summaries from tactical units. The TSOCs are positioned to serve as the interlocuter for real-time tactical insights and other U.S. government organizations impacted by financial technologies.

Beyond U.S. borders, developing nations lead global rankings for cryptocurrency adoption, which corresponds neatly with the extensive special operations footprint around the world.[44] USSOF should add a "fiscal preparation of the environment" component to deployment reports which includes analysis of digital asset activity to help capture broad economic variables inside their assigned region.[45] A real-time tactical perspective can offer indicators and warnings for adversary use of cryptocurrency or friendly forces sentiment and activity with cryptocurrency. SOF teams often serve as complimentary sensors on the ground to help gather human dynamics and strengthen information gathering capabilities.

B. A SHIFT IN STRATEGY FOR SOF

As competition on the world stage continues, the lines may continue to blur between legacy special operations and irregular warfare methods to keep pace in an era of strategic competition. The development of non-kinetic options for military practitioners are increasingly more valuable as operations to counter nation state adversaries generate extreme risk. The shift to strategic competition and integrated deterrence takes time and requires deliberate training validation processes prior to operational approval. SOCOM holds the largest percentage of financial management service members in the defense

[44] Chainalysis Chainalysis Team, "2022 Global Cryptocurrency Adoption Index," Chainalysis, September 14, 2022, https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/.

[45] Christian Breede, Kevin Stringer, and Sara Dudley, "A Counter-Threat Finance Approach to Competition," The Politics of Special Forces, n.d., https://podcasts.apple.com/us/podcast/episode-2-a-counter-threat-finance-approach-to-competition/id1553806860?i=1000557143750.

enterprise and demand for comptrollers' expertise may rise if financial technology integrates into pilot programs. As tactical teams observe more digital asset activity on the battlefield, comptrollers should be leveraged to improve battlefield forensics and analysis for cryptocurrency hardware and software. The integration of new occupational specialties with tactical teams is typically embraced by SOF and the shift in strategies demands a wider use of cross-functional teams and diverse expertise.[46] U.S. adversaries continue to apply dual-use technologies to disrupt traditional global order and influencers of power. China, as the pacing threat for the United States, may see digital assets as an offset technology to create overmatch during competition or crisis phase and help avoid direct military to military engagements.

China obtained first mover advantage by launching an active central bank digital currency, with plans to compete through the deployment of their digital yuan and leverage international one belt one road infrastructure to overlay new CBDC access points and continue expanding their influence.[47] Russia recently announced plans to launch a digital ruble and develop mutual settlements with China's digital yuan.[48] Time is of the essence for U.S. security strategies to account for current conditions where competitors and adversaries are actively employing dual purpose technologies such as Huawei for hardware and software development which comes outfitted to integrate digital asset tools.[49] It is difficult to anticipate the future intersection of global currencies, digital assets, and U.S. security strategies but expertise in all subsections of digital assets will likely be required to compete effectively.

---

[46] Davis Winkie, "New MOS and Formations Could Come to Army Spec Ops in Tech-Savvy Era," Army Times, July 2022, https://www.armytimes.com/news/your-army/2022/07/28/new-mos-and-formations-could-come-to-army-spec-ops-in-tech-savvy-era/.

[47] Darrell Duffie, "Can China Conquer Crypto?," *Foreign Affairs*, September 2, 2022, https://www foreignaffairs.com/articles/china/2022-04-22/can-china-conquer-crypto.

[48] Reuters, "Russia Plans to Use Digital Rouble in Settlements with China, Says Lawmaker," *Reuters*, September 26, 2022, sec. Currencies, https://www reuters.com/markets/currencies/russia-plans-use-digital-rouble-settlements-with-china-says-lawmaker-2022-09-26/.

[49] M Kimani, "China Leads Africa's Digital Currency Race," Yahoo, Michael, February 2021, https://finance.yahoo.com/news/china-leads-africa-digital-currency-202250648.html.

The U.S. should recommend more collaboration with tactical units to apply financial technology tools at the edge of conflict areas which will add non-kinetic options to better compete and strengthen alliances. Cryptocurrency may appear to serve a marginal role in security cooperation and partner building, however in developing regions with unstable national currencies, there is potential for higher rates of adoption than anticipated. The U.S. military could take a niche approach through special operations forces to help monitor adoptions rates and identify moments cryptocurrency or other digital assets serve U.S. security cooperation objectives.

Starling Labs is an academic research center that developed a new method to document Russian war crimes in Ukraine and prevent misinformation or entropy of evidence online. The lab was co-founded by Stanford University and University of Southern California's Shoah Foundation with collaboration from a global enterprise to include Hala Systems. Titled, Project Dokaz Alliance, the effort utilizes components of blockchain and cryptocurrency technologies to securely capture evidence of war crimes for use by the International Criminal Court.[50] The principles of transparency and immutability of blockchain technology allow for the data to be captured accurately and securely managed. "This process establishes the provenance of the data and allows prosecutors to prove it has not been tampered with from the field to the courtroom."[51] This example provides nonkinetic and irregular effects to hold U.S. adversaries accountable and support broader integrated deterrence strategies. Filecoin is the cryptocurrency used to support Project Dokaz by helping to incentivize users on the data storage and retrieval network. USSOF could apply research efforts to either expand upon Project Dokaz or build additional applications on Filecoin and IPFS replicating the secure processes Starling Labs developed for Project Dokaz.

50 University of Southern California, "Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court," USC Shoah Foundation, June 10, 2022, https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes.

51 University of Southern California.

C. A DRIVER OF CHANGE FOR POLICY IN DOD

As SOCOM continues to answer responsibilities for countering threat financing, a demand for education and training in cryptocurrency may emerge for tactical special operations units to compliment current processes and systems. SOCOM is chartered as DOD's lead and coordinating authority for counter threat finance. This requirement has allowed SOCOM to establish interagency relationships which could help tactical units maintain awareness of the latest U.S. guidance for digital assets. Former USSOCOM commander, General Raymond Thomas, in a 2017 posture statement to the U.S. Senate referenced the active support to interagency efforts and pointed to SOCOMs leading role for DOD in CTF.[52] U.S. DOD directive number 5205.14 *DOD Counter Threat Finance (CTF) Policy* originally released in 2010 and now incorporates changes from 2017 assigns responsibilities for countering terror financing, illicit trafficking, and other related adversary activities.[53] The policy window is opening for USSOCOM and tactical units to help illuminate threats and opportunities for financial technology and use existing relationships from the Global War on Terror's (GWOT) counter threat finance activities.

On U.S. SOCOM's website, the *SOCOM Vision and Strategy* report references the need to "innovate for future threats" and offers that "Over the next 10 years, we will modernize SOF, pioneer dynamic and unorthodox approaches (including the full toolkit associated with irregular warfare), leverage emerging technologies to mitigate adversarial activities by China, and create asymmetric advantages for current and future conflict."[54] One innovative step forward could be to leverage current counter threat financing expertise and programs of instruction to expand or adapt training pathways for tactical units to test and experiment with cryptocurrency.

---

52 *Statement of General Raymond A. Thomas, U.S. Army Commander United States Special Operations Command Before the Senate Armed Services Committee*, 115th Cong. (2017) (statement of Raymond A. Thomas, USSOCOM Commander).

53 Department of Defense, *DOD Counter Threat Finance (CTF) Policy*, DOD Directive 5205.14 (Washington, D.C: Department of Defense, 2017), https://www.esd.whs mil/Portals/54/Documents/DD/issuances/dodd/520514p.

54 USSOCOM, "SOF Vision and Strategy" (Tampa, FL: U.S. Special Operations Command, April 11, 2022), https://www.socom mil/sof-vision-and-strategy.

The overlap between cryptocurrency and SOCOM's CTF charter creates an opportunity space for SOF to take an important role in improving U.S. and partner nation education, testing, and application of cryptocurrency tools. Special operations units inherently offer the culture, capacity, and calculations to serve as the Department of Defense's driver of change for cryptocurrency technology and could help experiment with the costs and benefits for utility of cryptocurrency. This would allow the United States to shape global cryptocurrency adoption with the intent of countering nefarious activity and modernizing security strategies, while concurrently enabling economic development for our allies. Special operations forces, in particular, have a rich opportunity to embrace an irregular approach by leveraging key aspects of cryptocurrency that offer a menu of non-standard means of communication, digitized payments, and access to global communities, often with pseudonymity. By initiating the processes to test cryptocurrency, the SOF community can help identify what levels of adoption or curiosity are present in U.S. military formations and partner forces around the globe.

The bureaucracy and cumbersome defense enterprise is an issue for disruptive technology adoption, but there are signs of successful digital asset adoption in niche use cases and specialized military units. *Forging the Sword* by Benjamin Jensen highlights the importance of incubators and advocacy networks which USSOF has embraced through maker spaces down to the battalion level.[55] USSOF improved talent management and organized technical support formations to create environments conducive to successful innovation. Everett Rodgers wrote Diffusion of Innovation in 1995 but the five key factors are still useful: relative advantage, compatibility, complexity, trialability, and observability.[56] The relative advantage of cryptocurrency in developing regions may drive adoption the most among Rodgers' five factors, as populations face volatile national currency and limited access to U.S. dollars.

---

[55] Benjamin M. Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, California: Stanford Security Studies, an imprint of Stanford University Press, 2016). 17–19.

[56] Everett M. Rogers, *Diffusion of Innovations*, 4th ed (New York: Free Press, 1995).

THIS PAGE INTENTIONALLY LEFT BLANK

III. CONCEPTS FOR CRYPTOCURRENCY UTILITY

A. CRYPTOCURRENCY ON THE WORLD STAGE

U.S. citizens may struggle to see value beyond U.S. dollars (USD) however, individuals living in other countries may desire options outside of their nations denominated currency or even struggle to acquire USD. Cryptocurrency payment rails offer enticing cross-border transaction alternatives for remittances since fees over some blockchains can provide faster and cheaper means to reach family members' digital wallets.[57] The instability in Afghanistan and limited rights for women negatively impacted their access to financial infrastructure. Despite those challenges, some women in Afghanistan managed to build systems leveraging cryptocurrency combined with traditional hawala networks to receive donations or remittances and transition between fiat currency in Afghanistan.[58] The combination of a legacy hawala systems and cryptocurrency inside a nation with volatile infrastructure sheds light on the creativity for cryptocurrency opportunities compared to traditional finance systems.

Cryptocurrency and stablecoins offer developing regions access to global trade and have potential economic upsides in the future. National currencies in developing regions suffer from price volatility, often triggered by corruption or domestic conflicts, which can lead some communities searching for alternative stores of value. Many digitally native generations who were raised on mobile payment applications such as M-Pesa in East Africa, may continue to adopt emerging cryptocurrencies and other digital assets. If private stablecoins such as Circle's USDC and Tether's USDT, receive better oversight and possible global standards, digital natives may embrace more reliable alternate stores of value.

---

57 Hugo Renaudin, "Remittance and Payments: Crypto's Big Opportunity in Latin America," accessed October 27, 2022, https://www.nasdaq.com/articles/remittance-and-payments%3A-cryptos-big-opportunity-in-latin-america-2020-08-06.

58 Joshua Zitser, "Impoverished Afghan Women Are Receiving Emergency Aid in Crypto as the Taliban Limits Cash Withdrawals and Millions Go Hungry," Business Insider, accessed October 27, 2022, https://www.businessinsider.com/afghanistan-women-turn-to-cryptocurrency-to-feed-their-families-2022-1.

Bitcoin and other decentralized digital currencies can offer additional support to populations burdened under autocratic regimes. One example to emulate, during the COVID-19 health crisis, the United States approved support for oppressed health care workers and transferred humanitarian aid directly to Venezuelan citizens in the form of cryptocurrency to avoid a tightly controlled domestic financial system.[59] This example reveals how the alternative financial ecosystem of cryptocurrency allowed access to populations when traditional payment mechanisms were constrained or unable to complete the transaction.

Ultimately, cryptocurrencies inherent nation agnostic origins may provide an irregular option for the U.S. to deliver military aid for resistance elements while partially reducing signature and the associated risk with physical U.S. dollars. In regions with compromised smart city technology or robust digital firewalls, cryptocurrency communities with censorship resistance and privacy conscious culture offer unique ways to mitigate risk for oppressed populations and better circumvent adversary cyber controls.

In late 2022, Taiwan's Ministry of Digital Affairs adopted a decentralized protocol to help improve cybersecurity defenses and infrastructure resiliency in the face of Chinese aggression.[60] The public protocol is called the InterPlanetary File System (IPFS) which stores data across and wide network of nodes which removes centralized points of failure or expensive file storage servers. Decentralized file sharing systems are not new, however IPFS is unique by building a system intended to be interoperable with blockchains. Protocol Labs is the open-source research and development laboratory maintaining IPFS to facilitate growth. Filecoin which is a cryptocurrency built to incentivize peer-to-peer file storage and retrieval with IPFS helps the network maintain active users and nodes.[61]

---

[59] Gideon Long, "Digital Scheme Pays Venezuela Health Workers from Frozen Funds," Financial Times, December 10, 2021, https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18.

[60] Jason Nelson, "Taiwan Turns to Ethereum IPFS Tech to Thwart Chinese Cyberattacks," Decrypt, August 11, 2022, https://decrypt.co/107293/taiwan-turns-to-ipfs-tech-to-thwart-cyberattacks-from-china.

[61] "About Protocol Labs," Protocol Labs, accessed November 20, 2022, https://protocol.ai/about/.

B. MODERNIZE PARTNERSHIPS

The value proposition for cryptocurrency in special operations lies beyond the basic financial transaction component. In certain conditions, service members may find payments in virtual currencies help reduce both digital and physical signatures by removing transactions in U.S. dollars. This characteristic is undoubtedly helpful, but the potential to customize applications with cryptocurrency "software" for smart contracts or peer to peer communication highlights the underlying human dynamic where SOF units should build capability. SOF has an opportunity to monitor a pulse on shifting trends in financial technology and identify exquisite capabilities using cryptocurrency specific DApps tailor made for SOF operations which could prove valuable in future irregular warfare concepts.

The network effect of cryptocurrencies may be an underappreciated aspect however, not in the traditional finance sense, but for increasing access to new communities and populations.[62] The internet-based economy of cryptocurrency encourages network growth beyond borders and may help incentivize niche information gathering opportunities through surveys, fundraising for war efforts, or remote education and training concepts with foreign allies. "Over-the-horizon" or remote advise and assist operations are now more common with the proliferation of digital tools and applications to share information. The commercial sector is beginning to merge communication, financial, and social platforms together which stimulates the network growth of cryptocurrency as they become interoperable on everyday social platforms.

Foreign policy experts and military professionals should heed the advice on networks from John Arquilla who writes extensively on the topic; "leveling networks as actors of equal importance to nation-states" and highlights that networks often serve as counterweights to nation-state hegemon.[63] The emerging decentralized communications market connected to cryptocurrency may allow alternative methods for USSOF and partner

[62] Daniel Roberts, "How Crypto Adoption by Companies like Visa, PayPal, and Tesla Is Creating a Network Effect," Yahoo, February 2021, https://finance.yahoo.com/news/how-crypto-adoption-by-companies-like-visa-pay-pal-and-tesla-is-creating-a-network-effect-214639389.html.

[63] John Arquilla, "Of Networks and Nations," *The Brown Journal of World Affairs*, no. 14.1 (2007): 199–208, http://bjwa.brown.edu/14-1/of-networks-and-nations/. Pg 208.

forces to communicate over the internet. For example, the Bitcoin Lightning Network sparked a new company named, Impervious.ai which created an entirely new communication protocol and browser which uses the lightning network for secure peer-to-peer interaction.[64] There is potential for cryptocurrency to drive partner force preferences for communication platforms interacting remotely or over-the-horizon and USSOF members should be prepared to connect and interact appropriately.

1. Assist in Targeting and Network Analysis

The U.S. could leverage special operators experience and expertise for targeting methodologies in both steady state and conflict by combining blockchain network analysis with human dynamics in the operational environment. Comptroller's in SOCOM could supplement tactical targeting and analysis efforts for SOF units and the wider interagency working groups for digital assets. The transparency of cryptocurrency blockchains offers a unique ability to analyze and control sanctions but also create risk by publicly identifying individual transaction history.[65] This capability provides a double-edged sword as adversaries can observe the same transaction activity.[66] However, this does not dismiss the potential for effective pseudonymous transactions or communication but does require an increased level of training and knowledge with the cryptocurrency ecosystem. If training and education in the digital currency environment improves, U.S. military advisors can recommend best practices for targeting adversaries and managing the risks from cryptocurrency's transparent and immutable ledgers.

The United States improved techniques to counter terror financing and illicit drug finance networks over the last 20 years however, a plethora of laundering opportunities

---

64 Impervious, "Impervious Project," Your Portal to the P2P Internet, accessed October 31, 2022, https://www.impervious.ai/.

65 Adam Myers et al., "Crypto-Controls: Harnessing Cryptocurrency to Strengthen Sanctions," War on the Rocks, December 9, 2020, https://warontherocks.com/2020/12/crypto-controls-harnessing-cryptocurrency-to-strengthen-sanctions/.

66 Chainalysis Team, "Transparency in Blockchains Senate Hearing," Chainalysis, March 22, 2022, https://blog.chainalysis.com/reports/senate-hearing-underscores-value-of-blockchain-transparency/.

still exist globally, and cryptocurrency has only added to the menu.[67] Contrary to popular opinion, many financial task force experts focused on disrupting terror finance will argue cryptocurrency laundering is overstated and offers a valuable forensic tool.[68] In order for SOF to work safely and effectively with cryptocurrency and blockchains, units will need to incorporate these techniques into "hands on" training where U.S. comptroller's monitor USSOF and partner activity of the blockchain to mitigate risk prior to operational use.

In 2018 ISIL support networks were using steganography techniques to embed messages in images sent over messaging applications and transparent blockchain ledgers while leveraging open-source coding tools to encrypt the communication in plain sight.[69] This level of expertise is not difficult to attain but it must start with basic, overt employment of cryptocurrencies to build proficiency. U.S. military units should begin experimenting with cryptocurrency software and hardware tools in training scenarios to establish a low-risk baseline before attempting complex methods to obfuscate transactions or recommend options to allies. A training event which incorporates cryptocurrency could benefit from dual-purpose education by allowing tactical teams to experiment and simultaneously integrate blockchain forensics from intelligence or comptroller analysts as "red-hat" counterparties.

Comparable to financial intelligence tools which search networks for illicit activity, the transparent ledgers of most digital currencies can help improve accountability of foreign military aid. The digital breadcrumbs from blockchain transactions may lead to better oversight and management of rapidly procured funds or at minimum share insight to the level of digital currency adoption. Immediately after Russia invaded Ukraine in 2022, cryptocurrency donations flooded to Ukrainian government cryptocurrency wallet addresses. However, a more organized and pre-planned distribution system may have

---

[67] Laura Jones and Shawna Sinnott, "Money Talks: How Nonstate Armed Groups Finance Their Operations and Organizations," Modern War Institute, July 15, 2022, https://mwi.usma.edu/money-talks-how-nonstate-armed-groups-finance-their-operations-and-organizations/.

[68] Michael Morell, Josh Kirshner, and Thomas Schoenberger, "Report: An Analysis of Bitcoin's Use in Illicit Finance," The Cipher Brief, April 13, 2021, https://www.thecipherbrief.com/report-an-analysis-of-bitcoins-use-in-illicit-finance.

[69] Lily Hay Newman, "Mysterious 'MuslimCrypt' App Helps Jihadists Send Covert Messages," *Wired*, accessed October 27, 2022, https://www.wired.com/story/muslimcrypt-steganography/.

allowed more time and space for the United Nations to vote and structure support efforts. Additionally, an immediate and deliberate U.S.-led blockchain network analysis system may have offered better insight to Russian digital breadcrumbs over cryptocurrency networks to evade sanctions and help fund the invasion. USSOF should work towards building a structured cryptocurrency and blockchain targeting standard operating procedure with NATO and other allies before the next crisis occurs.

2. Cyber Partnerships and Information Gathering

Ukraine continues to provide a relative roadmap for cryptocurrency utility in support to allies and partners as the threats and opportunities are displayed for the world to take note.[70] As cryptocurrency donations to Ukraine surpassed 50 million U.S. dollars, the Ukrainian government realized the grassroots appeal for many foreigners around the world who are now able to provide modest support through micro-payments and avoid traditional banking fees and limitations.

The Ukrainian government's decision to include cryptocurrency donations and crowdsource military support after an invasion, is a great example of the potential utility of cryptocurrency in conflict areas and offer transparency with blockchain data.[71] The cryptocurrency broker in Ukraine, Kuna Exchange, revealed how the modernized hybrid banking system helps to finance a resistance movement or government during conflict and maneuver between the fiat currency market and cryptocurrency to meet the needs of customers.[72] Ukraine's banking system collapse during the Russian invasion revealed another example for the benefits to self-custody of digital currencies for emergencies, especially in unstable regions.

---

[70] Ananya Kumar and Nikhil Raghuveera, "Can Crypto Deliver Aid amid War? Ukraine Holds the Answer.," *Atlantic Council* (blog), April 4, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-answer/.

[71] United 24, "Aid For Ukraine – Donate Crypto to Ukraine," United 24: The initiative of the President of Ukraine, accessed October 27, 2022, https://u24.gov.ua/.

[72] Romain Dillet, "How Ukraine Is Spending Crypto Donations," *TechCrunch* (blog), March 2, 2022, https://techcrunch.com/2022/03/02/how-ukraine-is-spending-crypto-donations/.

In Eastern Europe "hunt forward" operations by allies with assistance from U.S. units help disrupt nefarious cyber activity. Cyber partnership training and execution complimented with special operations units is long overdue and will strengthen alliances and increase the value proposition for U.S. tactical forces.[73] Cryptocurrency expertise can be an important component of cyber security operations, and the U.S. defense enterprise will improve partnered cyber capability after innovating in the cryptocurrency ecosystem.

Some emerging technologies apply in all aspects of special operations and quickly scale to become unavoidable in conflict such as drones and mobile phones. One commonality among technological innovations are the vulnerabilities at the human layer either through faulty developer code or human end user errors. This analogy exists with cryptocurrency and typically dominate the headlines as speculative traders or greedy business owners will exploit cryptocurrency development and underlying software. An Article in the Cyber Defense Review outlines a value proposition for SOF personnel working in the cyber domain. The authors touch on the human vulnerabilities, often connected to social engineering, that erode cyber security measures. They present the idea SOF should be requested to apply human domain skill sets to defend or disrupt efforts in the cyber domain.[74] USSOF's diverse footprint offers a unique ability to interact with local populations and partner forces to illuminate cryptocurrency sentiment and potentially apply in supplemental security cooperation incentives or better compete with adversary strategies.

The U.S. military community is working to build a closer relationship between U.S. special operations forces, space, and cyber. A recent article published in the *Army Times* outlines the debate for adding more technical skills in operational detachments or tactical units of action.[75] The article references a growing partnership between SOF, cyber, and space departments to support strategic competition and demands for specialized tech-based

[73] Mark Montgomery, "Equipping U.S. Partners in Cyberspace Is a Must," The Cipher Brief, July 2022, https://www.thecipherbrief.com/column_article/equipping-u-s-partners-in-cyberspace-is-a-must.

[74] Patrick M. Duggan and Elizabeth Oren, "U.S. Special Operations Forces in Cyberspace," *The Cyber Defense Review* 1, no. 2 (2016): 73–80, http://www.jstor.org.libproxy nps.edu:2048/stable/ 26267360.

[75] Winkie, "New MOS and Formations Could Come to Army Spec Ops in Tech-Savvy Era."

skills. Many blockchain based applications which utilize cryptocurrency transactions to manage costs and incentive structures are not simple to use. If additional skillsets are delivered to SOF units, it will support practical applications for cryptocurrency in offensive operations. Cryptocurrency may grow to become one of the preferred currencies in cyber domains or the information environment and SOF could begin understanding the atmospherics through surveys in USSOF formations then expand to partner forces and foreign populations in areas of operation.

Emerging peer to peer communication and transaction tools like cryptocurrency may offer a vital bridge between the digital and human domain where elite units excel at building partner capabilities or gathering ground-truth information to help identify adversary vulnerabilities. As the SOF, cyber, space triade continues to build and integrate into training and operations, the diverse backgrounds and expertise in these formations could build creative and region-specific solutions on blockchain and cryptocurrency technology.

3. Include in Resistance Operating Concepts

Digital assets can help concepts in support resistance modernize by offering methods that reduce signature, embrace decentralization, resist censorship, leverage the cyber domain, and serve units with agility and speed. A pragmatic perspective of cryptocurrency will see the innovation simply as software that is programmable for specific decentralized applications. This view helps to determine use cases outside of standard digital financial transactions and check if a solution exists using a cryptocurrency protocol to build a smart contract or DApps. *The Resistance Operating Concept* released by the Joint Special Operations University was developed in conjunction with Baltic and NATO partners.[76] Despite offering immense information for both military and civilian roles in a resistance, the document does not include details for financial technology techniques or capabilities.

[76] Otto C. Fiala, *Resistance Operating Concept (ROC)* (MacDill Air Force Base, Florida: The Joint Special Operations University Press, 2020).

Many of the Baltic nations are applying the resistance operating concept and U.S. Special Operations Command Europe increased assistance to Baltic allies after Russia's annexation of Crimea in 2014.[77] The alternative digital payment rails embraced by Russia, are now leveraged against them by cryptocurrency savvy resistance leaders who understand the processes to procure physical goods and services using in-expensive and commercially available cryptocurrency with satellite internet.

In the *Resistance Operating Concept*, several key networks are necessary to be successful and the underground component is referenced to have "the greatest and most varied responsibilities. Each function should be established and organized prior to a crisis."[78] Financing is outlined as one of the seven key functions of the underground component of a resistance. The financing section of the book further drives home the importance or pre-planning, "Resistance organizations are often aided by allied or partner nations. In fact, we have stressed, these relationships are best begun prior to a crisis through joint training, information exchanges, agreements, and planning coordination."[79] If cryptocurrency was incorporated into resistance planning concepts prior to the Russian invasion in 2022, Ukrainian partners may have seized an opportunity to swap fait currency held in local banks to stablecoins or Bitcoin and remain agile pre-crisis. A cache of emergency funds stored on a cryptocurrency hardware wallet could help purchase both humanitarian and military aid but also allow for resistance leadership access to liquidity or alternative currency to expedite transactions locally. The traditional banks surrounded by a crisis or conflict, who are not prepared to handle instant crowdsourcing funds through digital assets may find support through resistance planning and preparation with digital assets. Substitute currency is briefly mentioned in the *Resistance Operating Concept*, but it does not reference cryptocurrency or expand upon the nuanced ways to properly handle cryptocurrency.

[77] Oren Liebermann, "How Ukraine Is Using Resistance Warfare Developed by the U.S. to Fight Back against Russia | CNN Politics," CNN, August 27, 2022, https://www.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index html.

[78] Fiala, *Resistance Operating Concept (ROC)*. 39.

[79] Fiala. 51.

A central component to survivability in resistance operations is proper organizational structure, specifically decentralization, compartmentalization, and redundancy. Those traits overlap with cryptocurrency principles and begs for continued exploration to ensure consistent funding to complicated resistance operations. Figure 2 from the *Resistance Operating Concept* manual offers a cell structure template for an underground organization in a resistance movement.

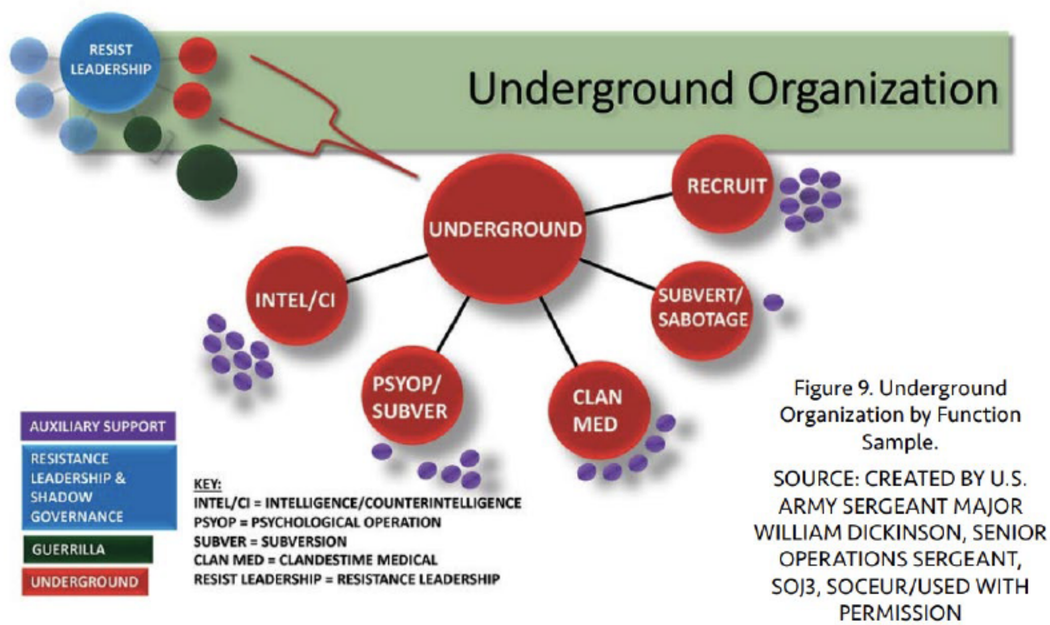


Figure 2. Example of ROC Compartmentalized Structure[80]

The compartmentalized nature of resistance organizations is necessary but difficult to match perfectly in real-world situations. Financial support cells often violate the principles of cell structure since diverse payment rails and alternative currencies are difficult to establish post-crisis or without deliberate planning. Additionally, internet connectivity is typically degraded or destroyed in regions. The Bitcoin network specifically, is built to sustain and continue in the face of catastrophic events as several

80 Source: Fiala. 35.

companies maintain Bitcoin Lightning Network nodes through private satellites. Blockstream and GoTenna are two private companies who developed open-source software and hardware to complete transactions for individuals with no connectivity.[81] Their products utilize mesh networks and TxTenna devices, a subsidiary of GoTenna, to hop service from one node with internet backhaul along a relay of devices to reach the "last mile" or a device with no service and conduct a Bitcoin transaction.[82] The data from the transaction is later published to the blockchain with the help of the mesh network relaying the confirmation details.

Figure 3 is sourced from a research paper directed by the Bank of International Settlements in 2017. This graphic helps emphasize the opportunity to add variance in currency choices for resistance components or functions and helps planners consider the dynamic value or monetary systems around the world. Financial technologies will likely continue to expand in digital global markets which also offer new methods to communicate privately with one another. Peer-to-peer digital payment tools could be incorporated in resistance concepts to create air gaps between highly sensitive cells or build redundancy in attempts to avoid central points of failure.

[81] Daniel Williams, "GoTenna with Blockstream Satellite," Blockstream, May 11, 2019, https://blog.blockstream.com/en-gotenna-satellite-api-integration/.

[82] TxTenna, "TxTenna: Route Around Censorship," November 28, 2022, http://txtenna.com/.

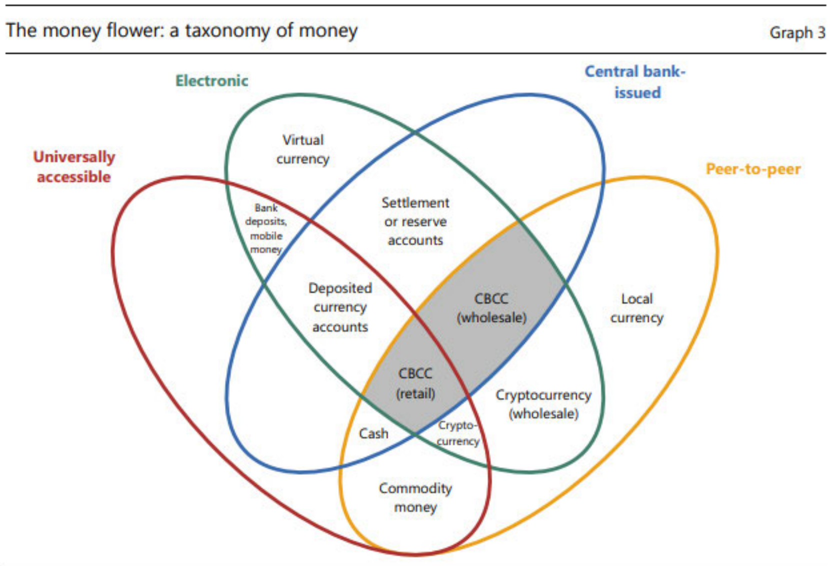


Figure 3. A Diagram Revealing Types of Money and Organizational Overlap[83]

The special operations community would benefit from a proactive discussion with foreign partners to gauge the sentiment toward cryptocurrency and highlight utility for certain special operations use cases for U.S. and allies. As the demographic in many developing regions are dominated by generations under the age of 30, security forces should embrace digitally native communities and prepare to apply cryptocurrency incentives or non-standard techniques and to break reactionary innovation cycles.

U.S. irregular warfare strategies could weaponize the cryptocurrency ecosystem and strengthen a network for integrated deterrence to supplement current contingency plans and offer alternative mediums of exchange if legacy systems are compromised. As military planners continue to refine and develop irregular warfare campaign plans; leaders should be reminded that not all irregular techniques need to be completely covert or clandestine. Some non-standard tools such as cryptocurrencies and emerging financial technologies can assist irregular warfare options by simply reducing the blatant fingerprints of physical U.S.

[83] Morten L. Bech and Rodney Garratt, "Central Bank Cryptocurrencies," SSRN Scholarly Paper (Rochester, NY, September 17, 2017), https://papers.ssrn.com/abstract=3041906. Pg 60

dollars or wire transfers between centralized banks. Sara Dudley in *Strategic Latency Unleashed* articulates the indirect and asymmetric approach cryptocurrency offers by "harnessing this technology to address underlying causes of illicit-actor penetration into vulnerable communities might finally allow SOF forces the ability not only to fight symptoms of bad acting and terror through direct action but also to employ the will of the underlying populations effectively to effect influence on their governance."[84] The learning curve for effective and responsible employment of cryptocurrency is steep and requires iterations of training and testing. The shifting roles of U.S. special operations units and allies in strategic competition requires more flexible options to remain under the threshold of conflict while still supporting resistance campaigns like in Ukraine.

---

84 Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. 280.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE CURRENT STATE OF BLOCKCHAIN AND CRYPTOCURRENCY

This chapter will start with a brief introduction to national defense innovation characteristics and trends cited as reasons for successful adoption. The chapter concludes with a summary and lessons learned from a NPS Blockchain Research Symposium: National Security Implications held on campus and virtually on 12–13 September 2022. The decision to organize a symposium focused on blockchain technology allowed for a larger group of participants and willingness from government organizations to consider dialogue that heavily included the contentious topic of cryptocurrencies. LTC Michael "Kelly" McCoy was the faculty lead and co-author for the symposium executive summary referenced below and the panel concepts referenced in the subsequent annexes.

A. INNOVATION ADOPTION TRAITS CRITICAL FOR SUCCESS

The reasons for successful diffusion of emerging technology vary depending on what publication and scholar but largely associate with organization culture, incubators, mavericks, leaders to champion ideas, and influence from policymakers. Benjamin Jensen's book, *Forging the Sword*, highlights the value of advocacy networks and the impact a profession has on innovation. When discussing doctrinal change in the military, Jensen offers that "cultural heuristics often bound potential solutions for battlefield challenges."[85] The idea of cultural heuristics arguably connects the debate for cryptocurrency utility and appropriateness in U.S. DOD. As referenced earlier, many U.S. citizens struggle to see value in alternative currencies, which may partially feed the heuristics to national security practitioners when conceptualizing the positive benefits to cryptocurrency. This research intends to offer a new lens to observe possible solutions to strategic competition arenas for USSOF and the broader security enterprise.

The research symposium at NPS delivered reason for optimism for responsible innovation of financial technology in DOD by connecting public and private advocacy

---

[85] Jensen, *Forging the Sword*. Pg 13.

networks to incubators and mavericks. When considering Rodgers' five factors, proving relative advantage, overcoming complexity, and compatibility rise to the top as factors for slowing adoption of cryptocurrency in special operations. The headwinds facing cryptocurrency lean heavily toward those three factors and relate back to the larger narrative surrounding cryptocurrency. The connection to illicit activity slows diffusion for U.S. security practitioners and the perception that cryptocurrency is mainly used for sanctions evasions or criminal activity must shift slightly for broader application. The natural heuristics referenced by Jensen also impact the perceptions of Rodger five factors and through deliberate training and education, cryptocurrency utility may expand beyond countering threat finance.

Professional comptrollers in the CTF teams understand cryptocurrency capabilities more than most SOF personnel and will help promote the narrative for cryptocurrency and assist in the innovative approach to transfer knowledge from one sector to another. Digital assets and cryptocurrency undoubtedly face early adoption phase hurdles, but the disruptive financial technology created new opportunities to quickly move money, pay for services, reduce signature, and improve transparency at a global scale which all provides value to SOF. As leaders in DOD advocate for more capabilities in financial technology, the established base of incubators and results-based formation of special operators will likely lead to productive research and development.

B. BLOCKCHAIN AND BEYOND: NATIONAL SECURITY SYMPOSIUM

1. Background and Context

In the Spring of 2022, NPS students and faculty established the Distributed Consensus: Blockchain & Beyond (DC:BB) movement to address the general misperceptions around blockchain technologies. When it comes to present geopolitical dynamics, especially with China, the knowledge gap in these innovations come at a significant opportunity cost to the United States. Specifically, for the U.S. military, blockchain technologies offer potential advantages from supply chain management to decentralized operations. To help counter this problem, DC:BB held a research symposium to initiate a conversation on the role and impact of blockchain technologies in a national security context – with the intent to build awareness, knowledge, and connections that can propel relevant research opportunities for students and faculty at the Naval Postgraduate School (NPS). The following synopsis was written by the author and NPS faculty member LTC Michael “Kelly” McCoy and include interpretations of expert panel discussions. Figure 4 is the formal Naval Postgraduate School flyer utilized for the symposium and distributed publicly prior to the event. NPS’s graphic design department designed the flyer artwork, provided materials, and conducted the printing all in house.

Figure 4. NPS Poster for Blockchain and Beyond: National Security Research Symposium

2. Notable Participants

NPS students and faculty largely represented Defense Analysis, National Security Affairs, and Computer Science departments. Industry leaders who participated included PayPal, Coinbase, Trail of Bits, Espresso Systems, Impervious, improbable.io, and many others. Outside academics and researchers include MIT, Stanford, Congressional Research Services, Starling Labs, Atlantic Council, Center for New American Security, and Lincoln Network.

3. Overview

Over the course of two days, the research symposium covered a wide range of topics ranging from comparative international perspectives on the use and role of blockchain technologies, the potential impact of blockchain technologies on U.S. national security, key policy considerations, operational utility of cryptocurrencies for special operations, use of blockchain technology for targeting, and research opportunities to explore with blockchain. The conference ended with four research presentations, which focused on use of cryptocurrency for SOF, use of blockchain for clandestine communications, contract management, and improving data resiliency through peer-to-peer data security leveraging blockchain technology.

C. TOP THREE POINTS FROM THE SYMPOSIUM

1. Blockchain Resiliency

Civilians impacted by conflict and/or political upheaval may benefit from blockchain technologies by offering immutable records such as digital identities for refugees and an alternative means to transact with digital assets when markets and economies are disrupted. Specific to the U.S. national security audience, global and borderless blockchains offer a new communication mechanism to reach populations and resist censorship or manipulation.

2. United States' Strategic Opportunity

The United States is positioned to assist allies who are looking for regulatory clarity and policy guidance to establish global norms in line with U.S. values for blockchain and digital assets. Panelists and participants noted the importance on the emergent demand for public/private partnerships to quickly improve awareness, capacity, and competency in the complex blockchain ecosystem. The DOD is too often overlooked in key stakeholder positions in U.S. government publications. Experts also routinely coalesced around the need for a whole-of-nation U.S. strategy for blockchain development.

3. Possible Geo-Political Split

Blockchain's diverse technology solutions reveal higher adoption rates with communities in developing regions, typically intended to help improve accountability in fragmented bureaucratic ecosystems (medical records, financial inclusion, federated licensing, and credentials) especially when applied through zero knowledge proofs. There is potential for a divergence in blockchain development and adoption between authoritarian regimes and democratic nations, underscoring the need to understand the implications of blockchain technology in U.S. national security strategies.

D. RECOMMENDED NEXT STEPS

1. Develop Partnerships between Industry, Researchers, and NWSI

Naval Postgraduate School (NPS), with their technical focus and expertise, undercurrent of strategic art and policy proficiency, and intent to support the warfighter in all that they do, is uniquely situated to lead in the exploration of building out research opportunities for blockchain technologies. As highlighted in the key findings, partnerships within this space are the key to moving forward and NWSI is specifically designed for this intent. Developing partnerships with industry leaders like Coinbase, PayPal, and others will be critical to successful adoption of blockchain technologies.

The Post-Conference Actions Taken: One introductory meeting has been completed between NWSI and Coinbase, with follow-on intent to develop education, training, and internship opportunities focused on understanding how to conduct blockchain intelligence analysis.

2. National Security and Blockchain Coalition of the Willing

Establish a decentralized open community of national security professionals, academics, researchers, and industry leaders. The initial intent of the Coalition of the willing (CoW) is to provide a space where information and opportunities focused on distributed ledger technologies and national security can be shared. As the CoW takes shape, we will respond to member demand and create additional opportunities for ideas, research, and opportunities to be shared amongst the group.

The Post-Conference Action Taken: Symposium attendees have been invited to join the Blockchain CoW channel on Signal.

3. Identify Sponsorship for Blockchain Technology Experimentation

As a general-purpose technology, blockchain provides a wide breadth of opportunities. However, given its nascent status in DOD there is little to no understanding how best to employ it. DC:BB recommends identifying either an institutional (U.S. Army Futures Command) or operational (USASOC) command who could serve as an intended sponsor for research and experimentation on blockchain technologies.

Post-Conference Actions Taken: This current thesis work, sponsored by USASOC, explores the utility of cryptocurrency in supporting special operations. This thesis is best situated to demonstrate value and grow opportunity for an enduring sponsorship.

E. PANEL 1: COMPARATIVE PERSPECTIVES FROM AROUND THE WORLD ON BLOCKCHAIN ADAPTATION

1. Objective

The goal of this panel was to focus on a geo-political level and offer a stratospheric view for the audience. The discussion was intended to help articulate how emerging technology is influencing the changing dynamics for the BRICS nations and set the tone for following topics nesting closer to U.S. policy or strategy. Present the question how do other countries, cultures, and region's view, use, and adopt these technologies? Intent is also to challenge American bias that we know best and have the right answer.

2. Key Findings

Panelists brought perspectives from across Asia (China and India), Africa, and Europe, specifically Russia and Ukraine. The panel was able to draw on examples from Ukraine and Africa, offering that blockchain provides immediate benefits in a conflict zone or where political upheaval brings discontinuous change:

Self-sovereign identification methods can help secure identities for refugees, as is the case in Ukraine. The technically advanced population in Ukraine built on this opportunity by leveraging the digital asset ecosystem during the invasion. Through this effort, Ukrainians effectively crowdsourced and stored value outside of the collapsed banking system. Subsequently, adoption across Ukraine and other unstable regions accelerated. Some nations pride themselves on resisting physical U.S. dollar transactions internally, presenting possible problems for national security practitioners in tactical environments.

Blockchain / digital assets can be viewed as either revolutionary or evolutionary – noting how some populations and generations quickly adopted smartphones and mobile payments over traditional centralized banking systems (no SWIFT or credit system).

China recognizes the decentralized and trustless nature of blockchain technology as a threat to their centralized approach to governance. China reached first mover advantage by creating a PRC issued Central Bank Digital Currency (CBDC). This new digital currency was released during the latest Olympics in China with additional plans to scale globally with the help of China's One Belt One Road infrastructure and global saturation in the mobile phone markets.

The high cost of currency conversion/exchange and loss of value for fiat currency helps adoption rates of digital assets and decentralized blockchain technologies.

India has the broadest adoption of blockchain technologies, which should be reassuring given it is the largest democracy in the world.

In observing how quickly sanctions tore down Russia's economy after their invasion of Ukraine, India expressed interest in finding a way to futureproof their economy through blockchain technologies and prevent such economic loss from possible sanctions.

F. PANEL 2: NATIONAL SECURITY IMPLICATIONS OF WEB3

1. Objective

This panel's intent was to discuss the value-side argument behind web3, with the focus on decentralization, autonomy, removing intermediaries, and read-write-create ownership. The discussion attempted to provide varying perspectives capturing whether web3 has national security implications for the United States because it is reshaping the world or if it is all hype and the world, along with its societies within it, are not evolving to a decentralized network state. Additionally, the panelists could offer opinions on how the U.S. could responsibly on-ramp institutions to the ecosystem and mitigate risk of AML/ CTF/Sanctions/Diminished Fiat currency influence?

2. Key Findings

Panelists discussed blockchain technologies in context of the web3 movement, which centers on decentralization, autonomy, and removing state and non-state intermediaries ranging from technology companies, like Google and Meta, to nation-states.

The strategic culture of the United States, with a focus on individual freedoms and penchant towards decentralization is a natural match for web3 – and should be embraced as a soft power advantage against other authoritarian regimes.

The United States is at risk if it fails to lead the adoption of web3 – as it opens the door for other actors (nation-state or network-state) to fill that void with their own special interests that may not align to liberal world order.

G. PANEL 3: POLICY CONSIDERATIONS AND CHALLENGES FOR BLOCKCHAIN TECHNOLOGIES

1. Objective

The objective for this panel was to discuss the evolution of blockchain technologies and their current state, with a focus on how they are perceived by the larger public. Some of the general questions posed: Where are the present opportunities and real-use applications? How do we help move from thinking Ponzi scheme to general purpose technology and enabler? Take a broader strategic outlook toward U.S. Security Cooperation leveraging Web3 technologies, how can the U.S. generate more competency in Web3? How might the U.S. take on a leadership role in global adoption and how would this influence foreign policy? What does it look like to scale in Web3 and is it possible for the U.S. to be a net exporter of Web3 expertise? The intent is to cover where web3/ blockchain technologies have evolved from and where they currently are in terms of capabilities and providing services. Ideally, audience members will leave discussion with key points and considerations about web3/blockchain technology that will help them breakdown barriers to adoption by understanding areas of potential vice unsubstantiated hype.

2. Key Findings

Panelists discussed the evolution of blockchain technologies (web3) and their current state, potential uses, and the policy challenges surrounding them.

When it comes to digital assets, most U.S. policymakers focus their attention on the digital dollar development and analysis of a U.S. approved central bank digital currency (CBDC).

Any blockchain/web3 idea should be evaluated for the business, legal, and distributed ledger technology (DLT) cases that define it. At present, at least one element of the DLT is left vague and undefined.

Most U.S. leaders and policymakers are briefed only on extreme examples or issues, which inhibits responsible development and innovation in both public/private organizations. A quote by Leslie Lamport in 1987 was highlighted to emphasize the trials of distributed consensus; "A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable."[86]

Overarching consensus on the key limitation of public blockchain technologies: Given the immutable chain is public, without zero knowledge proofs, privacy is impossible—as all transactions are public. Given the identification of an individual and their wallet address, their entire financial history (on that wallet) and who they associate with can be quickly discovered.

H. PANEL 4: CRYPTOCURRENCY FOR SPECIAL OPERATIONS

1. Objective

The objective for this panel framework was to discuss the tangible threats and opportunities of specially selected U.S. DOD units experimenting with digital assets and the broader Web3 ecosystem. The goal is to be as concrete as possible with real world tools which may provide value to security practitioners. Offer ideas for how the Web3 community can best articulate the potential without immediately losing non-technically savvy people. State the relative advantage cryptocurrency or blockchain offers compared to legacy systems.

2. Key Findings

Blockchain and digital assets (to include cryptocurrency) offer lesser-known positive use cases like censorship resistant peer to peer payments, better economic inclusion, cheaper global payment system, and a new medium for information and distribution.

Cryptocurrency has already displayed relevance on the battlefield and in moments of crisis by supporting fast payments and crowdfunding a resistance element. Blockchain and cryptocurrency is a social movement, often happening in frontier environments

[86] Leslie Lamport, "Distribution," May 1987, https://www.microsoft.com/en-us/research/publication/distribution/.

overlapping with SOF footprints. Blockchain payment rails can provide creative opportunities for SOF operators to influence and shape an environment with allies and partners.

Synthetic and metaverse environments have both a training and operational role in the military. These environments help transfer real world experiences into virtual environments at scale and enable the testing of modeling concepts. Blockchain technologies, to include digital assets, can help unify different commercial metaverses and transfer value through underlying cryptocurrency settlement protocols. Decentralized information collection, with the help of blockchain and the digital asset ecosystems, can feed into synthetic environments to update data for U.S. and partner force training and employment.

The U.S. military is still exploring where to place blockchain training and expertise within the DOD organizational structures and prefers to match incumbent tools or training with emerging blockchain and financial technology capabilities. SOF is an ideal place to start with research and development to offer recommendations for blockchain or digital asset integration into DOD manning, training, organization, and equipment requirements.

I. PANEL 6: USE OF BLOCKCHAIN THREAT FINANCING AND TARGETING

1. Objective

The objectives for this panel were to discuss threats and opportunities for end users applying blockchain technology and the general targeting methodologies it provides for the U.S. National Security enterprise. Additionally, to help the audience understand the pros and cons of blockchain technology, threat finance role in competition, and the need to educate and build proficiency for security practitioners utilizing cryptocurrency. Highlight some of the current (unclassified) successes but share insight into current gaps in capabilities that stand to benefit from additional research. Discuss the value of threat financing connected to irregular strategies and nested under the concepts for strategic competition / integrated deterrence.

2. Key Findings

There is a need for U.S. national security practitioners to understand the connection of blockchain technology and threat finance, specifically allied targeting approaches and adversary techniques utilizing blockchain.

U.S. personnel and allied end users who are employing blockchain (or digital assets) must understand the strengths and weaknesses of the technology to mitigate and account for risk. The private sector is generally more advanced in monitoring illicit activity on blockchains. Mutual interests exist in building stronger relationships between industry leaders and government agencies, for the purpose of targeting adversary activities, such as ransomware, theft, and laundering.

DOD could establish information sharing programs with the Department of Treasury and Justice to align emerging financial technology with on-going and future irregular warfare security strategies for competition and integrated deterrence.

J. PANEL 7: RESEARCH OPPORTUNITIES AT NPS AND BEYOND

1. Objective

The main objectives for this panel were to share emergent topics and requirements for DLT research; discuss sponsorship opportunities for DLT focused research such as CRADA's; highlight possible opportunities derived from the 2023 NDAA SEC 5913 and other relevant R&D sections. The discussion should help the audience identify future opportunities for research and sponsorship to include specific processes to establish contact and legally develop research agreements or learn from on-going partnerships.

2. Key Findings

The Naval Postgraduate School could serve as a unique hub of technical and conceptual resources by connecting students and faculty with commercial leaders and DOD sponsored research initiatives.

There are many siloed blockchain research programs (Stanford, MIT, DARPA) that support current U.S. national security objectives but there is no coherent campaign, designated organization, or aggregate research and development.

The Biden Administration released a call to action for digital asset development recommendations in March 2022 and a subsequent Digital Asset Framework in September 2022, proving a need to increase collaboration and research.

The 2023 NDAA includes SEC 5913 "National Research and Development Strategy for Distributed Ledger Technology." This guidance will continue to build momentum for fiscal and operational support to blockchain research broader U.S. public/private collaboration.

K. RESEARCH PRESENTATIONS

The utility of cryptocurrency for Special Operations Forces extends broadly across the whole digital asset ecosystem and directly supports methods to modernize partnerships while simultaneously allowing SOF units to share lessons learned with U.S. decision-makers. Cryptocurrency has positive use cases in the resistance operating concept, improving the SOF-Cyber-Space Triade, offering non-standard information collection techniques, provide opportunities to mitigate risk to personnel, and reduce costs from physical cash. Overall, the perceived utility of cryptocurrency in SOF goes beyond techniques to disrupt threat finance processes, however clear regulation and policy will be required to scale beyond niche pilot programs.[87] For the complete recording of the 30-minute presentation from the research symposium on 13 September 2022, see https://nps.edu/web/nps-video-portal/-/cryptocurrency-utility-for-special-operations.

Covert communications over the Ethereum blockchain is possible and relatively simple if a modest amount of training is dedicated to the process. The transparency of the Ethereum blockchain allows for the immediate publication and distribution of financial transactions, which helps prevent manipulation by third parties. However, prior planning

[87] Michael Rowen, "Cryptocurrency Utility for Special Operations - Video Portal - Naval Postgraduate School," September 13, 2022, https://nps.edu/web/nps-video-portal/-/cryptocurrency-utility-for-special-operations.

is essential and required between the two communicating entities to ensure covert communications are effectively exchanged. Transparent blockchains are pseudonymous, which means public wallet addresses are observable while personal identity behind the transaction is not apparent. By utilizing open-source encryption tools, it's possible to send a transaction from a pre-planned wallet address to a random (unaffiliated) address which holds the encryption hash intended to be decrypted into the covert message.[88]

CSE Engineering presented their blockchain product leveraging the benefits of smart contracts (customizable programs/applications on blockchain) to automate enforcement of spending controls, dictate payment rules, check for sanctioned wallets, and simplify reporting. Smart contracts offer unavailable solutions to some of biggest challenges facing government financial management—specifically for supply chain traceability and internal controls.[89]

Constellation Network shared research for their product currently in SBIR contract USTRANSCOM to create an end-to-end data security solution using blockchain and distributed data management. "The goal is to further develop the solution as a standard for use in securely exchanging mission data with commercial partners across the Defense Transportation System (DTS)".[90]

---

[88] "Framework for Anonymized Covert Communications: Ethereum Blockchain-Based Concept - Video Portal - Naval Postgraduate School," accessed October 31, 2022, https://nps.edu/web/nps-video-portal/-/framework-for-anonymized-covert-communications-ethereum-blockchain-based-concept.

[89] "CSEngineering – Engineering Freedom through Digital Transformation," CSEngineering, accessed October 31, 2022, https://cse-corp.com/.

[90] "Constellation Network: Trusted in Federal Cybersecurity," Constellation Network website, accessed October 31, 2022, https://constellationnetwork.io/.

V. CONCLUSION

The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. Beyond financial settlements, cryptocurrency offers the ability to build private and secure applications on public blockchain infrastructure to deliver valuable non-standard communication or data management tools for military operations. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace.

The DOD should not sit idly by and watch financial technology outpace USSOF capabilities or allow China and Russia to manipulate digital currency markets to proliferate invasive CBDC's and diminish U.S. influence. The DOD and more specifically, SOCOM should push operational leaders to identify ways to operationalize cryptocurrency through tailored non-standard applications to support special operations concepts. The public-private innovative cluster for cryptocurrency can help inject new thinking for gray-zone operations and SOF's role in strategic competition. The disruptive nature of "internet money" demands an open mind to account for the relative advantage in both offensive and defensive postures.

Tactical units should start to view cryptocurrency as software or nuanced pieces of equipment to handle carefully but remain willing to use for training purposes. Military leaders should work towards a standard validation pathway comparable to current pay agent and field ordering officer programs of instruction to normalize digital asset use in training and operations. SOCOM's comptroller community will be invaluable by providing connective tissue to interagency partners and sharing legal boundaries as changes or updates to regulation occurs. Ultimately, a hybrid version of digital asset employment may be the logical direction for scaling digital asset and cryptocurrency utility in military operations.

A Harvard Business Review article in 2014 titled, *Understanding "New Power,"* offers a framework of old and new power models for business. The authors state, "new power operates differently, like a current. It is made by many. It is open, participatory, and peer-driven. It uploads, and it distributes. Like water or electricity, it's most forceful when it surges. The goal with new power is not to hoard it but to channel it."[91] The elements of new power according to the authors accurately depict both extremes of cryptocurrency markets today such as intoxicating hype and influential networks disrupting entrenched old power. Cryptocurrency warrants attention from SOF units since the communities and conditions with high levels of adoption correlate to SOF areas of operation. Special operations units are well suited to channel the new power of cryptocurrency and proactively support national security objectives.

A. RECOMMENDED WAY FORWARD

One hypothetical pilot program for tactical forces would be granting approval to store stablecoins and cryptocurrency with electronic wallets on designated mobile phones. If a U.S. special operations team identifies high adoption rates in their assigned partner force and region, they should have an opportunity to request access to digital currency during the deployment. A future where tactical teams utilize smart phone applications and digital wallets to store stablecoins will offer the advantage of immediately accessing the cryptocurrency market by swapping stablecoins for cryptocurrency tokens. This concept can be replicated in the United States during training events and refined over time to incorporate recommendations from the U.S. national security enterprise.

A modernized digital future would help prevent moments when the only currency option for service members is to withdraw in person and carry physical bundles of cash, often in dangerous environments and elevating risk to military members and customers. The cryptocurrency peer to peer ecosystem, known as decentralized exchanges, and certain cryptocurrency mobile application tools allows end users to immediately swap their

[91] Jeremy Heimans and Henry Timms, "Understanding 'New Power,'" *Harvard Business Review*, December 1, 2014, https://hbr.org/2014/12/understanding-new-power.

stablecoin token with another alternative cryptocurrencies within seconds.[92] If a foreign merchant prefers to receive a specific cryptocurrency, the service member or customer can rapidly swap digital currencies and send payments to the merchant's wallet address. This payment agility at the point of sale would help many special operations units deployed and at the edge of conflict, choose the best currency for every unique circumstance. Funds for each operational deployment are requested well in advance and require multiple levels of accountability. Tactical cryptocurrency pilot programs may also reveal streamlined accountability with the help of transparent blockchain ledgers and reduce overall expenses from travel and currency conversion fees.

Figure 5 presents a synopsis of the pilot program concept and was developed for this thesis with the help of NPS's media fusion office. The concept presents a basic step in cryptocurrency capability for tactical SOF members for peer-to-peer transaction options. This workflow example is intended to show an overt process for financial settlements using cryptocurrency and currently available commercial products and services.

[92] Arcane Research, "The State of Crypto - The P2P Market" (Norway: Arcane Research, October 1, 2020), https://arcane.no/research/reports/the-state-of-crypto-the-p2p-market.

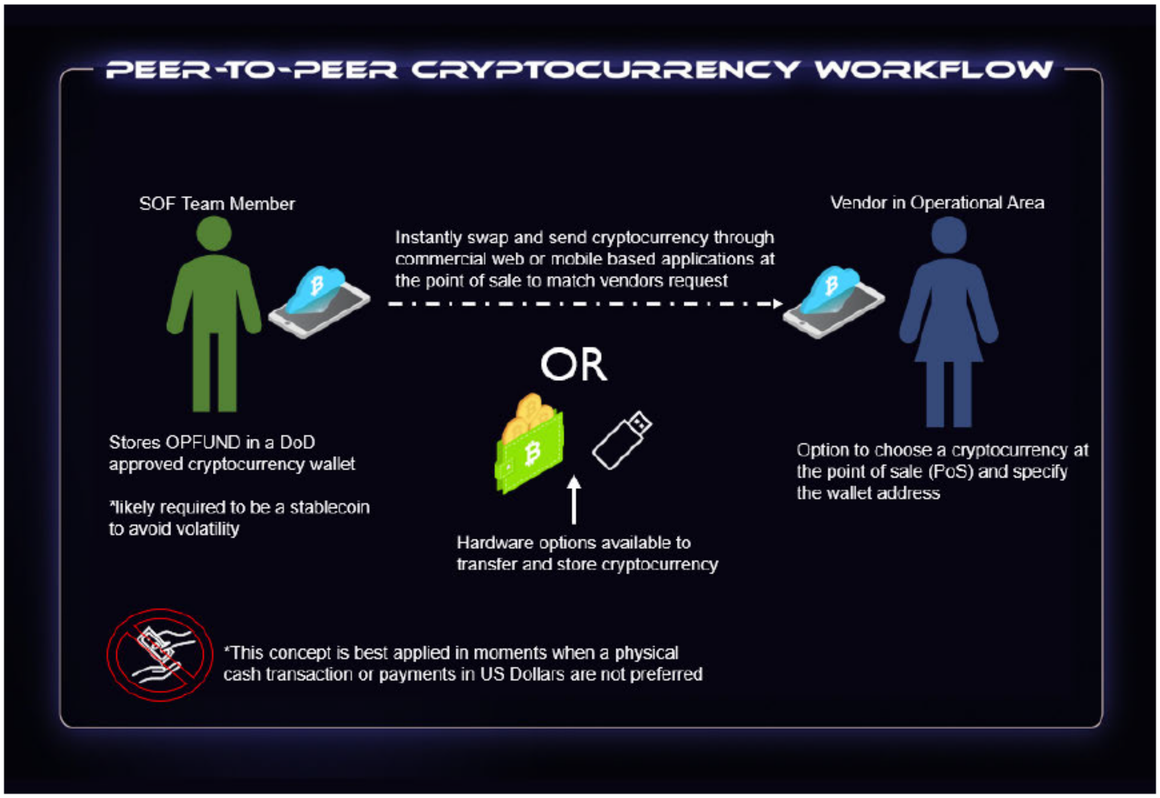


Figure 5. Pilot Program Workflow

Figure 6, also created for this thesis with NPS's media fusion office, is intended to show a workflow with commercial business logos to further emphasize the range of products available to assist in pilot program development and experimentation. The logos represent steps that may be used along a peer-to-peer transfer process but this is not all encompassing or depicting the mandatory process for all transactions. Circle's stablecoin, USDC, and Bitcoin were the focus for this particular example, but many comparable companies exist for other cryptocurrency blockchains. The intent with this graphic is to reveal the diverse ecosystem which includes decentralized identity, stablecoin options, electronic wallets, mesh network devices, and private internet browsers. Figure 7 provides a legend for the company logos depicted in Figure 6 workflow.

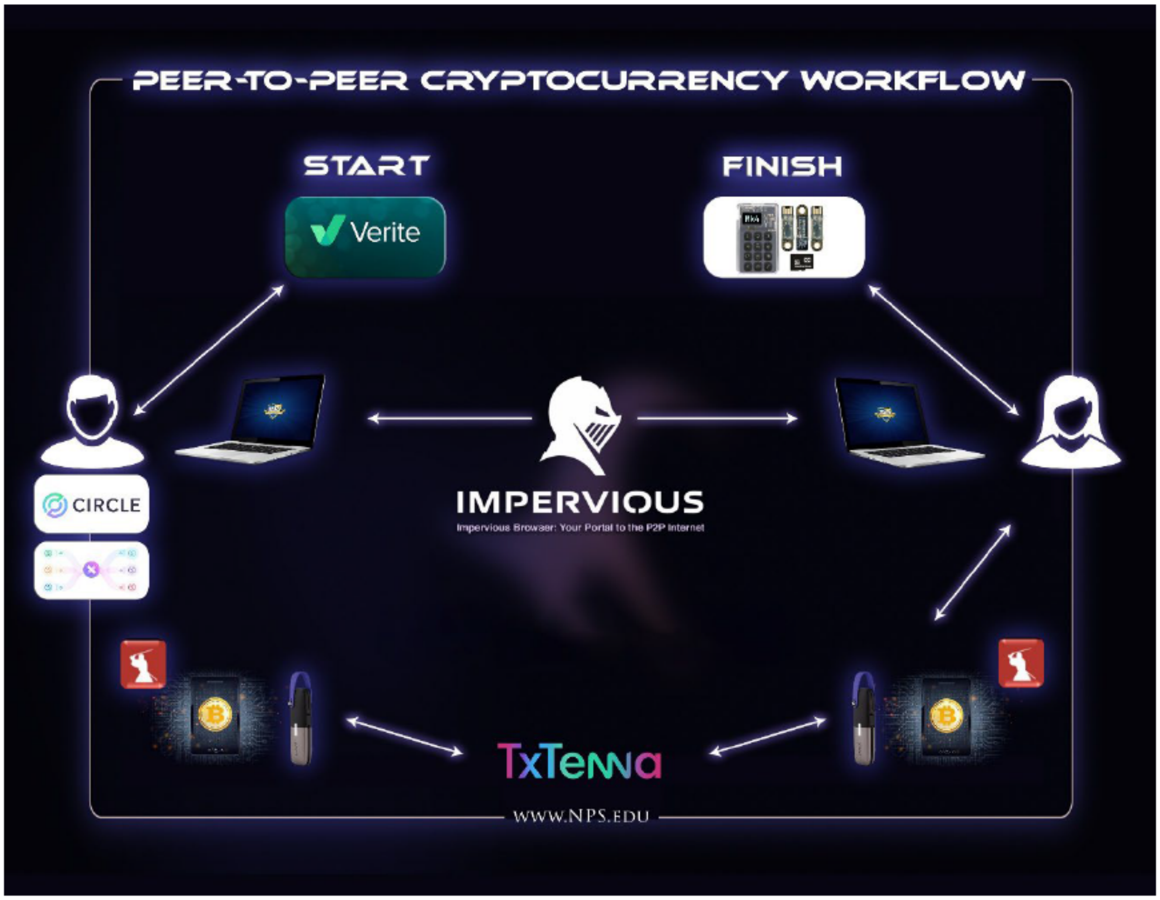


Figure 6. Commercial Workflow Example

Figure 7. Legend for Commercial Company Workflow

The workflow examples attempt to provide a starting point for additional research and development for end-users or tactical teams. The example presented is not frictionless and does require additional steps to complete depending on the point of origin for funds. The general framework helps to set the baseline for including a proof-of-concept training exercise for USSOF. Additionally, cybersecurity testing and assessments should be implemented prior to operational use of these services. However, SOF should begin education and local training with this type of basic pilot program or workflow.

Overall, a cryptocurrency pilot program is an attractive way of developing a niche tool to supplement legacy processes and one that encourages creative problem-solving, accountability, and novel risk mitigation when applied correctly. As proficiency increases for building smart contracts and DApps with cryptocurrency, SOF formations will likely find additional use cases or offer better training and solutions to partner forces.

As U.S. special operations forces continue to build organic cyber talent, the barrier for entry into the cryptocurrency ecosystem will become more manageable. The initial steps for experimentation should be developed now to account for administrative hurdles prior to testing various overt concepts and develop a baseline proficiency to mitigate risk beyond benign operational use cases.

A survey or poll among the USSOF formation is a reasonable option to start developing awareness of cryptocurrency literacy or curiosity. Additionally, a proactive discussion between operational units and partner forces globally can help gauge interest and adjust future research accordingly. Civilian and military research facilities may serve as a valuable hub to connect commercial projects with battlefield challenges or the military incubators attempting to harness digital asset concepts. The DOD innovation network can help matchmaking between tactical end-users who bring real-world use cases and commercial companies with expertise to tailor software applications or deliver unique hardware. The disruptive nature of financial technologies is forcing SOF to consider financial lines of communication as legitimate options for nonkinetic effects from friendly and enemy forces.[93]

B. RECOMMENDED AREAS FOR ADDITIONAL RESEARCH

The 2023 NDAA SEC 5913 highlights research for distributed ledger technology and this could assist with cryptocurrency education and broader understanding of the threats and opportunities. The consensus around blockchain or DLT research allows for exploration of cryptocurrency testing and localized training to deliberately build understanding and capability in SOF. Research institutions connected to the innovation network can enable project teams of researchers for quantitative analysis and cybersecurity assessments of the open-source software which also helps reduce the burden on operational DOD cyber organizations.

[93] Smith, "Applying Financial Capabilities to Achieve Multi-Domain Effects: Using Financial Capabilities Operationally Rather Than Transactionally." 55.

The transparency of public cryptocurrency blockchains allows access to new types of data sets for operational research faculty and students. Academic institutions could develop more cooperative research agreements with commercial blockchain analytics companies to maintain a steady stream of information to merge network analysis and social sciences depending on the accuracy of region-specific data. This type of research would benefit the DOD and many other stakeholders working to responsibly develop digital asset regulation in the United States.

Climate security research with cryptocurrency, and specifically "proof of work" processes such as Bitcoin, may identify beneficial steps to improve prototyping, testing, and operating green energy devices in austere environments. The thought to include Bitcoin mining hardware next to green energy generation like wind, solar, and thermal has been discussed but little has been lobbied for government sanction testing in austere locations or when energy transfer infrastructure is expensive or non-existent. Bitcoin mining devices connected to sustainable energy prototypes may seem inappropriate but the potential to offset the fiscal burden for research and development through Bitcoin rewards may help in incentivize future experimentation. Since SOF units are typically deployed to austere locations and could benefit from sustainable energy equipment, additional research to assist interagency, academic partners, or allies in testing prototypes may be mutually beneficial.

Perhaps the most intriguing area for continued research between cryptocurrency and special operations is from non-standard communications concepts. Specifically, mesh networks incentivized through cryptocurrency may offer unique ways to approach security strategies. Companies like Helium and Pollen Mobile revealed grassroots models to help scale a mobile 5G network with a local population by offering rewards for "proof of coverage."[94] The benefits of inherent encryption standards on blockchain and smaller form factor routers or antennas may lead to reliable peer to peer communication protocols and mesh networks to cover regions with limited service. Additionally, the opportunity to circumvent Chinese owned 5G infrastructure with the help of local communities

[94] Decrypt / Andrew Hayward, "Samsung, Qualcomm Back FreedomFi, Helium's 5G Crypto Network Partner," Decrypt, March 15, 2022, https://decrypt.co/95153/samsung-qualcomm-back-freedomfi-heliums-5g-crypto-network-partner.

maintaining decentralized networks may prove invaluable in the future. However, more research is required to help determine feasibility, security concerns in both hardware and software, and country specific obstacles for spectrum ownership among many other variables.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. PANEL CONCEPT SHEET 1

Panel 1 (12 September 2022)

Title: Blockchain & National Security Around the BRICS

Objective: This panel should focus on a geo-political level and offer a stratospheric view for the audience. Help to articulate how emerging technology is influencing the changing dynamics for the BRICS nations and set the tone for following topics nesting closer to U.S. policy or strategy. How do other countries, cultures, and region's view, use, and adopt these technologies? The intent is also to challenge traditional American bias that we know what is best and have the right answer.

Panel Members:
Moderator: Dr. Leo Blanken: NPS Faculty Lead/ Co-Founder for Applied Design for Innovation Curriculum

Panelist 1 – Mark Gabriele: USG Senior Advisor, Lead Author of 2018 DHS Report on Blockchain Technologies, (Russia)

Panelist 2 – Jonathan Bench: International Business Attorney, Harris-Bricken, (China)

Panelist 3 – Founder bc13o Technology Group, (Ukraine)

Panelist 4 – Selina Hayes: Founder / CEO of Hayes Group, (Africa)

Panelist 5 – John Medel: International Policy Team, Coinbase, (India)

Framing Questions:

Mark – In developing the 2018 DHS report on blockchain technologies, what was your take-away on how blockchain has been adopted around the world? Specifically, can you share any examples of what Russia was or has been doing?

Jonathan – China is a highly centralized nation, how does the decentralized nature of blockchain fit into China's vision of the future? Is there a disconnect between the people and the government of China? What are the challenges and opportunities Facing China with the emergence of web3?

bc13o Technology Group – Being on the ground in Ukraine for a few months now, can you tell us about the role you have seen crypto and blockchain take on? Is there a use for blockchain on the battlefield? In the conflict space? What does that look like?

Selina – Adoption of cryptocurrency in Africa is rather high compared to the rest of the world. Why is that? Where do you think the U.S. fits into Africa's FinTech growth comparatively to China, Russia, India? With the ongoing winter for crypto, hasn't that placed those who trusted their use at a greater disadvantage and loss than if they stuck to their country's fiat?

John Medel – India has the highest adoption rate of web3 and crypto. Why is that? What is it that drives adoption in India and is it unique to their culture or something we'll see across the globe as adoption scales? Looking out a decade, what are the potential outcomes of India being a leader adopter of web3?

General Questions for Conversation:

1. On a scale of importance, where would you rate blockchain technologies? What would you equate blockchain technology too – especially in the context of your countries? Is this really a revolution or is it hype? To the point of this event – does your respective countries governments view any elements as a national security threat or maybe a soft or hard power opportunity?

2. How have blockchain technologies shaped the elements of national power in your country? Has there been impacts in your country's ability to flex power diplomatically, via information, militarily, or economically? Or is blockchain and the associated web3 movement purely a private sector impact?

3. The United States is at a critical point in the history of blockchain regulations. From your perspectives, what are the larger impacts if the United States seeks to clamp down on innovation in this sector? What are the impacts for the U.S.? What are the impacts in your respective countries? Would there be any?
    a. Follow-on Question – What should the United States learn from your respective countries experience in dealing with blockchain technologies and crypto?

4. How has the use of blockchain technologies, like cryptocurrencies changed over the years in your respective countries? How has government control or regulation shaped it?

5. Let’s talk about other elements of blockchain technologies – Decentralized Autonomous Organizations – or DAOs. DAOs are easily global in nature. Has there been adoption of DAOs or explicit prohibition of participating in them in your respective countries? How might the strategic culture of your country shape or influence the DAO movement? Or will the DAO movement potential shape some countries?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PANEL CONCEPT SHEET 2

Panel 2 (12 September 2022)

Title: National Security Imperative or Peril of web3

Objective: Discuss the value-side argument behind web3 – the focus on decentralization, autonomy, removing intermediaries, and read-write-create ownership. Provide varying perspectives capturing whether web3 has national security implications for the United States. Is web3 reshaping the world or is it all hype?

Panel Members:
Moderator – CPT Jay Long: Innovation Officer

Panelist 1 – August Cole: Renowned author exploring the future of conflict through Fictional Intelligence storytelling, non-resident senior fellow at Atlantic Council among several others

Panelist 2 – Antonio Garcia Martinez (AGM): Author, internet native, early ad-tech developer, and "research scientist"

Panelist 3 – Spencer MacDonald: Building and enabling talent, supported by mutual understanding, to drive effective technological innovation within DOD

Framing Questions:

August – Can you walk the audience from web 1.0 to web3 and what possible implications you see on the horizon? What do you see life, and more specifically, our national security challenges and opportunities looking like in the future?

Antonio – The Network State is an emerging idea born out of web3, can you help the audience understand what a Network State is and how it could be part of our future? What are the key elements that are unique from web3 that make it possible?

Spencer – The U.S. Government, especially DOD, has had their challenges in working with the tech industry. Are we doomed to repeat our mistakes? What does success look like for the United States national security apparatus to leverage the opportunities afforded by web3?

General Questions for Conversation:

1. Is web3 a natural match for America and the liberal world order born out of World War 2? How might web3 be a destabilizing impact on our current systems? How might they be co-opted against us by China or Russia?
2. I can't mention blockchain in my professional circles without having to be apologetic…how do we move beyond the hype and speculation? How do we get towards achieving greater adoption? And maybe more important…greater adoption of what?
3. To the title of this panel, is web3 an enabler, a threat, or a distraction for national security? How so?
4. Focusing on decentralization and trustlessness, how might we see that play out in future warfare? Is the U.S. going to sponsor bounties to go after our adversaries?

APPENDIX C. PANEL CONCEPT SHEET 3

Panel 3 (12 September 2022)

Title: Policy Challenges: Opportunities for Strategic Competition

Objective: Discuss the evolution of blockchain technologies (web3) and their current state – with a focus on how they are perceived by the larger public. Where are the present opportunities and real-use applications? How do we help move from thinking ponzi scheme to general purpose technology and enabler? Take a broader strategic outlook toward U.S. Security Cooperation leveraging Web3 technologies, how can the U.S. generate more competency in Web3? How might the U.S. take on a leadership role in global adoption and how would this influence foreign policy? What does it look like to scale in Web3 and is it possible for the U.S. to be a net exporter of Web3 expertise? The intent is to cover where web3/blockchain technologies have evolved from and where they currently are in terms of capabilities and providing services. Ideally, audience members will leave discussion with key points and considerations about web3/blockchain technology that will help them breakdown barriers to adoption by understanding areas of potential vice unsubstantiated hype.

Panel Members:
Moderator – Tom Dixon: Senior Account Executive, Lukka. Former DIA Chief of Operations

Panelist 1 – Michael Mosier: General Counsel, Espresso Systems. DoJ; White House NSC; Treasury; adj_prof. Georgetown Law

Panelist 2 – Alex McLeod: Parlay Protocol, Blockchain uses for businesses

Panelist 3 – Evan Sultanik: Computer Security Researcher, Trail of Bits

Panelist 4 – Chris Jaikaran: Policy perspectives, Congressional Research Service

Panelist 5 – Jesse Spiro: Header of PayPal cryptocurrency wing to work on regulatory policy

Framing Questions:

Framing of Blockchain Technologies – Hype vs Reality:

Chris – Let's talk about the inherent limitations of blockchain technologies and the web3 movement…there are some serious hurdles to the hype. Can you break that down for us?

Evan – You wrote a piece covering whether or not your problem needs a blockchain solution. Can you break down the space in which blockchain is best designed to function within?

Alex – Given your experience, what innovative successes have you seen from using blockchain technologies? Given what Chris and Evan laid out, where do you see the opportunities?

Policy Challenges for Blockchain – What are the policy discussions around this technology? Why do they matter?

Michael – You've been on the frontlines of the executive branch in looking at the darker problems and illicit activities people point to as to why blockchain is bad. Can you give us an inside look of how blockchain technologies like crypto are being viewed inside the executive branch? What are the concerns and problems shaping those discussions?

Chris – With your work and research, what have you consistently seen to be the most pressing policy issues generated by blockchain associated technologies?

Jesse – From the private sector perspective, what are the essential policy problems you see that need to be solved? Is regulation a good thing or a bad thing? How big of an impact can these discussion cause?

General Questions for Conversation:

1. Is web3 and its associated blockchain technologies an important sector for the United State to take lead in? Is it a public problem or a private sector issue?

2. Blockchain is a bit of a dirty word within the government and largely to anyone who isn't an early adopter. Can blockchain move from being considered a ponzi scheme to general purpose technology and enabler? How do we do this?

3. Taking a broader strategic outlook toward U.S. Security Cooperation and leveraging Web3 technologies, how might the U.S. generate more competency in Web3, to take a leadership role in global adoption and how does this influence foreign policy?

4. What does it look like to scale in Web3 and is it possible for the U.S. to be a net exporter of Web3 expertise?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. PANEL CONCEPT SHEET 4

Panel 4 (12 September 2022)

Title: Cryptocurrency Ecosystem: The Operator's New Infrastructure?

Objective: Discuss the tangible threats and opportunities of specially selected U.S. DOD units experimenting with digital assets and the broader Web3 ecosystem. The goal is to be as concrete as possible with real world tools which may provide value to security practitioners. Offer ideas for how the Web3 community can best articulate the potential without immediately losing non-technically savvy people. State the relative advantage cryptocurrency or blockchain offers compared to legacy systems.

Discuss questions posed by operational members of the military such as: how does the global adoption rates of the cryptocurrency ecosystem potentially impact the broad U.S. military footprint? What is the future direction of NFTs and where are areas of potential research to push NFTs to the next level? Will novel decentralized identification methods overtake some of the utility functions from NFTs? What is the process to merge physical assets or processes to help build logical NFT functionality and will it diffuse into the national security or defense sector? How can synthetic environments improve U.S. military training and operations? How will the metaverse or other synthetic environments integrate with digital assets and is there a role for the military?

Panel Members:
Moderator – MAJ Scott Rowen: NPS Student, U.S. Army, 3rd Special Forces Group

Panelist 1 – George LeMeur: Head of business operations at Impervious.ai, fmr 1st Special Forces Group

Panelist 2 – Cameron Armstrong: Founder VF Protocol, eCommerce Start-up and financial modeling, former U.S. Army Infantry Officer

Panelist 3 – Michael Pavek: Senior technical product manager at Improbable.io, former U.S. Army Officer

Panelist 4 – LTC Chris Robinette: Battalion Commander 5th BN SWCS, PWC Finance and Acquisition, former 10th Special Forces Group

Framing Questions:

George – Impervious uses the term Peer-to-Peer to discuss the tools and infrastructure it builds. Why do you make this distinction and how is p2p relevant to operators?

Cameron – Where do you see the future direction of NFTs and what is the relevance for national security? Will novel decentralized identification methods overtake some of the utility functions from NFTs?

Michael – How can synthetic environments improve U.S. military training and operations? How will the metaverse or other synthetic environments integrate with digital assets and is there a role for the military? Can you touch on the question if blockchain is truly helpful and/or a practical tool for metaverse development and scaling?

Chris – How do you see leaders shifting their mindset towards emerging technologies and including methods to integrate these concepts into doctrine, manning, training, and equipping? Does the idea for creating a new and more technical military occupational specialty into SOF units have weight and is it needed?

General Questions for Conversation:

1. What are your opinions regarding the learning curve or the barrier of entry at some traditional tactical units for incorporating Web3 technologies?

2. How do you approach the opinion many of these Web3 technologies are not important to military operations or digital assets are outside of the scope of DOD operations?

3. Can emerging decentralized identification technology help mitigate the risks for service members if granted approval to use more blockchain, digital assets, metaverses in military operations? How does the transparency of public blockchains create a double-edged sword for military units?

4. Any recommendations for the U.S. Defense enterprise to responsibly integrating advanced Web3 commercial company products with cumbersome but motivated DOD/SOF units, for example the potential branding or marketing issues when associated with governments?

APPENDIX E. PANEL CONCEPT SHEET 6

Panel 6 (13 September 2022)

Title: Targeting and Counter Threat Finance

Objective: Discuss threats and opportunities for end users applying blockchain technology and the general targeting methodologies it provides for the U.S. National Security enterprise. Help the audience understand the pros and cons of blockchain technology, threat finance role in competition, and the need to educate and build proficiency for security practitioners utilizing cryptocurrency. Highlight some of the current (unclassified) successes but share insight into current gaps in capabilities that stand to benefit from additional research. Discuss the value of threat financing connected to irregular strategies and nested under the concepts for strategic competition / integrated deterrence.

Panel Members:

Moderator – MAJ Aaron Heaviland: NPS Student, Foreign Area Officer, previously in 75th Ranger Regiment

Panelist 1 – COL Brian Smith: USASOC Counter Threat Finance, SOF centric Targeting and Finance approach in Irregular Warfare

Panelist 2 – Alex Zerden: Lawyer, fmr White House Advisor, U.S. Treasury CTF in Kabul

Panelist 3 – Mike Aleman: Senior Director at PayPal's global financial crime and blockchain innovation development

Framing Questions:

> **Alex and Brian** – Can you help the audience understand the pros and cons of blockchain technology and the connection it has with threat finance? How does it play a role in competition with other nations or organizations, and touch on the need to educate and build proficiency for security practitioners utilizing cryptocurrency.
>
> **Brian** – Can you discuss threats and opportunities for end users applying blockchain technology and the general targeting methodologies it provides for the U.S. National Security enterprise.

Alex – Can you discuss civilian lines of effort focusing on the Department of Treasury and Justice that covers strategies for combating terrorism financing, laundering and illicit finance and then operational methods such as sanctions designations and criminal prosecutions?

Michael – Can you help some of the DOD population contextualize how PayPal or generally how private industry frame illicit finance and counter terrorism financing?

General Questions for Conversation:

1. Can you share insight to the role of the darknet to include negative impacts from the proliferation of ransomware and cyber intrusions/hacking? How does the transparency of blockchain factor into the analysis for CTF and anti-money laundering compliance?

2. What is the black swan event that keeps you up at night or generates the most cause for concern?

3. In relation to CTF, does the U.S. need to clarify the legal framework for digital assets and blockchain technology or are the current legal boundaries adequate and effective? If changes are needed, will minor adjustments to definitions and policy help fill the legal gap or is a drastic shift in guidance and regulation required?

4. Is there a need for U.S. SOCOM to better leverage public-private engagements to understand new business models, identify and address development obstacles, threat identification, attribution, or techniques?

APPENDIX F. PANEL CONCEPT SHEET 7

Panel 7 (13 September 2022)

Title: Distributed Ledger Technology (DLT) & Research Opportunities

Objective: (1) Discuss emergent topics/requirements for DLT research; (2) Discuss sponsorship opportunities for DLT focused research (i.e. CRADA); (3) Highlight possible opportunities derived from the draft 2023 NDAA SEC 5804 and other relevant R&D sections. The discussion should help the audience identify future opportunities for research and sponsorship to include specific processes to establish contact and legally develop research agreements or learn from on-going partnerships.

Panel Members:
Moderator – Sheila Vaidya: Emerging Technology Portfolio Lead, NWSI, NPS

Panelist 1 – Dr. Evan Sultanik: Computer Security Researcher at Trail of Bits
(Topic: DARPA sponsored research)

Panelist 2 – Jonathan Dotan: Director of Starling Lab, Stanford University
(Topic: Opportunities for innovative use of blockchain solutions at the tactical level)

Panelist 3 – Gene Keselman: Executive Director of MIT Innovation Initiative
(Topic: Opportunities for applied research and innovation from MIT perspective)

Panelist 4 – Will Schweitzer: Protocol Labs
(Topic: Emerging areas for DLTs that coincide with national security applications)

Panelist 5 – John Kothanek: Vice President Global Intelligence Cryptocurrency, Coinbase, Blockchain Analytics (Topic: Blockchain analytics as an emergent research method)

Framing Questions:

> **Evan** – What has been your experience in developing research for DARPA sponsored research? Do you see both demand and room for growth for more in depth research?
>
> **Gene** and **Jonathan** – How have you seen academic research into blockchain technologies evolve over the year or years? What has worked? What failed?

John – How do you see blockchain changing research methods today or in the near future? What kind of opportunities does that open?

Will – Drawing on your tactical special operations experience, and current perch with Protocol Labs – how would you want to focus emerging research to generate opportunities at the tactical level?

General Questions for Conversation:

1. Let’s talk relevance, timeline, and research opportunities. Why are blockchain technologies relevant to the Navy or the U.S. military more broadly? How would you assess the technological readiness of these technologies? Are we talking adoption within the next 10 years, or is it further out? What are the research opportunities you see for NPS students and faculty?

2. For someone who doesn’t know blockchain, explain to me where the research opportunities are in this space? What type of academic research would be useful, especially from an applied research perspective?

3. On the TRL scale, what are the emergent topics researchers should focus on from your perspective?

APPENDIX G. DIGITAL ASSET AND CRYPTOCURRENCY RESOURCE GUIDE

These resources are intended to provide a starting point to discover more knowledge in the digital asset ecosystem and increase understanding in cryptocurrency terminology.

Many of the resources are cited in the thesis however, this product may help reduce the burden when searching for reading material or clarity.

The reports or websites recommended below are only a snapshot of the ecosystem and cover several years of innovation for the digital asset markets or analysis in national security affairs.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abdalla, Alyce. "U.S. Strategy and the Future of Money: Advancing U.S. Interests During a Financial Transformation." The Strategy Bridge, August 2022. https://thestrategybridge.org/the-bridge/2022/8/29/us-strategy-and-the-future-of-money.

Antonopoulos, Andreas M., and Gavin Wood. *Mastering Ethereum: Building Smart Contracts and DApps*. First edition. Sebastopol, CA: O'Reilly, 2019.

Arcane Research. "The State of Crypto - The P2P Market." Norway: Arcane Research, October 1, 2020. https://arcane.no/research/reports/the-state-of-crypto-the-p2p-market.

Arquilla, John. "Of Networks and Nations." *The Brown Journal of World Affairs*, no. 14.1 (2007): 199–208. http://bjwa.brown.edu/14-1/of-networks-and-nations/.

Bech, Morten L., and Rodney Garratt. "Central Bank Cryptocurrencies." SSRN Scholarly Paper. Rochester, NY, September 17, 2017. https://papers.ssrn.com/abstract=3041906.

Berg, Leandro. "RTF Report: Combatting Ransomware." Institute for Security and Technology (IST). Accessed August 13, 2021. https://securityandtechnology.org/ransomwaretaskforce/report/.

Blanken, Leo. "Special Operations Forces as a Rapid Prototyping Laboratory." Edited by Philip Swintek. *Center for Global Security Research*, January 2021. http://hdl.handle.net/10945/67924.

Boston, Federal Reserve Bank of. "Project Hamilton Phase 1 Executive Summary." Federal Reserve Bank of Boston, February 3, 2022. https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx.

Brady, Rich, and Bill Arnold. "Data Analytics: From Raw Data to Informed Decisions." *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022). https://asmconline.org/armed-forces-comptroller/.

Breede, Christian, Kevin Stringer, and Sara Dudley. "A Counter-Threat Finance Approach to Competition." The Politics of Special Forces, n.d. https://podcasts.apple.com/us/podcast/episode-2-a-counter-threat-finance-approach-to-competition/id1553806860?i=1000557143750.

Busch, Kristen. “Blockchain: Novel Provenance Applications.” Washington, D.C: Congressional Research Service, April 12, 2022. https://crsreports.congress.gov/product/pdf/R/R47064.

Chainalysis Team, Chainalysis. “2022 Global Cryptocurrency Adoption Index.” Chainalysis, September 14, 2022. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/.

Cohen, Eliot A. *Commandos and Politicians: Elite Military Units in Modern Democracies*. Harvard Studies in International Affairs, no. 40. Cambridge, Mass.: Center for International Affairs, Harvard University, 1978.

Coinbase. “Crypto Basics - What Is Mining?” Coinbase Learn, 2022. https://www.coinbase.com/learn/crypto-basics/what-is-mining.

Coinbase Institute. “Coinbase Institute.” Accessed October 31, 2022. https://www.coinbase.com/institute.

Constellation Network website. “Constellation Network: Trusted in Federal Cybersecurity.” Accessed October 31, 2022. https://constellationnetwork.io/.

Gemini. “Cryptocurrencies vs. Tokens: Digital Assets.” Accessed October 26, 2022. https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference.

CSEngineering. “CSEngineering – Engineering Freedom through Digital Transformation.” Accessed October 31, 2022. https://cse-corp.com/.

Davis, Zachary S, Frank Gac, Christopher Rager, and Jennifer Snow. *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. Livermore, CA: Center for Global Security Research, 2021.

Denning, Peter J., and Ted G. Lewis. “Bitcoins Maybe; Blockchains Likely.” *Sigma XI-The Scientific Research Society*, December 2017.

Department of Commerce. “Responsible Advancement of U.S. Competitiveness in Digital Assets.” Digital Asset Competitiveness Report. Washington, D.C: U.S. Department of Commerce, September 2022. https://www.commerce.gov/files/digital-asset-competitiveness-report.

Department of Defense. *DOD Counter Threat Finance (CTF) Policy*. DOD Directive 5205.14. Washington, D.C: Department of Defense, 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520514p.

Dillet, Romain. “How Ukraine Is Spending Crypto Donations.” *TechCrunch* (blog), March 2, 2022. https://techcrunch.com/2022/03/02/how-ukraine-is-spending-crypto-donations/.

Dostov, Victor, and Pavel Shust. “Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?” *Journal of Financial Crime* 21, no. 3 (January 1, 2014): 249–63. https://doi.org/10.1108/JFC-06-2013-0043.

Dudley, Sara, Travis Pond, Ryan Roseberry, and Shawn Carden. “Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency.” *Joint Force Quarterly*, no. 92 (2019): 58–64.

Duffie, Darrell. “Can China Conquer Crypto?” *Foreign Affairs*, September 2, 2022. https://www.foreignaffairs.com/articles/china/2022-04-22/can-china-conquer-crypto.

Duffie, Darrell, and Elizabeth Economy. “Digital Currencies: The U.S., China, And The World At A Crossroads.” Working Group. Hoover Institute, 2022. https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads.

Duggan, Patrick M., and Elizabeth Oren. “U.S. Special Operations Forces in Cyberspace.” *The Cyber Defense Review* 1, no. 2 (2016): 73–80. http://www.jstor.org.libproxy.nps.edu:2048/stable/26267360.

Exec. Order No. 14067. Executive Order on Ensuring Responsible Development of Digital Assets (2022). https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

Fiala, Otto C. *Resistance Operating Concept (ROC)*. MacDill Air Force Base, Florida: The Joint Special Operations University Press, 2020.

“Framework for Anonymized Covert Communications: Ethereum Blockchain-Based Concept - Video Portal - Naval Postgraduate School.” Accessed October 31, 2022. https://nps.edu/web/nps-video-portal/-/framework-for-anonymized-covert-communications-ethereum-blockchain-based-concept.

Frebowitz, Ryan L. “Cryptocurrency and State Sovereignty.” Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/59663.

Gemini. “Crypto Glossary - Cryptopedia.” Gemini Cryptopedia, 2022. https://www.gemini.com/learn/glossary.

Harsono, Hugh. “Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain.” *The Cyber Defense Review* 5, no. 3 (2020): 153–60. https://www-jstor-org.libproxy.nps.edu/stable/26954878.

Hayward, Decrypt / Andrew. “Samsung, Qualcomm Back FreedomFi, Helium’s 5G Crypto Network Partner.” Decrypt, March 15, 2022. https://decrypt.co/95153/samsung-qualcomm-back-freedomfi-heliums-5g-crypto-network-partner.

Heimans, Jeremy, and Henry Timms. "Understanding 'New Power.'" *Harvard Business Review*, December 1, 2014. https://hbr.org/2014/12/understanding-new-power.

House, The White. "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets." The White House, September 16, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

Impervious. "Impervious Project." Your Portal to the P2P Internet. Accessed October 31, 2022. https://www.impervious.ai/.

International Trade Administration. "El Salvador Adopts Bitcoin as Legal Tender." U.S. Department of Commerce. International Trade Adminstration, June 2021. https://www.trade.gov/market-intelligence/el-salvador-adopts-bitcoin-legal-tender.

Jensen, Benjamin M. *Forging the Sword: Doctrinal Change in the U.S. Army*. Stanford, California: Stanford Security Studies, an imprint of Stanford University Press, 2016.

Johnson, Jason D. "Bitcoin: A Technology-Influenced Social Movement." Master's thesis, Naval Postgraduate School, 2019. https://calhoun.nps.edu/handle/10945/63988.

Joint Knowledge Online. "New USSOCOM J35 Counter Threat Finance (CTF) Curriculum." Joint Chiefs of Staff, August 4, 2022. https://www.jcs.mil/JKO/Latest-News/JKO-Customer-Spotlights/Article/3115355/new-ussocom-j35-counter-threat-finance-ctf-curriculum/.

Jones, Laura, and Shawna Sinnott. "Money Talks: How Nonstate Armed Groups Finance Their Operations and Organizations." Modern War Institute, July 15, 2022. https://mwi.usma.edu/money-talks-how-nonstate-armed-groups-finance-their-operations-and-organizations/.

Kanth, Vikram K. "Blockchain for Use in Collaborative Intrusion Detection Systems." Master's thesis, Naval Postgraduate School, 2019.

Kimani, M. "China Leads Africa's Digital Currency Race." Yahoo. Michael, February 2021. https://finance.yahoo.com/news/china-leads-africa-digital-currency-202250648.html.

Kumar, Ananya, and Nikhil Raghuveera. "Can Crypto Deliver Aid amid War? Ukraine Holds the Answer." *Atlantic Council* (blog), April 4, 2022. https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-answer/.

Lamport, Leslie. "Distribution," May 1987. https://www.microsoft.com/en-us/research/publication/distribution/.

Chainalysis Academy. "Learn Cryptocurrency." Accessed October 31, 2022. https://academy.chainalysis.com/page/learn-cryptocurrency.

Liebermann, Oren. "How Ukraine Is Using Resistance Warfare Developed by the U.S. to Fight Back against Russia | CNN Politics." CNN, August 27, 2022. https://www.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html.

Limba, Tadas, Andrius Stankevičius, and Antanas Andrulevičius. "Towards Sustainable Cryptocurrency: Risk Mitigations from a Perspective of National Security." *Journal of Security and Sustainability Issues*, December 19, 2019. https://repository.mruni.eu/handle/007/16063.

Long, Gideon. "Digital Scheme Pays Venezuela Health Workers from Frozen Funds." Financial Times, December 10, 2021. https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18.

McBride, Megan, and Zack Gold. "Cryptocurrency: A Primer for Policy-Makers." Arlington, VA: Center for Naval Analyses: Analysis and Solutions. Accessed October 26, 2022. https://www.cna.org/reports/2019/08/cryptocurrency-primer-for-policymakers.

———. "Cryptocurrency: Implications for Special Operations Forces." Arlington, VA: Center for Naval Analyses: Analysis and Solutions, August 2019. https://www.cna.org/reports/2019/08/cryptocurrency-implications.

Merwe, Andria van der. "A Taxonomy of Cryptocurrencies and Other Digital Assets." *Review Business: St. Johns University*, no. 41 (2021): 30–43. https://www.stjohns.edu/sites/default/files/uploads/Review-of-Business-41%281%29-Jan-2021.pdf.

Montgomery, Mark. "Equipping U.S. Partners in Cyberspace Is a Must." The Cipher Brief, July 2022. https://www.thecipherbrief.com/column_article/equipping-u-s-partners-in-cyberspace-is-a-must.

Morell, Michael, Josh Kirshner, and Thomas Schoenberger. "Report: An Analysis of Bitcoin's Use in Illicit Finance." The Cipher Brief, April 13, 2021. https://www.thecipherbrief.com/report-an-analysis-of-bitcoins-use-in-illicit-finance.

Myers, Adam, William Szymanski, Daniel Jackson, Ellen Wynkoop, Pete Heine, Tyler Hoffman, and Bri Mostoller. “Crypto-Controls: Harnessing Cryptocurrency to Strengthen Sanctions.” War on the Rocks, December 9, 2020. https://warontherocks.com/2020/12/crypto-controls-harnessing-cryptocurrency-to-strengthen-sanctions/.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin.Org*, October 2008. https://bitcoin.org/en/bitcoin-paper.

Nelson, Danny, and Anna Baydakova. “Ukraine Leads Global Crypto Adoption, Chainalysis Says in New Report,” September 8, 2020. https://www.coindesk.com/markets/2020/09/08/ukraine-leads-global-crypto-adoption-chainalysis-says-in-new-report/.

Nelson, Jason. “Taiwan Turns to Ethereum IPFS Tech to Thwart Chinese Cyberattacks.” Decrypt, August 11, 2022. https://decrypt.co/107293/taiwan-turns-to-ipfs-tech-to-thwart-cyberattacks-from-china.

Newman, Lily Hay. “Mysterious ‘MuslimCrypt’ App Helps Jihadists Send Covert Messages.” *Wired*. Accessed October 27, 2022. https://www.wired.com/story/muslimcrypt-steganography/.

Newmyer, Tory. “Pentagon Launches Effort to Assess Crypto’s Threat to National Security.” *Washington Post*, September 23, 2022. https://www.washingtonpost.com/business/2022/09/23/darpa-crypto-national-security/.

Pero, Michael C. “Understanding Bitcoin and It’s Utility for Special Operations Forces.” Naval Postgraduate School, 2022. https://calhoun.nps.edu/handle/10945/69701.

Protocol Labs. “About Protocol Labs.” Protocol Labs. Accessed November 20, 2022. https://protocol.ai/about/.

Renaudin, Hugo. “Remittance and Payments: Crypto’s Big Opportunity in Latin America.” Accessed October 27, 2022. https://www.nasdaq.com/articles/remittance-and-payments%3A-cryptos-big-opportunity-in-latin-america-2020-08-06.

Reuters. “Russia Plans to Use Digital Rouble in Settlements with China, Says Lawmaker.” *Reuters*, September 26, 2022, sec. Currencies. https://www.reuters.com/markets/currencies/russia-plans-use-digital-rouble-settlements-with-china-says-lawmaker-2022-09-26/.

Rivers, Martin Leo. “Got Bitcoin, Will Buy Intel: U.S. Government Offers Cryptocurrency Bounty In Radical New Approach To Fighting Cybercrime.” Forbes. Accessed October 27, 2022. https://www.forbes.com/sites/martinrivers/2021/07/18/got-bitcoin-will-buy-intel-us-government-offers-cryptocurrency-bounty-in-radical-new-approach-to-fighting-cybercrime/.

Roberts, Daniel. “How Crypto Adoption by Companies like Visa, PayPal, and Tesla Is Creating a Network Effect.” Yahoo, February 2021. https://finance.yahoo.com/news/how-crypto-adoption-by-companies-like-visa-pay-pal-and-tesla-is-creating-a-network-effect-214639389.html.

Rogers, Everett M. *Diffusion of Innovations*. 4th ed. New York: Free Press, 1995.

Rosen, Stephen Peter. *Winning the next War: Innovation and the Modern Military*. Cornell Studies in Security Affairs. Ithaca, NY London: Cornell University Press, 1994.

Rowen, Michael. “Cryptocurrency Utility for Special Operations - Video Portal - Naval Postgraduate School,” September 13, 2022. https://nps.edu/web/nps-video-portal/-/cryptocurrency-utility-for-special-operations.

Smith, Brian A. “Applying Financial Capabilities to Achieve Multi-Domain Effects: Using Financial Capabilities Operationally Rather Than Transactionally.” *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022): 54. https://asmconline.org/armed-forces-comptroller/.

Team, Chainalysis. “Transparency in Blockchains Senate Hearing.” Chainalysis, March 22, 2022. https://blog.chainalysis.com/reports/senate-hearing-underscores-value-of-blockchain-transparency/.

Thomas. *Statement of General Raymond A. Thomas, U.S. Army Commander United States Special Operations Command Before the Senate Armed Services Committee*, 115th Cong. (2017) (statement of Raymond A. Thomas, USSOCOM Commander), May 4, 2017.

TxTenna. “TxTenna: Route Around Censorship,” November 28, 2022. http://txtenna.com/.

United 24. “Aid For Ukraine – Donate Crypto to Ukraine.” United 24: The initiative of the President of Ukraine. Accessed October 27, 2022. https://u24.gov.ua/.

University of Southern California. “Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court.” USC Shoah Foundation, June 10, 2022. https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes.

USSOCOM. “SOF Vision and Strategy.” Tampa, FL: U.S. Special Operations Command, April 11, 2022. https://www.socom.mil/sof-vision-and-strategy.

Vranken, Harald. “Sustainability of Bitcoin and Blockchains.” *Current Opinion in Environmental Sustainability*, Sustainability governance, 28 (October 1, 2017): 1–9. https://doi.org/10.1016/j.cosust.2017.04.011.

Williams, Daniel. “GoTenna with Blockstream Satellite.” Blockstream, May 11, 2019. https://blog.blockstream.com/en-gotenna-satellite-api-integration/.

Winkie, Davis. “New MOS and Formations Could Come to Army Spec Ops in Tech-Savvy Era.” Army Times, July 2022. https://www.armytimes.com/news/your-army/2022/07/28/new-mos-and-formations-could-come-to-army-spec-ops-in-tech-savvy-era/.

Zitser, Joshua. “Impoverished Afghan Women Are Receiving Emergency Aid in Crypto as the Taliban Limits Cash Withdrawals and Millions Go Hungry.” Business Insider. Accessed October 27, 2022. https://www.businessinsider.com/afghanistan-women-turn-to-cryptocurrency-to-feed-their-families-2022-1.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

MIT Connection Science & Engineering

MIT Connection Science

MIT Connection Science & Engineering
[redacted]

2 March 2023

Office of Science and Technology Policy
RFI: Digital Assets Research and Development
[redacted]

Response to OSTP Request for Information (RFI) on Digital Assets Research & Development

To whom it may concern,

With this submission, we would like first to thank the Office for Science and Technology Policy (OSTP), FTAC and NIRD for undertaking the collection of inputs under the current RFI.

We strongly believe that the emerging area of digital assets is crucial for not only the US Economy, but for the global economy. New forms of IT infrastructures will be needed in order for the benefits of a digital assets ecosystem to be realized and appreciated.

However, before many of the useful features of digital asset can be adopted by mainstream financial organizations as part of their IT infrastructure, the functions and processes related to digital assets and decentralized asset networks must be formalized, evaluated from a cybersecurity perspective and then standardized.

The following are some of the current challenges in digital assets and decentralized asset networks, with their Topic Number:

- *Interoperability protocol for decentralized asset networks* (Topic #1): We believe that in the future there will be a proliferation of asset networks that are either private (closed) or publicly accessible (or hybrids thereof). This reflects the nature of business relationship and the need for business communities to develop their respective asset networks. Currently, most blockchain-based asset networks seek to raise artificial “walled gardens” at the expense of the end-user as the asset holder. Users (i.e., the average non-technical investor) desire the flexibility to transfer their digital assets (in the form of liquid value or NFTs) across networks with ease.

  There is strong role for the government – and in this case the OSTP and NIRD – to encourage, promote and fund efforts to develop standardized interoperability protocols for decentralized asset networks. The example of DARPA in the late 1980s – and its support for ARPAnet and then the Internet – comes to mind as an succesful example of how policy and technological implementations in standard organizations such as the IETF (Internet Engineering Task Force) created tremendous benefit of the nation’s digital economy.

- *Digital-asset profiles, Authorities to define profiles, and Issuers of digital-assets* (Topic #3): Digital assets today are represented on blockchain through various tokens (fungible and non-fungible), and no coherent definition of a legally acceptable digital asset form has been adopted by the FinTech industry. This lack of definition introduces possible risks to the ordinary buyer who may be unaware of the legal status of pure-digital assets (digital only asset) and hybrid-assets (e.g. token representation of an off-chain physical asset). Federal R&D could direct to exploring the permissible composition of digital assets (i.e., its asset Profile), and the establishment of business registration mechanisms for entities seeking to publish asset profiles (i.e. the prospectus of a new digital asset), and the registration mechanisms for entities who seek to be Issuers of instances of the digital assets (e.g. tokens on the blockchain) following one or more of the acceptable asset-profiles. Standardization might ultimately lead to a legal definition of a set of "Asset Key Information Documents" like Key Information Documents (KIDs) for packaged retail investment and insurance products in the European Union[1]. Furthermore, strengthening of investor protection via some sort of investor risk profile as defined, for example, in MIFID[2].

- *The formal definition of blockchain virtual machine languages* (Topic #3): Risks from using smart contracts on blockchain-based networks can be reduced by focusing R&D on formal definitions of blockchain virtual machine languages. Smart contract execution platforms are usually sets of computing nodes that consistently interpret smart contract code as a virtual machine (e.g., the Ethereum Virtual Machine). Smart contract developers are coding in a language (e.g., solidity) directly interpreted by the virtual machine. R&D should focus on formal definition of blockchain virtual machine languages where all aspects of the language are unambiguously defined. Moreover, R&D in blockchain should focus on architectures that enable traditional programmers with skills in traditional programming languages to code and deploy smart contracts on blockchains.

- *Paths for integration of existing asset infrastructures* (Topic #4): Blockchain application architectures should allow for non-blockchain applications to seamlessly interact with smart contracts. This implies not only the need for new forms of API integrations between non-blockchain and blockchain systems, but also for upgrading blockchain infrastructure to massively scalable throughput as well as asset interoperability between non-blockchain and blockchain systems.

- *Improving the software quality of smart contracts* (Topic #5): The smart contract programming life cycle is still in its infancy. Today smart contracts are often directly deployed in blockchain live networks (i.e. mainet) with little or no software testing. This poor practice in software quality assurance lags behind standard engineering practices in terms of requirement specifications and/or quality assurance processes. In that context, R&D activities should include high-level blockchain-agnostic specification languages for specifying digital asset semantics, supporting

[1] https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_14_299

[2] https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-387_en.pdf

tools for defining white/black box test suites as well as tools to analyze code coverage for test suites.

- *Accountable Privacy-Preserving Digital Identities* (Topic #4): Other areas of concern include the formalization of accountable digital identities utilized on decentralized asset networks. International organizations that seek to address Anti-Money Laundering (AML) and Combating Terrorism Financing (CFT), such as the FATF, have defined high-level policies pertaining to the Originator and Beneficiaries of asset transfers. However, there is a tremendous gap currently between policy and implementation. Many *Virtual Asset Service Providers* (VASP) handling customers' digital assets find it difficult to maintain customer data privacy while adhering to FATF and BSA regulations. Thus, we believe that accountable privacy-preserving digital identities remain a frontier of R&D that must be prioritized.

We thank the OSTP, FTAC and NIRD for the opportunity to share our thoughts regarding the current state of digital assets and decentralized asset-networks, and possible future directions for policy development and R&D.

We are happy to engage further should you seek more detailed information regarding any of the above bullets/areas of concern.

Yours sincerely,

Dr Thomas Hardjono
Technical Director
MIT Connection Science & Engineering
Founder of IETF Secure Asset Transfer Woking Group
[redacted]

Dr Denis Avrilionis
Founder and CEO
Compellio SA, Luxembourg, EU
Member of EU European Blockchain Services Infrastructure (EBSI)
[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

MIT Digital Currency Initiative (MIT DCI)

ABOUT THE DIGITAL CURRENCY INITIATIVE (DCI)

The mission of the MIT Digital Currency Initiative (MIT DCI) is to create a future where moving value across the internet is as intuitive and efficient as moving information. Founded in 2015, and based at the MIT Media Lab, we are a team of open-source developers, and experts in distributed systems, cryptography, security, and economics, conducting research to advance the security, scalability, and privacy of digital currency systems. The MIT DCI also serves as a neutral convener for governments, nonprofits, open-source developers, and the private sector.

This note responds to the Request for Information on Digital Assets Research and Development that the White House Office of Science and Technology Policy issued for responses by March 3, 2023. We outline below the research priorities that MIT DCI has identified in this field for 2023-2024 and that we have launched, are planning to launch, or are exploring with potential research collaborators. Our intention is to publish research papers, policy notes, and open source code to promote dialogue and encourage practical experiments to help ensure that digital assets will serve the public good.

Central Bank Digital Currency and OpenCBDC

High fees and limited access have prevented traditional electronic transaction systems from evolving fast enough to keep pace with the demand for online digital payments. For these and other reasons, central banks around the world are considering issuing digital forms of their currencies to the public. We believe CBDC's promise goes beyond payment efficiency and financial inclusion, however; we see them as an opportunity for a ground-up redesign of our legacy payment systems.

Our CBDC research collaborations center around OpenCBDC, the first major open-source CBDC codebase. Maintained by the MIT DCI, the first contribution to the project was OpenCBDC-tx, an experimental transaction processor that emerged from joint research with the Federal Reserve Bank of Boston. OpenCBDC-tx can process up to 1.7M transactions per second.

We're actively seeking contributions to OpenCBDC and welcome collaboration proposals from individual engineers and scholars, as well as government, business, and civil society leaders. Through collaborative, multi-disciplinary technical research, we will evaluate CBDC design choices under different assumptions and requirements, evaluate tradeoffs, and ultimately learn how digital currency systems can be designed to best advance privacy, user agency, innovation, and financial equity.

Research priorities:

(1) Core architecture: Investigate and define the requirements of a core CBDC platform

(2) Privacy and compliance: Investigate how to balance, e.g., user privacy from the central bank and the desire of law enforcement to access transaction data. We are launching work in Q1 2023 with a central bank partner into exploring various forms of privacy preserving technology and the use of data vaults, considering regulatory objectives under various scenarios.

(3) Programmability and API: Consider new and existing models for programmability (e.g., spending conditions and smart contracts). We expect to release our report and host a webinar on the research in the spring of 2023.

(4) Usability and functionality: Investigate designs for wallets, merchant interactions, use cases, designs for authorization, as well as various roles for intermediaries.

(5) Offline Transactions: explore solutions to permit users to make payments with CBDC when data connectivity is intermittent or not available, preventing double-spending of currency. We seek research collaborators at present.

(5) Beyond retail payments (wholesale CBDC, cross-border, and interoperability): Extend retail CBDC testing environments to implement and experiment with financial flows across additional industries; explore tools for interoperability between CBDCs and legacy financial infrastructure. Currently in discussions with potential research collaborators to experiment with cross-border transaction platforms to promote interoperability between CBDCs of different jurisdictions. Separately, we are discussing with a potential collaborator the use of CBDCs to increase capacity and efficiency of the securities financing markets while maintaining robust regulatory requirements by enabling the use of CBDC-based smart contracts in repurchase (repo) transactions.

To learn more:

- Visit OpenCBDC for links to papers, current research priorities, and how to get involved.
- Explore our collaborations, including those with the Federal Reserve Bank of Boston, Bank of England, and Bank of Canada.
- Read our technical paper: A High Performance Payment Processing System Designed for Central Bank Digital Currencies**.**

Centering Users in the Design of Digital Currency

What will it take for digital currency technology to realize the promise of a radically improved financial system that protects user privacy and increases user agency? In addition to foundational technology research, we believe it will require a robust awareness of the experiences and needs of everyday people inside and outside the traditional financial system. That's why we're collaborating with user researchers and social scientists to surface user insights that can inform our work as technologists as well as contribute to the public-policy dialogues surrounding digital currencies.

Research priorities:

(1) Global CBDC and financial inclusion study. This multidisciplinary research with Maiden Labs (funded by Financial Services for the Poor at the Bill and Melinda Gates Foundation) seeks to identify the technical and policy design choices most likely to increase financial inclusion and mitigate harm to the poor. Through iterative feedback loops between people and policymakers, this research aims to identify the greatest risks and opportunities for users, and to investigate *whether*, and if so, specifically *how* CBDCs might improve financial inclusion.

To learn more:

- Read our report, "CBDC: Expanding Financial Inclusion or Deepening the Divide?", and watch the webinar associated with our report.

(2) National US user-research to examine some of the riskiest and most-common assumptions about prospective CBDC users and use cases.

To learn more:

- Download our collaborative US study: Centering Users in the Design of Digital Currency.

Security of Digital Assets and Decentralized Networks

The security of the underlying decentralized networks is critical to the safety of the digital assets that are issued upon them. Because decentralized financial networks are relatively new, they need to be systematically hardened, and the infrastructure around them matured, to meet the growing role they play in our economy.

To this end, MIT DCI launched the Bitcoin Security Initiative in 2021 as a four-year research and development program. The initiative is also a home for industry leaders looking to strategically support open-source software.

Research priorities:

(1) Bitcoin Core development: The DCI employs three Bitcoin core developers—we believe providing resources to those who are well-positioned to make a positive contribution to Bitcoin is the best way to ensure the project's longevity. As Bitcoin is the world's largest cryptocurrency, it serves as an environment to understand how to best harden and protect networks built using decentralized technology.

(2) The long-term viability and economic security of decentralized networks (e.g., the stability of fee-based rewards as well as the different security guarantees between Proof of Work (e.g., in Bitcoin) and Proof of Stake (e.g., in Ethereum) consensus algorithms.

To learn more:

- Visit the Bitcoin Security Initiative.
- See release of Bitcoin Core 23.0 which includes new features, various bug fixes and performance improvements, as well as updated translations.

To learn more:

- Download our collaborative US study: Centering Users in the Design of Digital Currency.

Currency Efficiency Research

As a neutral digital currency research lab, the MIT DCI has fielded many questions about the energy consumption of Proof of Work (PoW) cryptocurrencies (e.g., Bitcoin). Given the potential environmental impacts of unjustified energy use, we recognize the importance of this issue;however, we see a disturbing lack of rigor, neutrality, and concrete data pervading the conversation. To that end, our Currency Efficiency research project is an attempt to isolate the root concerns, offer a usable framework, and gather rigorous data in order to help move forward in a productive manner, eventually allowing for a meaningful, rational assessment of Bitcoin's environmental impact.

Research priority:

Move beyond questions of raw energy consumption to instead examine the relationship between inputs (e.g., energy) and outputs (e.g., affordances) to ask how efficient a currency is at performing the tasks it purports to perform. In other words: what are we actually getting (in terms of value secured, features, ease of storage/transport, etc.) in exchange for the energy required to operate and guarantee any given currency?

To learn more:

- Visit us online at: www.dci.mit.edu/currencyefficiency

MIT Digital Currency Initiative
MIT Media Lab
Massachusetts Institute of Technology
Dr. Neha Narula, Ph.D., Director
March 3, 2023

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

MITRE

MITRE's Response to the OSTP RFI Supporting a National Digital Assets R&D Agenda

March 3, 2023

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
[redacted]

[redacted]

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs); participate in and lead public-private partnerships across national security and civilian agency missions; and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's 10,000-plus employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

Over the past several years, MITRE has provided unbiased, trusted advice to multiple federal agencies and U.S. policymakers who seek to better understand rapidly changing technology developments across the full spectrum of digital and crypto-assets from cryptocurrencies, stablecoins, Central Bank Digital Currencies (CBDCs), and non-fungible tokens (NFTs). We have developed partnerships on key digital asset topics with industry, academia, and the nonprofit sector to understand, research, or develop capabilities—for example for the development of high-throughput, reliable, safe, and private payment systems; the interconnectivity of the digital assets system with the traditional financial system to illuminate contagion and system risks; the unmasking and retrieval of sophisticated money laundering activities enabled by illicit use of cryptocurrencies; and examination of how digital assets could impact U.S. economic and national security. Specifically, over the past two years MITRE has held several digital assets technical exchange meetings, bringing together the digital assets industry, government, and nonprofit sector to share insights and deepen a collective understanding of policy goals, challenges, and the current state of technology developments to gain a more holistic view of how the government and industry should tackle the many challenges in the digital assets ecosystem.

Introduction and Overarching Recommendations

MITRE supports the government's efforts in developing a National Digital Assets Research and Development Agenda to drive important research on key digital asset technology topics. We recommend this Agenda focus not only on advancing the state of the art but also on providing data and experiences in maximizing opportunities or mitigating risks that can guide future operational and policy decisions in a data-driven manner.

Strategic Structure. MITRE recommends that the Fast Track Action Committee ensures that the Agenda will strategically drive federal activities and enable the Executive Office of the President (EOP) to assess individual activities and holistic progress toward its unifying vision. It may help to use a strategic planning framework that is consistent with the Government Performance and Results Act.

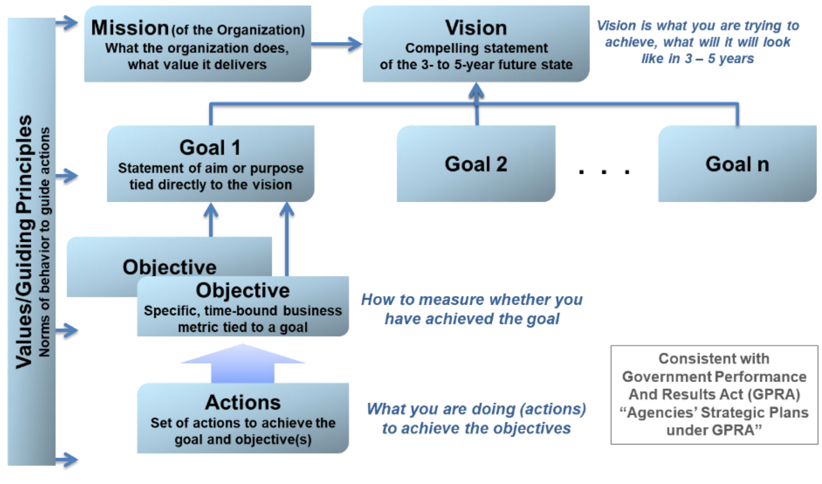


Figure 1. Strategic Planning Framework with Values/Guiding Principles

Such a structured planning framework provides:

- A set of values and principles that guides all subsequent activities
- A universal and compelling vision for the future of digital assets research
- A series of goals that collectively enables the vision to be met
- Subordinate objectives and strategies that are specific and time-bound and that both help drive activities to successfully meet goals and provide the EOP the ability to measure progress

Organizing Taxonomy. The Agenda will also benefit greatly with an organizing taxonomy (or Glossary) that establishes a common government digital assets vernacular and will aid in increasing meaning and control as new technologies are introduced. An organizing taxonomy will also aid in R&D activities such as, but not limited to, 1) building virtual models to simulate the kinds of markets that digital assets might enable and how they may interact with the traditional financial markets, 2) addressing increasing adoption of digital assets that undermine national security and intelligence missions as well as criminal and civil investigations, 3) prototyping simplified interfaces for consumers to access digital assets, and 4) testing approaches to balance privacy and identity across multiple government authorities. While doing so is not a common National Science and Technology Council activity, there are examples where it has been beneficially executed—including in issuing policy for agencies to consistently leverage this terminology in their science and technology (S&T) activities.[1]

[1] D. Blackburn and M. Garris. A National Science and Technology Council for the 21st Century. 2021. MITRE, https://www mitre.org/sites/default/files/2021-09/pr-21-2388-national-science-technology-council.pdf.

Questions Posed in the RFI

1. *Goals, sectors, or applications that could be improved with digital assets and related technologies*: Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered.

Digital assets and related technologies hold significant promise to decrease costs, increase trust and security, and more equitably share value creation. Like the advent of other new technologies, however, there is often a considerable amount of overpromising and underdelivering on what digital asset technology can transform, at least at this stage of its development. Below we discuss several areas where digital assets and related technologies could provide benefits.

Finance, Payments Systems, and U.S. Dollar (USD) Demand. Most digital assets projects to date have aimed to transfer value more quickly, efficiently, and securely compared with the current financial system while simultaneously improving access. Stablecoins utilizing public blockchain infrastructure have enabled inexpensive, secure, nearly instant, and stable cross-border transactions. Prior to stablecoins, there was no mechanism for retail investors to access the USD and preserve their purchasing power. Digital assets may also provide important opportunities for disadvantaged populations around the world by improving the efficiency and cost-effectiveness of international remittances sent by migrant workers back to family members in their home countries. It is estimated there are currently 100+ cryptocurrency remittance companies that aim to provide alternatives to traditional wire transfer services.

Supply Chain. As globalization has fragmented supply chains across the world, it is increasingly difficult to ascertain the provenance of components and subcomponents of the technology we consume. Digital asset technology has the potential to provide a unique new way to unequivocally track the aggregation of intellectual property, manufacturing data, and testing regimes for hardware and software.[2] From software libraries underpinning an enterprise application to bias testing performed on a machine learning model, the U.S. can help ruggedize our supply chains with transparency and illumination. Further, global shipping logistics are increasingly looking toward digital asset technology for solutions, as a large portion of those transactions remain rooted in analog bill of lading mechanisms.

Healthcare. Current approaches struggle to ensure individuals' ownership and control of their own Electronic Medical Records (EMRs) and personal health data, thus risking adverse usage of this sensitive information. A digital asset technology solution for EMR data, however, could dramatically improve patient care through secure, electronically portable, and consistent health records. An early example of such a system is MIT Media Lab's MedRec.[3] Medical research might also be accelerated by compensating users for contributing their data to retrospective trials and population health studies, much as individual participation in prospective, interventional clinical trials is compensated, and hence incentivized, today.

[2] MITRE supported a 2022 National Institute of Standards and Technology/National Cybersecurity Center of Excellence study on "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability." Available on request.

[3] MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis. 2014. Massachusetts Institute of Technology, https://www media mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/. Last accessed February 27, 2023.

Digital Property Rights and the Metaverse. One of the fundamental building blocks of digital asset technology is the concept of digital property rights. NFTs existing on decentralized public infrastructure make the idealized concept of sovereign ownership of unique digital property a reality. As the public increasingly values digital assets alongside physical assets, the metaverse can become an environment in which to uniquely interact with these wholly digital assets.[4]

2. *Goals, sectors, or applications where digital assets introduces risks or harms*: Information about goals, sectors, or applications where digital assets might introduce risks or harms, and examples of where risks or harms are already being manifested.

Cryptocurrency's Role in Facilitating Ransomware Attacks. Cryptocurrency has become the ransomware payment instrument of choice for cyber actors targeting individuals; federal, state, local, tribal, and territorial governments; critical infrastructure operators; small and medium businesses; and the cyber insurance (and re-insurance) markets. The explosion of ransomware attacks in recent years has made victims in virtually every sector of commerce and elements of government at all levels,[5,6] driving reliance on cyber insurance. Individuals and businesses are also harmed through crypto scams in a variety of ways outside of ransomware. These include crypto pump-and-dump schemes, private key compromises, smart contract compromise or misuse, and a host of other illegal or unethical schemes against both sophisticated and unsophisticated cryptocurrency users.

Digital Assets' Introduction of Various Threat Vectors for National Security. Digital assets can diminish the efficacy of U.S. economic policy through introducing mechanisms to transfer value outside of the USD and outside of the U.S. and partner-based financial infrastructure. Cryptocurrencies are a unique problem because they are a complete payment system that avoids infrastructure like the Society for Worldwide Interbank Financial Telecommunications, which the U.S. relies on to implement financial sanctions. North Korea has profited from this in a major way, utilizing cryptocurrency-enabled ransomware to fund their WMD program.[7] Russian oligarchs were also able to use cryptocurrencies to evade financial sanctions after the Ukrainian invasion. Russian cryptocurrency miners were able to continue to mine bitcoin, taking advantage

[4] R. Belk, et al. Money, Possessions, and Ownership in the Metaverse: NFTs, Cryptocurrencies, Web3 and Wild Markets. 2022. Journal of Business Research, https://www.sciencedirect.com/science/article/abs/pii/S0148296322007147. Last accessed February 27, 2023.

[5] Ransomware Threats against Local Agencies Shows No Sign of Slowing in 2022. 2022. StateScoop, https://statescoop.com/ransomware-threats-against-local-agencies-shows-no-sign-of-slowing-in-2022/. Last accessed February 20, 2023. This recently released report paints a bleak picture of the prevalence of ransomware in government, at both the central government and local government levels.

[6] Three Affiliated Tribes Hit by Ransomware Attack, Holding Tribal Information Hostage. 2021. Native News Online, https://nativenewsonline net/currents/three-affiliated-tribes-hit-by-ransomware-attack-holding-tribal-information-hostag. Last accessed February 20, 2023. Tribal governments have been hit by ransomware, disrupting tribes' access to their email and other information systems.

[7] U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats. 2022. U.S. Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0768. Last accessed February 27, 2023.

of the country's combination of cool weather and cheap electricity. Iran has also explored the use of cryptocurrency to facilitate international trade.[8]

3. *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets:*

Addressing Digital Asset Tax Compliance Needs. Public Law No. 117-58 (November 2021) requires brokers (e.g., cryptocurrency exchanges, peer-to-peer money transmitters, financial institutions that provide crypto investing services) to report all digital asset transactions (e.g., cost basis, sales) beginning in January 2024. In simple terms, individual taxpayers engaged in digital asset trading and the businesses that facilitate digital asset trading must file tax returns to report the values of those trades, and the Internal Revenue Service must enforce the reporting requirements for those exchanges. Because digital asset values are considerably more volatile than physical assets, but are significantly easier to trade and occur in higher daily volumes, there is a significantly higher overhead for both voluntary compliance and enforcement. To help mitigate this overhead for taxpayers, research should be conducted to explore techniques that can automate the tracking of digital asset basis—especially for transactions that occur on decentralized exchanges and transactions that involve transfers across multiple exchanges. To support tax enforcement efforts, additional research is required to determine how digital assets can be used to advance abusive tax shelter strategies.

Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT). Whether cryptocurrencies, stablecoins, CBDC, or other digitized forms of value, due diligence standards for identifying and reporting illicit finance, sanction-evasion, and fraud activities must be based on a reasonableness standard to associate the asset with an entity (i.e., person, business, or other form of entity). The current AML/CFT and sanctions regime is based on the principle that the financial intermediary (e.g., bank, MSB, fiduciary) will and should have adequate controls in place to associate the value to the entity for the specified purpose (e.g., AML/CFT, sanctions, fraud). Regardless of whether a financial regulator has jurisdiction over a particular form of digital asset, development of a reasonableness standard framework for association of "the who to the asset" is imperative. The framework should lay out the key variations of responsibilities for diligence monitoring by the community—from those where there is a clear fiduciary intermediary to those where there is not where a reasonable intermediary. For those digital assets that are truly decentralized—where no one entity has insight into due diligence AML/CFT and sanctions monitoring—not-for-profits/nongovernmental organizations could be authorized to perform the due diligence. R&D specifically into the types of entities that could be established and funded to perform fully decentralized AML/CFT and sanctions monitoring is an area for exploration.

Equitable Access. To help underserved communities harness the benefits of digital assets while reducing their risks, barriers to adoption must be understood. These barriers must be considered across several dimensions, including access and financial inclusion, usability, security, privacy, and interoperability. MITRE identified 11 key user-centered issues that need to be further

---

[8] D. Dudley. Iran Dabbles in Crypto for Cross-Border Trade, in Effort to Bypass Sanctions. 2022. Forbes, https://www forbes.com/sites/dominicdudley/2022/08/10/iran-dabbles-in-crypto-for-cross-border-trade-in-effort-to-bypass-sanctions. Last accessed February 27, 2023.

researched to achieve an equitable and usable token-based CBDC wallet (please see detailed discussion in Appendix A).[9] For example, offline capabilities address barriers of particular importance for both usability and access across all populations. By addressing these barriers and incorporating user-centered digital wallet design, all citizens—especially those who have been underserved by the traditional banking system—can leverage digital assets more efficiently, effectively, and safely.

4. *R&D that should be prioritized for digital assets*: Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present.

Maximizing the Benefits of a New Decentralized Payment System while Mitigating Illicit Financial Activities. These new easily accessible peer-to-peer payment systems and distributed applications fueled by a myriad of digital assets can allow for greater distribution of economic wealth. However, they present an economic and technical hurdle to a number of government missions. For instance, an explosion of broadly adopted digital assets and investments through decentralized finance might in some circumstances also erode the standing of the U.S. dollar as the global reserve currency and provide a new mechanism to scale illicit financial activities that can undermine trust in the overall financial ecosystem. To make that less likely, the following questions should be explored:

1. How can adversaries combine cyber and economic techniques, tactics, and procedures to compromise national security and government services? Addressing this issue requires research to develop sensors, ontologies of behavior, and systems/environments for modeling and empirical experimentation. These building blocks can form the basis of varieties of mechanisms for effects across government missions, such as degrading criminals' logistical capabilities, avoiding systemic economic tipping points, and creating secure blockchain resources.
2. What data science techniques can be developed to track illicit actor use of privacy-enhancing coins such as Monero and Zcash?
3. What extensions are required to existing threat-sharing intelligence standards, such as Common Vulnerabilities and Exposures/Common Weakness Enumeration, to capture digital asset-based illicit financial activities and exploits?
4. How can unique government authorities be asserted upon decentralized payments without violating their underlying transaction mechanisms?
5. What cryptography advances can help increase the speed of computational algorithms used in tools for law enforcement interdiction?
6. How can legitimate users be guided away from illicit environments while offering them similar privacy?
7. How can on and off ramps into the digital assets ecosystem be improved to better enforce Know Your Customer (KYC) standards?

[9] B. Scollan and E. Darling. Designing Digital Currency Wallets for Broad Adoption. 2023. Journal of Payments Strategy & Systems, 17(1), forthcoming.

8. How can government play a role in setting standards for the safety of code that defines these socio-technical systems, such as smart contracts in decentralized autonomous organizations?
9. What challenges need to be overcome to better enable cross-agency sharing of digital asset data and intelligence?

Research Strategies to Reduce Systemic Financial Risk from Decentralized Finance. Regulatory agencies such as the Commodity Futures Trading Commission and Securities and Exchange Commission are facing a host of new challenges to address the stability issues associated with digital asset markets.[10] Traditional approaches that involve applying regulatory controls such as asset risk disclosures, liquidity minimums, and trading rules to centralized intermediaries such as stock exchanges don't translate well for digital assets that trade in decentralized market systems. In these complex economic systems, small perturbations can have cascading effects in unpredictable ways and can undermine the stability and integrity of the system as a whole in short order. The following are topics of recommended research to mitigate these risks:

1. Determine interdependencies between decentralized protocols that can lead to financial contagion in digital asset markets.
2. Discover which controls can be applied to detect and mitigate potential contagion.
3. Research which real-time data extract, transform, and load techniques can help quickly identify digital asset liquidity fragmentation across centralized/decentralized protocols and market participants.
4. Promote research efforts to develop modeling and simulation tools that can test the impact of regulatory "what-if" scenarios on the behaviors of market participants.
5. Conduct research to uncover fundamental economic mechanisms in digital asset protocols that can result in a "run on the bank" and corresponding "death spiral" of liquidity.

Advancing Global Decentralized Digital Identity and Digital Data Research to Protect Citizen Privacy and Enable the Evolution of Governance. The need to protect individual privacy and the need for service providers to comply with KYC, Customer Due Diligence, and AML regulations are conflicting goals that require solutions that balance private interests with national security. At the heart of this conflict is the need to prevent abuse or misuse of individual identities and data. Given the advent of decentralized identity technologies, portable and verifiable KYC credentials and zero-knowledge proof (ZKP) research should be prioritized to explore the potential to achieve a good balance. In particular:

1. How can ZKPs be scaled to provide customized citizen services while preserving the privacy of transactions? This should include statements about measuring whether a given transaction or action is allowed without revealing the contents and making statements describing quantities, materials, and identities of involved parties (e.g., this transaction contains no bad actors) without revealing any of this data to others?
2. What are the technical and social barriers to growing and adopting decentralized identity solutions? How can they be overcome?

---

[10] There have been many congressional hearings on this topic over the past year, such as a February 14 Senate Committee hearing on "Crypto Crash: Why Financial System Safeguards Are Needed for Digital Assets."

3. How can the computational overhead of privacy-enhancing technologies (PETs) such as homomorphic encryption, secure multiparty computation, differential privacy, blind signatures, and ring signatures be reduced to enable solutions for larger problem sets?
4. How can PETs allow industry to exchange data in a secure and privacy-enhanced way, as well as to comply with state, national, and international data protection regulations?
5. How can PETs help government agencies monitor privacy risk, meet privacy compliance requirements, and strategically address privacy policy and technology challenges?
6. How can post-quantum cryptography (PQC) be used to perform digital asset transactions?
7. How can identity and transaction delegation via Attribute Based Encryption or Identity Based Encryption be performed using PQC?

The Potential of Digital Assets to Meet the Needs of the Underbanked/Unbanked. The U.S. Treasury Department's Strategic Plan for Fiscal Years 2022–26[11] calls for progress on financial innovation with a deliberate emphasis on financial inclusion. Unfortunately, many of the current use cases for digital assets are centered on investment opportunities and may not align directly with the needs of underbanked or unbanked populations. That said, digital assets may have considerable potential to help disadvantaged populations, not least in providing a possible future way to accelerate, target, and mitigate fraud, waste, and abuse in disbursements of government economic stimulus or crisis response aid. The underlying web3 technologies may also help reduce financial transaction fees—thus also potentially helping the underbanked—and help make possible more viable or safer alternatives to predatory inclusion services such as payday lending and title loans. Research efforts should explore the following:

1. Can peer-to-peer decentralized financial payment systems benefit communities located in domestic banking deserts?
2. If government grants were administered using a decentralized ledger, would this help reduce fraud, waste, and abuse?
3. Can digital asset-based decentralized lending protocols assist communities in U.S. persistent poverty counties to overcome traditional barriers to accessing capital?

CBDC Research Priorities. Research conducted into the progress of other countries' CBDCs—namely China's—has illustrated the United States' lack of progress in this area, relatively speaking, but has also yielded useful insights into which areas to prioritize when conducting research for the creation of a CBDC. Further insights into research priorities when attempting to create a CBDC were gleaned during MITRE's involvement in the OpenCBDC project (Project Hamilton), conducted by MIT's Media Lab in conjunction with the Federal Reserve Bank of Boston:

1. Privacy/Auditability: How can users be given fine-grained privacy over their transactions, while at the same time providing the visibility needed for the financial system and law enforcement? Users want a digital currency with the anonymity of cash.
2. Policy and Architecture: How would a CBDC fit into existing systems? Who would operate it (e.g., federal reserve, local banks, treasury)? What are the implications for other payment providers (e.g., Visa, Mastercard, Paypal)?

---

[11] Treasury Strategic Plan 2022-2026. 2022. U.S. Department of Treasury, https://home.treasury.gov/system/files/266/TreasuryStrategicPlan-FY2022-2026.pdf.

3. Scalability: If the entire U.S. population was using such as system, could it handle the load, even at extremes such as the holiday shopping season?
4. Key Management (for the average person): How can approaches to private key recovery be simplified for the average person? What recovery/insurance system might be introduced for loss or remediation of theft?

Additional research questions specific to a U.S. CBDC are included in Appendix B.

5. *Opportunities to advance responsible innovation in the broader digital assets ecosystem*: Information about opportunities for the United States to advance responsible innovation in the broader digital assets ecosystem, in areas that are adjacent to R&D.

<u>Maintaining and Increasing Participation in U.S. and International Bodies that Influence Standards for Digital Assets</u>. The United States should participate in working groups across the full spectrum of digital assets to learn, leverage, and influence research within the ecosystem. The realization that the U.S. may likely not be in the international driver's seat on this topic further underscores this need. For example, the Federal Reserve Board of Governors and the Federal Reserve Bank of New York are members of the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures, an international standards setter that promotes, monitors, and makes recommendations about the safety and efficiency of payment, clearing, settlement, and related arrangements. This type of participation should provide significant knowledge and technical expertise into the design of a potential U.S. CBDC. Participation in the BIS's Innovation Hub—particularly new projects like Pyxtrial, which aims to develop a platform to monitor stablecoin's balance sheets—should offer important technical understandings for both stablecoin and CBDC projects. As security and reliability will be perhaps the most important elements of a potential U.S. CDBC architecture, the Office of Science and Technology (OSTP) should leverage research currently being undertaken by NIST, including MITRE participation in efforts to utilize blockchain technology to improve the security and traceability of microelectronics and industrial control software. Finally, influence in projects in which the U.S. is not a core member, such as the BIS's mCBDC initiative, will be critical for integrating democratic norms and interoperability with a potential U.S. CBDC.

<u>Convening International Partners to Advance an Inclusive Vision to Strengthen Democratic Values Pertaining to the Use of Digital Assets</u>. The United States should organize and lead a coordinated international effort—involving officials both from likeminded, democratic governments and from private sector entities—to counter Chinese efforts to advance authoritarian digital asset-related standards[12] with a coordinated *non*-authoritarian approach that promotes decentralized values. These efforts should build on the recent directives issued to U.S. agencies to "leverage U.S. positions in international organizations to message U.S. values related

[12] See, for example, J. Zheng and M. Chen. Web3 in China: Will It Happen, and What Form Will It Take?. 2022. Technode, https://technode.com/2022/08/25/web3-in-china-will-it-happen-and-what-form-will-it-take/. Last accessed February 27, 2023.

to digital assets," as detailed in the White House Framework for Responsible Development of Digital Assets.[13]

Advancing Accessibility Standards that Reduce Burden of Technology Adoption. The interfaces currently available to access the digital assets ecosystem require individuals to have a high level of technical sophistication and fail to meet basic Section 508 accessibility standards. This failure is due in part to the lack of adoption of user-centered design principles and a counterproductive focus on providing solutions primarily for a tech-savvy, early-adopter market segment—which limits the potential for rapid and widespread uptake and use case development. Standards bodies should set minimum requirements for accessibility to help mitigate the potential for a widening digital divide.

6. *Other information that should inform the R&D Agenda:*

Given the wide breadth of digital assets research needs that span multiple technological, social, policy, and financial and economic dimensions, an important first step is the development of an organizing framework to map research interdependencies, ambiguities, tradeoffs, and overlaps against a unifying set of use cases to help sequence and prioritize a productive research portfolio. This ensures that a foundational set of knowledge is retained in a coordinated manner, and is particularly essential when multi-disciplinary, multi-stakeholder teams are involved. This framework can serve to inform potential research solicitation and prioritization of investments and provide transparency to leadership teams that are accountable to deliver on Executive Order directives.

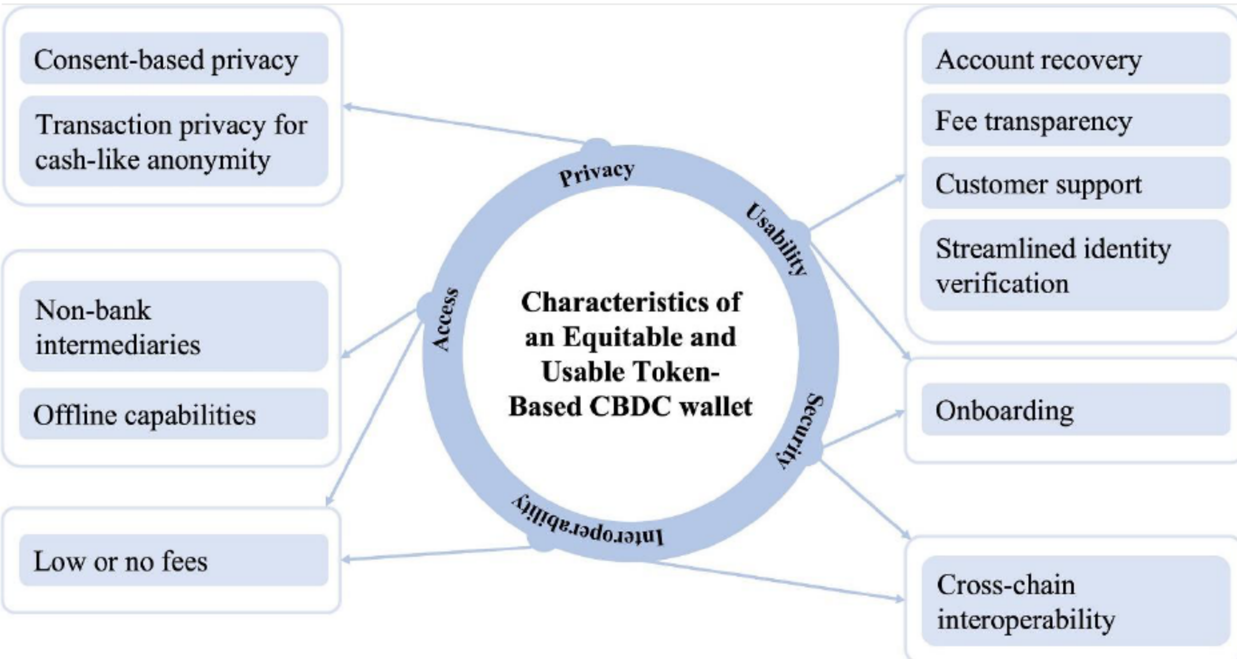
Furthermore, OSTP's charge to drive the national R&D agenda on digital assets will require convening a diverse set of stakeholders from across government, industry, and academia to identify pockets of digital assets expertise and to collaborate, where appropriate, on those technological advancements and innovations. In cases where there are uniquely specialized areas of expertise in industry or where there are overlapping mission objectives with government, it may be beneficial to investigate the potential for creating public-private partnerships to advance research on certain topics and/or to leverage or expand existing investments being made in digital assets research across government. Having a "big picture" view of the research needs and mapping that to the various entities with which the government may seek to collaborate based on their expertise on those needs will be a critical early step to support a national research strategy.

When the research agenda is fully formed and mature for execution, significant additional efforts will be required to manage and sustain the overall portfolio. It will be critical to establish an overall approach for synthesizing and integrating the outcomes from the various research projects to ensure the government is fully leveraging the value from those investments. Additionally, to support the large-scale technical research projects that will be needed, it may also be necessary to design a national strategy for investments in the labs and computing environments that will be critical to support that experimentation.

[13] FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets. 2022. Executive Office of the President, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/. Last accessed March 1, 2023.

Appendix A. Pre-Publication Information from Designing Digital Currency Wallets for Broad Adoption

MITRE identified 11 key user-centric issues to achieve an equitable and usable token-based CBDC wallet.[14]



UX area	Issues	Opportunities	Potential solutions
Low or no fees (access; interoperability)	• Lack of funds is the primary barrier to financial inclusion • High minimum balance requirements for accounts are a barrier to those who lack funds	• Cryptocurrencies can be transferred internationally in real time with little to no fees	Develop a CBDC with little to no fees and consider the cost of access (e.g., mobile devices, internet fees).
Non-bank intermediaries (access)	• Identity-based accounts require an intermediary	• Token-based accounts may not require an intermediary	For a CBDC, promote innovation in a two-tiered payment system by including new, non-bank intermediaries (e.g., intermediaries that offer payment services but do not handle customer funds). If people can access it only through a traditional

[14] B. Scollan, and E. Darling. Designing Digital Currency Wallets for Broad Adoption. 2023. Journal of Payments Strategy & Systems, 17(1), forthcoming.

UX area	Issues	Opportunities	Potential solutions
			bank, it will not be appealing to the unbanked.
Offline capabilities (access)	• Reliable internet access can be a barrier to financial inclusion	• Innovations in offline payments in other countries like India • Innovative methods for feature phone payments and banking in India • SMS-based crypto wallets used with stablecoins in Rwanda, Kenya, and Uganda	A CBDC should offer offline capabilities and access options on multiple device types (including hardware card and paper). Further research on mobile payments innovations in offline, feature phone, and SMS can be used to inform CBDC policy and design.
Customer support (usability)	• Non-custodial wallets have no customer support	• Customer support best practices of some custodial wallets and mobile payment wallets	A CBDC should provide customer support.
Fee transparency (usability)	• There is confusion around gas fees and transaction speed for crypto wallets	• UI design best practices from other domains (e.g., e-commerce user interface techniques that provide the user with transparent payment options based on delivery speed)	Wallets that interact with a CBDC should provide clarity and predictability regarding any fees, limits placed on spending amounts, number of transactions a person can make, etc.
Streamlined identity verification (usability)	• KYC/AML processes are cumbersome	• Simplify KYC/AML processes through user research and regulatory changes	A CBDC should offer tiered access that allows for a simplified KYC process. Further usability research on KYC/AML should be conducted, targeting populations that are unbanked or lack access to government IDs.
Account recovery (usability)	• Users must safeguard the seed phrase for non-custodial crypto wallets	• Help citizens keep their money safe and secure	A CBDC should make clear the importance and best practices of safeguarding one's funds. There should be a safe and secure way for users to recover their accounts if they have a lost password or lost device.

UX area	Issues	Opportunities	Potential solutions
Onboarding (usability; security)	• Potentially increased exposure to phishing that targets wallets • Crypto wallets have a steep learning curve	• Help citizens feel their money is safe and secure	CBDC wallets should provide clear onboarding materials to help novices enter the space. Wallets that interact with a CBDC should adhere to a higher security standard to inspire trust in the security of the issuer, intermediaries, the underlying technology, and the level of fraud protection offered.
Cross-chain interoperability (security; interoperability)	• Most of the money stolen by hackers in 2022 targeted cross-chain bridges, which are used to facilitate the transfer of funds between blockchains	• Achieve interoperability goals while preserving security	A CBDC should increase interoperability while improving security through broad adoption of standard protocols or use of an interlinked approach.
Transaction privacy for cash-like anonymity (privacy)	• Cryptocurrency transactions are not private: the sending address, receiving address, transaction amount, and date and time are all recorded on a public ledger that anyone can view	• Explore ZKPs • Determine the right balance between privacy and oversight	Use privacy by design methods. Learn from pilot implementations that leverage ZKPs (e.g., MIT Digital Currency Initiative's zkLedger).
Consent-based privacy (privacy)	• Users have concerns about data privacy (from peers and from the government) for financial transactions being exposed to third parties through a national digital ID	• Decentralised Identifiers (DIDs) enable a verifiable, decentralised digital identity that allows a user to create an identification token that contains their personal information and prove their identity without needing a central authority such as a bank or credit card company to create and manage the identity	Conduct further research into the use of DIDs to increase CBDC privacy. Consider data sharing with appropriate safeguards such as separating transaction and personal data. A token-based CBDC wallet must clearly communicate what information the government can see and why it needs to see it. Allow users to maintain a sense of authority and control of their personal data.

Appendix B. CBDC-Specific Research Questions

Additional CBDC-specific research questions aligned to the format published in the OSTP September 2022 report, "Technical Evaluation for a US Central Bank Digital Currency System."

Design Element	Focus Areas	Research Questions	Design Choices
Participants	Transport Layer	What approaches can be used to handle proxy authorizations? What implications exist for wholesale vs. retail implementations?	Less Intermediated vs. More Intermediated
	Interoperability	What data and data interchange standards are required for interoperability with third-party systems? What standards can help advance the accessibility challenges of different types of wallets for different user demographics?	Less vs. More Technical Interoperability with Other Payment Systems Human Coordination vs. Technical Interoperability
Governance	Permissioning	Is the system permissioned (and if so, how) or permissionless? What tradeoffs must be addressed if there is a permissionless substrate with a permissioned app layer?	Permissioned vs. Permissionless vs. Hybrid
	Identity Privacy	Which aspects of identity are kept private/confidential, from whom, under what circumstances, and how? How important is privacy to U.S. consumers, and does the perception of a lack of privacy threaten adoption of a CBDC?	Known to Central Bank vs. Intermediary vs. No One
	Remediation	Is there an end user layer that delays transaction finalization and a settlement layer that is immutable vs. a monolithic single layer?	On-Ledger vs. Off-Ledger Multi-Layer vs. Monolithic
Security	Cryptography	How can proofs-of-compliance be engineered that allow for law enforcement insights for legitimate transactions while masking transaction-level data?	Public-Key Cryptography (PKC) vs. PKC with Zero-Knowledge Proofs vs. Other
	Secure Interfaces	What security standards are required to mitigate cyberattacks at CBDC access points? Which key management options and wallet designs would work best for different types of users? How can new tactics, techniques, and procedure threats be mitigated?	Opensource vs. Proprietary Standards

Design Element	Focus Areas	Research Questions	Design Choices
Transactions	Transaction Privacy	How do privacy protections impact other requirements, such as processing speed, system/network security, scalability, and/or maintenance costs?	More Private vs. More Observable Transactions vs. Layering
	Transaction Programmability	Should atomic transaction bundling be supported?	Supported vs. Not Supported Atomic vs. Not Atomic
Data	Ledger History	Can decentralized data stores be used to provide transaction data security and privacy for end users?	None vs. Centralized vs. Distributed
Adjustments	Fungibility	Can the CBDC system support non-fungible units? What use case is envisioned, and how is it balanced with privacy—i.e., if all units have non-fungible properties, then are all units potentially traceable?	Fungible vs. Non-Fungible Units
System Stability	Core Stability	Which architectural features help reduce the failover time of the core processing application?	Speed vs. Robustness
	Market Stability	Could a U.S. CBDC create new vectors for economic contagion? Which leading indicators could provide an early warning of systemic risk? What "circuit breakers" could help contain external and internal economic shocks?	Private Risk Management vs. Federal Backstops
	Sociotechnical Stability	How does a CBDC solution compare competitively with alternative payment systems for trust and security? What are the implications for a CBDC-issued centrally vs. a digital dollar issued by multiple vendors? How can computational analysis be applied to systems composed of and secured by self-directed agents? What sociotechnical factors drive instability?	Centralized Stability vs. Tokenomic Stability Systems of Agents vs. Systems of Bits

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

MobileCoin Foundation

MobileCoin Foundation **www.mobilecoin.org**

The MobileCoin Foundation coordinates and encourages a global community of developers working together to co-create the simplest possible encrypted and payments network. GR Contact: Dana Hudson [redacted]

Clear and Present Danger: The financial underpinnings of the United States are at significant risk of being undermined by the People's Republic of China. China is actively working towards new global standards for digital financial assets - to include China's own cryptocurrency stablecoin, Central Bank Digital Currency (CBDC), and the China-based alternative to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) which would include Russia, Iran, and others.

- China's version of a CDBC already has developed code to delete and replace SWIFT codes for banks and financial institutions worldwide.
- If China undermines SWIFT and advances its own cryptocurrency stablecoin - while the U.S. lacks any clear digital financial assets policy - then China, Russia, Iran, and North Korea will supercharge their arsenal of capabilities to navigate around trade restrictions and sanctions.
- China-backed Binance, the world's leading cryptocurrency exchange platform, has helped Iran trade $7.8 billion despite U.S. sanctions intended to cut Iran off from the global financial system.

Without clear U.S. policy around digital financial assets, the dollar risks being dethroned. This is a grave national security issue - not only benefitting China, Russia, Iran, and North Korea, but also damaging lawfully sanctioned U.S. efforts operating with low-visibility signatures at home and abroad.

Action Is Needed Now: Policy clarity around digital financial assets is needed, requiring any digital financial assets in the U.S. to **achieve privacy, security, compliance** comparable to existing U.S. bank protocols associated with dollar cash transactions. Whereas China is advancing its own cryptocurrency stablecoin and CBDC with no privacy for its citizens - thus further strengthening its authoritarian control - U.S. digital financial assets **must provide privacy, security, and compliance simultaneously**.

- Commerce on the Internet has come to rely almost exclusively on centralized financial institutions serving as trusted third parties to process digital financial payments.
- The lack of U.S. regulatory clarity, as it relates to digital financial payments, enables China to undermine the U.S. dollar - and simultaneously prevents the emerging U.S. digital financial assets industry from working with banks who are already highly regulated.
- Congress can fix this - and stop China's undermining of the U.S. and global financial system
    - **Privacy of transactions**
    - **Security of wallets and encrypted storage of digital financial assets**
    - **Trusted and compliant protocols that follows the rule of law**

MobileCoin Foundation **www.mobilecoin.org**

The MobileCoin Foundation coordinates and encourages a global community of developers working together to co-create the simplest possible encrypted and payments network. GR Contact: Dana Hudson - [redacted]

Language to consider::

Whereas foreign actors are advancing their own cryptocurrency stablecoin and their own Central Bank Digital Currency with no privacy - thus further strengthening authoritarian control - U.S. digital financial assets must provide privacy, security, and compliance simultaneously. As such, the U.S. government is required, and U.S. banking institutions are encouraged, to utilize innovative, beneficial uses of digital financial assets, to include those used for electronic payments, to advance U.S. values and strengthen the dollar insofar that this use of digital financial assets simultaneously demonstrates (1) privacy of transactions, (2) security of wallets and encrypted storage of digital financial assets, as well as (3) compliance to existing U.S. bank protocols and the rule of law associated with dollar cash transactions.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

North American Securities Administrators Association, Inc. (“NASAA”)

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
[redacted]
www.nasaa.org

NASAA

March 3, 2023

By email to: DARD-FTAC-RFI@nitrd.gov

Ms. Rachel A. Wallace
Deputy General Counsel
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

RE: Request for Information; Digital Assets Research and Development

Dear Ms. Wallace:

On behalf of the North American Securities Administrators Association, Inc. ("NASAA"),[1] I am writing in response to the *Request for Information; Digital Assets Research and Development* (the "RFI") posted in the Federal Register by the Office of Science and Technology Policy ("OSTP"). We appreciate the opportunity to provide public comment regarding digital asset research and development priorities.[2] NASAA is committed to protecting investors from fraud and abuse, a commitment that can be supported by research devoted to technology tools and protocols that make digital assets and the businesses that handle them more secure and compliant with the law.

This letter focuses on the RFI's solicitation of comments involving "goals, sectors, or applications where digital assets might introduce risks or harms."[3] Our concerns rest on vulnerabilities and risks in the digital asset ecosystem that have not been fully appreciated by government research and attention. We recommend that the OSTP devote efforts into areas where owners and traders of digital assets are victimized, and accordingly develop tools for customers, regulators and law enforcement agencies to combat these abuses.

[1] Organized in 1919, NASAA is the oldest international organization devoted to investor protection. NASAA's membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico, and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

[2] The RFI is available at https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development.

[3] RFI at 5045.

I. Improving Market Manipulation Detection and Monitoring

There is still insufficient data and insight into various components of the digital asset ecosystem, which prevents regulators and law enforcement agencies from being able to perform effective analyses of potential threats to customers. A more detailed examination into the full life cycles of various forms of digital assets and digital asset-based business models, the activities of the various actors along those life cycles, and particularly how those actors monetize various aspects of digital asset enterprises would be worthwhile to help regulators and law enforcement agencies detect fraud and other regulatory violations. Studies show that fraud and abuse exist within the digital assets markets, and state and federal securities regulators are actively bringing cases to combat digital asset-based frauds and regulatory violations.[4] Further research would provide greater clarity as to where the potential for misconduct exists. NASAA welcomes research and development efforts that would help regulators and law enforcement agencies improve detection and monitoring practices.

For example, academic research investigating occurrences of pump and dump schemes and coin washing on cryptocurrency exchanges demonstrates that significant misconduct occurs in digital asset trading. Studies involving pump and dump schemes show that self-organized groups arrange frauds on digital platforms such as Telegram, Reddit and Discord.[5] According to these studies, the operators announce a target token to members of a group and communicate buy signals once the highest-ranking members have purchased the token at relatively low prices.[6] A rise in

---

[4] *See*, *e.g.*, Press Release, NASAA, *NASAA and SEC Announce $45 Million Settlement with NEXO Capital Over Interest Bearing Accounts* (Jan. 19, 2023), https://www.nasaa.org/67039/nasaa-and-sec-announce-45-million-settlement-with-nexo-capital-over-interest-bearing-account/?qoid=newsroom; Press Release, Alabama Securities Commission, *Sand Vegas Casino Club Located in the Metaverse is Soliciting Investors to Invest Real Money in Un-Registered Investments* (Apr. 13, 2022), https://www.asc.alabama.gov/News/2022%20News/4-13-2022_Sand_Vegas.pdf; and Press Release, NASAA, *NASAA and SEC Announce $100 Million Settlement with BlockFi Lending, LLC* (Feb. 14, 2022), https://www.nasaa.org/62000/nasaa-and-sec-announce-100-million-settlement-with-blockfi-lending-llc/?qoid=newsroom. NASAA emphasizes that the role of state securities regulators has been critical to customer protection, and therefore any effort to preempt the reach of state securities regulators over digital asset enterprises would directly imperil efforts to protect customers from theft, fraud and regulatory violations. To the extent that the OSTP's work extends to policy considerations, NASAA encourages OSTP to review our *Core Principles for Evaluating Federal Legislation Relating to Digital Assets*. *See* Letter from Melanie Lubin, NASAA President, to Senator Sherrod Brown and Representative Patrick Toomey (Jan. 28, 2022), https://www.nasaa.org/wp-content/uploads/2022/01/NASAA-Letter-to-SBC-HFSC-Leadership-re-NASAA-Core-Principles-for-Evaluating-Federal-Legislation-Relating-to-Digital-Assets.pdf.

[5] *See*, *e.g.*, Massimo La Morgia et al., *The Doge of Wall Street: Analysis and Detection of Pump and Dump Cryptocurrency Manipulation* at 2-5 (May 3, 2021), https://arxiv.org/pdf/2105.00733.pdf; Friedhelm Victor et al., *Cryptocurrency Pump and Dump Schemes: Quantification and Detection* at 2 (Nov. 22, 2019), https://www.researchgate.net/publication/337442475_Cryptocurrency_Pump_and_Dump_Schemes_Quantification_and_Detection; and Tao Li et al., *Cryptocurrency Pump-and-Dump Schemes* at 1-2 (Jan. 2019), https://www.researchgate.net/publication/329132134_Cryptocurrency_Pump-and-Dump_Schemes.

[6] Felix Eigelshoven et al., *Cryptocurrency Market Manipulation – A Systemic Literature Review* at 9 (2021), *available at* https://www.researchgate.net/publication/354995772_Cryptocurrency_Market_Manipulation_A_Systematic_Literature_Review.

the price spurs non-members to invest in the token and, when the price reaches a peak, members sell their tokens for a profit while non-members are left with a much less valuable asset.[7] Coin washing is another digital asset scheme where traders simultaneously buy and sell the same asset to create artificial market activity to distort the price and entice unknowing investors to trade.[8] These examples demonstrate some of the varied ways that digital assets can be subjected to manipulation when left without proper oversight.

The pseudonymous nature of digital assets renders the ecosystem vulnerable to fraudulent misconduct. These same features also make market manipulation difficult to detect and address when it occurs. For regulators and law enforcement agencies to better prevent the types of schemes discussed above, greater analysis that leads to the development of better detection and monitoring tools is needed. Specifically, research and development materials should include analyses that help improve the ability to detect and monitor incipient abnormal trading activities.

II. Securing Digital Assets Held by Intermediaries from Theft

NASAA would also encourage research into how customer digital assets are stolen when they are in the custody of intermediaries, such as exchanges. A custodial wallet is a digital wallet where a customer's private keys are held by a third party.[9] These keys allow access to the underlying digital assets. Many customers who participate in digital exchanges use exchange-provided custodial wallets to allow the exchanges to trade the assets. But, if an exchange suffers a cybersecurity breach hackers can steal both the private keys and customer assets. Just one example of such a theft involved Mt. Gox, a Bitcoin exchange where over $450 million in customer assets were lost when the exchange was hacked.[10]

It is crucial that research is conducted into understanding what vulnerabilities allow for these incidents to occur. Understanding the vulnerabilities of intermediaries to the loss of customer wallets and assets could lead to the development of enhanced custody controls or to the recommendation of enhanced cybersecurity controls tailored to the needs of digital asset businesses and their customers. Increased research and development could also lead to policy prescriptions, including disclosure and auditing requirements, to ensure that such intermediaries have both appropriate policies and procedures and the means to make customers whole. Greater security in the digital assets marketplace would improve both customer confidence and economic growth.

---

7 *Id.*

8 Lin William Cong et al., *Crypto Wash Trading* at 2 (July 2021), *available at* https://arxiv.org/ftp/arxiv/papers/2108/2108.10984.pdf.

9 *See* Konstantinos Chalkias et al., *Proofs of Solvency in Blockchain Custodial Wallets and Exchanges* at 1 (Mar. 17, 2022), *available at* https://eprint.iacr.org/2022/043.

10 *Id.*

III. Conclusion

For the reasons expressed above, NASAA supports the OSTP's desire to prioritize research and development related to digital assets. Trading digital assets introduces risks for customers, and further research would better identify those risks. Identification of these risks would also provide the foundation to develop tools that regulators and law enforcement agencies can use to prevent these harms from occurring. We ask OSTP to focus on threats in the digital asset space that pose the greatest risks to customers, including manipulative trading practices and security of digital wallets held by intermediaries.

Sincerely,

[redacted]

Andrew Hartnett
NASAA President and
Deputy Commissioner,
Iowa Insurance Division

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Nathan Merill

From:	[redacted]
To:	DARD-FTAC-RFI
Subject:	RFI Response: Digital Assets R&D Agenda
Date:	Saturday, January 28, 2023 9:10:04 AM

To Nik Marda, Anna Brady-Estevez, and James Joshi, and whomever else it may concern:

I am writing in response to the RFI with regards to digital assets research and development.

My belief is simple and straightforward:

All existing cryptocurrencies are scams and should be banned. Their prices are heavily manipulated and driven by fraud, and they are, collectively, a Ponzi scheme.

All the companies issuing "stablecoins" should be shut down and investigated for fraud. Stablecoins are effectively a means of counterfeiting US Dollars (USD).

The only digital assets that should be allowed are Central Bank Digital Currencies (CBDCs) issued by the US and other developed countries with strong banking/finance industry regulations.

The entire crypto industry is a ponzi scheme.

Because cryptocurrencies have no way to generate value (they aren't some sort of business that produces a product or service) there is no way for them to generate value. Meanwhile, it costs money to operate these networks.

As such, the only way for anyone to make money off of cryptocurrencies is to sell them for a higher price than they purchased them for.

This is the "greater fool" theory, and is inherent to all ponzi schemes – the initial investors cannot make money because there is no value-generating asset, so the only way for them to make money is to get pay outs from later people who come in.

Because of the overhead expenses of operating these networks, cryptocurrency "investors" always are at a loss in real life, because you can only make money by selling them to someone for more than you bought it for, but the networks cost money to operate, so the net will always be a loss on average across all investors in the sector.

This is why online cryptocurrency communities contain a lot of memes about DCA (investing money constantly), HODL (meaning to hold onto assets and never let go of them), "Diamond Hands" (again, not selling off their assets), and similar memes designed to encourage people to hold onto their crypto – because when people pull their money out of a ponzi scheme, if people pull out more money than is coming in, the ponzi scheme will collapse.

Stablecoins, likewise, offer the illusion of people having "real" money in the system and discouraging them from pulling out; this serves to allow people to think that their money is “safe”, but these currencies are not truly backed by USD. In fact, it’s literally impossible for them to be. These are another critical component of the Ponzi scheme – by letting people see their assets grow “in the system” and keeping their assets there, the users don’t pull out more real money than exists in the system and collapse the scheme.

The supposed appreciation of cryptocurrency is driven almost entirely by fraud.

According to Bitwise’s report to the FEC, https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf 95% or more of the supposed trade volume of bitcoin is “non-economic”, i.e. fraudulent, designed to simulate trade volume and to manipulate prices. As other cryptocurrencies show these same patterns, this is almost certainly the case for all of them.

Over recent years, the modern-day increase in value has been driven by manipulation using stablecoins – primarily Tether, and more recently BUSD and other so-called stablecoins, which are purportedly backed by $1 USD each.

Here is how the con works:

1. The people who issue the stablecoins claim that the stablecoins are backed 1:1 with USD, making them equivalent to $1 USD.
2. However, in reality, the stablecoins aren’t backed by anything - the issuer simply creates them. This is why Tether and Binance have been resistant to undergoing audits. Binance has publicly admitted that their tokens have not “always” been backed, and Tether was found by the state of New York to have not been backed, which resulted in the company issuing them being sanctioned by the state of New York and banned from doing business there. https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal
3. The stablecoins are then used to purchase cryptocurrency assets. Because the stablecoin issuers can print an infinite amount of stablecoins, they can purchase these cryptocurrencies at arbitrarily high prices, as well as purchase them from themselves in “wash trades” to make it appear like they are being purchased at higher prices. This allows them to manipulate the price of these assets higher. This is why such a high percentage of bitcoin purchases are made using “Stablecoins” rather than real money. https://crypto-anonymous-2021.medium.com/the-bit-short-inside-cryptos-doomsday-machine-f8dcf78a64d3 https://miro.medium.com/v2/resize:fit:720/format:webp/1*khpKB3DTiXm8v05uZ9rCsA.png https://miro.medium.com/v2/resize:fit:720/format:webp/1*TsCPBPpMlYmI5pMWAMOoYw.png https://miro.medium.com/v2/resize:fit:720/format:webp/1*85xFugkRPM_9krGPN8-irw.png https://miro.medium.com/v2/resize:fit:720/format:webp/1*erl_pALuZ4ij2ePl4HkrHQ.png https://miro.medium.com/v2/resize:fit:720/format:webp/1*8xF_uY0xt1cD78rWCLmCyg.png
4. They then use the illusion of these assets being highly valuable and going up in value to sell these crypto assets to incoming people for real money (USD, typically). This is how the scheme actually makes money.

This scheme is, in effect, the creation of counterfeit US Dollars using stablecoins.

Indeed, spending a few minutes reflecting on the existence of Stablecoins, it is obvious that they must not be backed; if they were backed 1:1 by USD, then why would they even exist at all? It makes no sense – unless they either aren't backed by USD, or are being used for things that it would be illegal to use USD for.

This is precisely what is going on. Many ostensibly foreign exchanges are "unbanked" in order to evade US financial regulations, yet primarily do business with Americans and use these "stablecoins" as a means of keeping up the pretense. These were giving out large "rewards" of stablecoins, such as Tether, for years – and yet none of these exchanges were giving out similarly large rewards in USD, suggesting that these coins, despite ostensibly being worth $1 USD each, were not being valued like USD.

https://crypto-anonymous-2021.medium.com/the-bit-short-inside-cryptos-doomsday-machine-f8dcf78a64d3

They also allow for very high levels of leverage in many cases, allowing for further price manipulation using these "stablecoins". Moreover, many of these exchanges are not truly offshore; they keep up a pretense of being offshore to avoid US financial regulations but use a shell company in the US to help get people into them. For instance, Binance has a Binance US which is ostensibly independent, but there is significant evidence that Binance and Binance US comingle funds, suggesting they are a single entity.

https://dirtybubblemedia.substack.com/p/is-binanceus-a-fake-exchange?utm_source=direct&utm_campaign=post&utm_medium=web

While some of these entities claim that these coins can be redeemed 1:1 with USD, this is often not really the case; Tether, for instance, will only redeem actual USD to a small number of other crypto entities – all of whom are deeply entrenched in the Tether ecosystem.

Indeed, Tether's supposed backing by USD is clearly impossible: **in 2020, there was more Tether issued than existed foreign currency in all of the banks in the Bahamas (where Tether is based) put together**. The amount of Tether in existence rose from $4,600 million to $10,000 million in 2020, while the amount of foreign currency in the Bahamas rose by only $600 million over the same timespan

https://miro.medium.com/v2/resize:fit:4800/format:webp/1*sZuis07R0b7qXkyqXTBrow.png

It would be literally impossible for Tether to get enough USD from banks in the Bahamas to cover its Tether related liabilities.

But it gets worse than this: it is likely that literally every part of crypto has always been a fraud from its very inception.

Bitcoin itself is almost certainly a Ponzi scheme itself by design.

The basic principle behind Bitcoin is that it is a deflationary currency – there is a limited amount of bitcoin that will ever be produced, and thus, according to the claims that are used to drive its price higher, it can only get more and more valuable over time, because the supply is limited but the demand isn't.

But a few moments reflection will reveal that there is no reason for it to actually be deflationary in real life. There is no reason for its demand to continue to go up over time – in fact, its sharply limited number of transactions per second makes it very bad as a currency, limiting how many people could ever practically use it in the first place – and it generates no value.

How can Bitcoin purportedly gain value when it generates no value, and in fact, costs money to operate the network?

The answer is, of course, this is a contradiction in terms.

What is actually going on is that Bitcoin is a Ponzi scheme – people who buy in can only make money if they can find a "greater fool" to buy in at a higher price, because Bitcoin itself can generate no value, as it produces no products and provides no services.

A bitcoin is always worth a bitcoin – no more and no less – but the amount of energy used to do these transactions only goes up over time, meaning more and more value is lost over time through transfers of this fake "currency".

No, the idea that it is "deflationary" and has a "limited supply" is used to drive FOMO – Fear Of Missing Out – and give people the sense that it is an asset which will only go up in value over time, without there being any actual underlying thing of value to do that.

Indeed, it is possible to create an infinite number of copies of the Bitcoin network, and an infinite number of other cryptocurrencies – there is no actual limit on the amount of "crypto" in existence, which means that there is no reason to even believe it would be deflationary in the first place.

The government should take the following steps with regards to cryptocurrencies and stablecoins:

1. **Ban the issuance of so-called stablecoins by non-governmental entities** – the issuance of digital tokens that are purportedly backed by $1 USD is just a backdoor way to counterfeit USD and a way to defraud people.
2. **Ban the purchase of stablecoins using USD**.
3. **Ban the purchase of cryptocurrency using USD**.
4. **Ban the trade of cryptocurrency in the US**.

There is no value in these things except for defrauding consumers. They purport to go up in value or to be worth a set amount of money, but neither of these things can be true – they generate no value which would cause them to appreciate in value (unlike a corporation or other investment), they have very undesirable properties as far as digital transfer of money goes (high transaction fees, low number of transactions per second), and they enable fraud and de-facto counterfeiting of USD.

If the US government wants to issue a **Central Bank Digital Currency**, it should not use blockchain technology. There is no advantage to blockchain technology.

Instead, it should use a simple digital ledger system that is regularly backed up.

Transaction fees of any such CBDC should be very, very low, and CBDCs should exist for the benefit of consumers, not the benefit of banks. These should try to minimize fees and make it as easy as possible for people to transfer money, while simultaneously keeping a ledger of all transactions which can be used for tax purposes. It should be verifiable who is making these transfers, who the money is coming from, and where the money is going on.

It would be wise to restrict any US CBDC either to entities within the US, or to within developed countries with strong controls on the finance industry and fraud (the US, Canada, Australia, New Zealand, Japan, Northern and Western Europe). Right now there is a huge amount of digital currency fraud, and by making it impossible for entities outside of our sphere of influence to be able to use this money, it will make it much harder to use this for fraud and also drive countries towards wanting better financial regulations that would make them compliant with our CDRB so they could use it.

We do not want to have this CBDC be useful to Russia, North Korea, Iran, or other entities that are sanctioned; we do not want to allow them to use our electronic currency system to evade sanctions.

Additionally, some developing countries – like India and Nigeria – are engaging in large amounts of phone and email fraud, trying to defraud Americans of their money. These countries should not be allowed to be part of any sort of CBDC network, as we do not want people to be able to transfer their money to these fraudsters. Moreover, excluding countries from the network that are engaged in lots of illegal activity will help force these countries to clean up their act.

Unfortunately, I believe the same should also apply to Mexico and other places in Central America, to avoid allowing the drug cartels there to easily launder money, as well as places like the Bahamas, which have enabled a lot of crypto-fraud (such as Tether).

The only digital assets (money equivalents) that should be allowed in the US are CBDCs – and only those issued by the US and other developed countries with strong finance controls and controls against fraud.

Thank you for your time reading this response.

I believe that a total ban on all cryptocurrency and stablecoins is what is best for the US economy and US consumers, now and in the future. It is not innovation; it is fraud.

A central bank digital currency issued by the US government could be useful, but it needs to not use the blockchain, have minimal transaction fees, exist primarily for the benefit of end consumers, be traceable, and not be available to entities where large amounts of fraud and money laundering are occurring, and not be available to sanctioned countries.

Sincerely,

Nathan Merrill
Member of the Public and Employee of the State of Oregon

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Onai Inc.

Onai Inc.(Organization)
Industry (Small Business)

Office of Science and Technology Policy (OSTP): RFI Response: Digital Assets R&D Agenda

Goals, sectors, or applications that could be improved with digital assets and related technologies:

We start by highlighting the emerging impact on healthcare and biomedicine. Our company, Onai, for example is using privacy-preserving blockchain technology to enable analyses of patient data across healthcare institutions—without any data leaving each hospital or being exposed in any way to the other institutions. We are even able to train sophisticated AI models in this fashion. This enables us to remove the tension between fully leveraging data for public benefit and keeping data totally secure and private. Development of this technology was funded in part by the NSF.

As another example, we are a performer on an NCATS initiative to bring the power of blockchain-enabled privacy-preserving analytics to drug discovery where data is often highly proprietary and confidential.

These technologies also enable better collaboration and use of resources. For example, we are able to create a marketplace for scheduling of automated lab equipment, etc., while enabling anyone to add functionality, without needing a central gatekeeper as would be needed with a traditional database. Open science is the best science.

Outside of biomedicine, there are also key applications in defense, distribution of public benefits, and finance.

***Opportunities to advance responsible innovation in the broader digital assets ecosystem*:**

Given the wide applicability of privacy-preserving technologies and the number of domains impacted (law enforcement, healthcare, etc.), there would be value in federal opportunities to apply innovations within the government to public problems. The key value of pilots and engagement here is not funding, but rather two-way learning. Researchers and innovators could learn deeply about the details of a government data problem and those in the public sector would learn more about the abilities and limitations of this new technology, where it can prove itself useful and where it cannot.

Other information that should inform the R&D Agenda:

Given the appearance of efforts to regulate or prohibit Bitcoin “proof of work” mining, we believe it important for Government officials to understand these proofs to a sufficient degree to not accidentally inhibit “proofs of useful work” or other types of computations and Sybil resistance mechanisms.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

OneName Global, Inc.

RFI RESPONSE– DIGITAL ASSETS R&D AGENDA

onename

RFI For Office of Science and Technology Policy

Created by:

Christopher J Kramer

President & CEO

OneName Global, Inc. - Respondent type: Entity, C-Corp

[redacted] -

[redacted]

INITIATIVES

- CBDC that will help grow the economy, provide societal benefits, and advance equity and inclusion.

- A Properly designed CBDC system rollout that prioritizes security & safety, while maximizing opportunity and benefits to the American people.

- Fully interoperable ledger system that prioritizes recommendations outlined in reports pursuant to E.O. 14067, such as OSTP's report titled *Climate and Energy Implications of Crypto-Assets in the United States.*

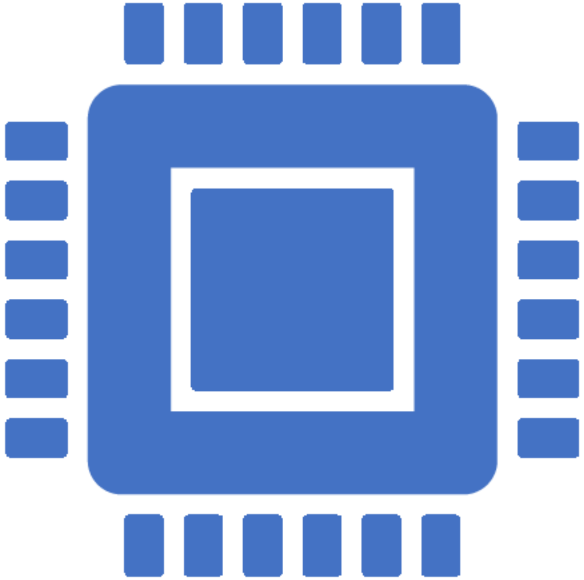
RECOMMENDATIONS

- Initial “opt in” CBDC rollout that will create excitement with a framework of benefits to include financial health, and governance that will grow the economy and incentivize CBDC adoption.

- The CBDC platform will include user profiles, digital wallets, artificial intelligence enabled - scalable AML/KYC technology, 2FA that will allow a safe environment for adoption and learning, while maximizing benefits of a CBDC platform for the American people.

- A multi-blockchain, fully interoperable platform and ledger system to include a developed API that can help facilitate a safe CBDC rollout with the ability to support member banks travel rule and tracking requirements to streamline efficient deployment of clearing and settlement of tokenized financial assets for a structured CBDC rollout. CBDC will leverage blockchain protocols that are energy efficient *such as proof of stake (POS) and delegated proof of stake (DPOS) protocols for maximum CBDC efficiencies..*

Scalable, Secure & Energy Efficient Blockchain



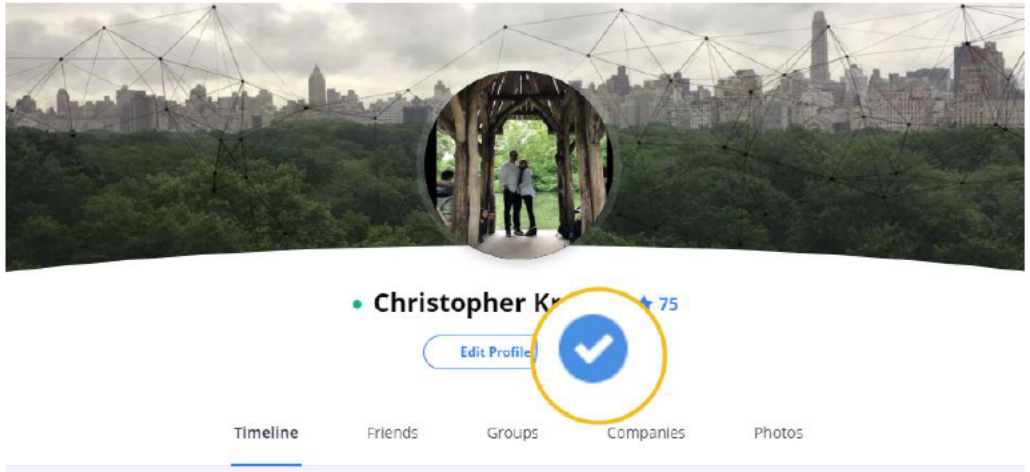
- The system should leverage a hybrid web2/web3 multi-cloud, hyper-scaling technology, to support scale with top level security and energy efficiency. The Blockchain currently boasts 100K transactions per second (TPS) thousands of distributed nodes, and 3 second block times that uses POS and DPOS protocols that will allow a CBDC to meet E.O. 14067 climate and energy requirements.

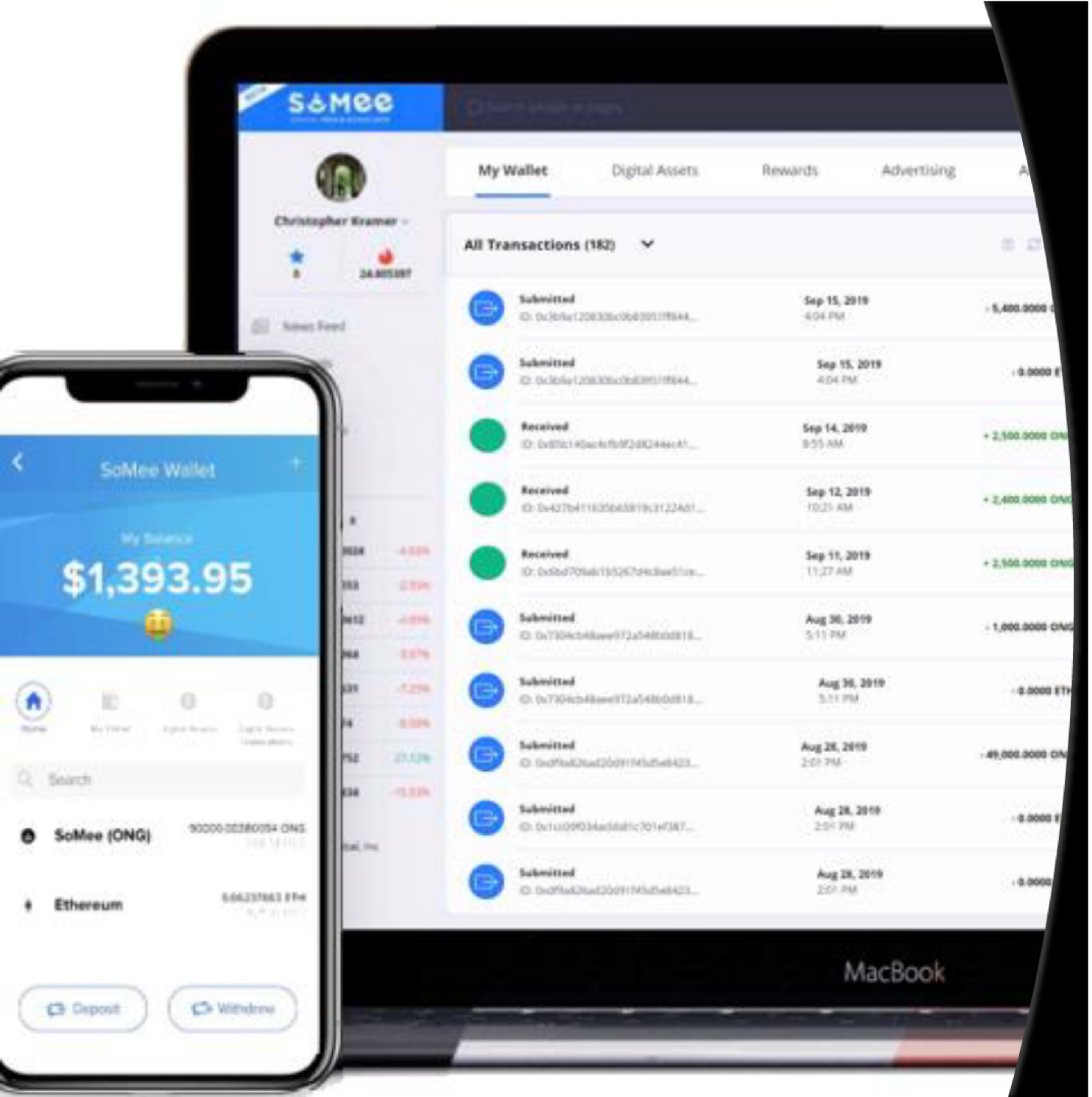
RECOMMENDATIONS

- **Simple Customer Onboarding**

A CBDC system that allows simple onboarding of customer profile accounts with the ability to leverage web2 design (text, 2FA) interactions to control web3 actions.

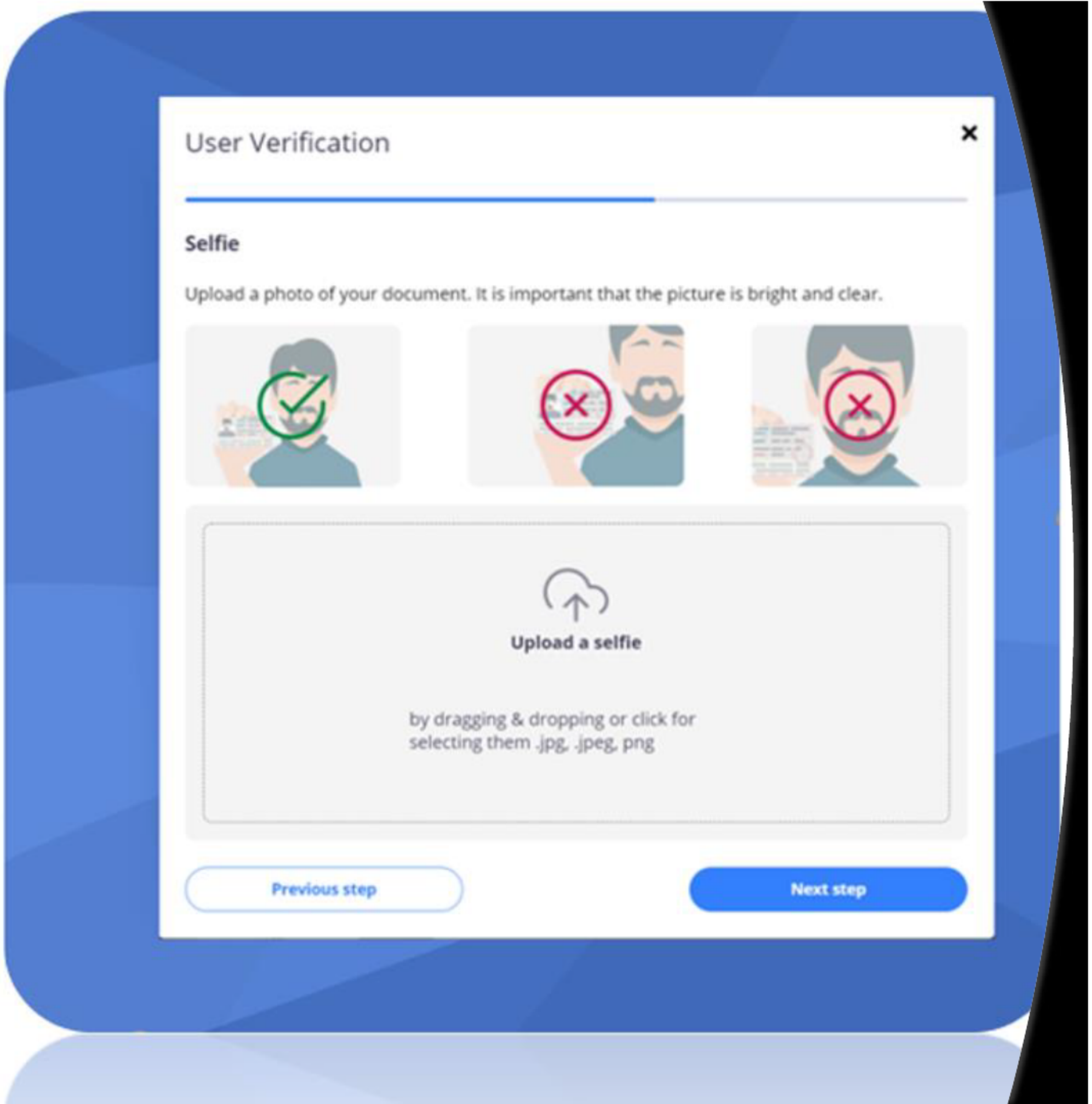
I.E. it needs to be extremely simple for the average person to use.





Built For Simplicity and Security

- Easy profile set up.
- 1 click noncustodial wallet creation – Separate, secure password required.
- 20+ noncustodial wallets generated at signup automatically.
- Multi-two factor authentication methods for user security.
- Available on Web & Mobile Via IOS & Android Stores.



Scalable AML/KYC

The existing technology utilizes an artificial intelligence enabled, scalable user verification system that is AML/KYC compliant and meets strict and secure data handling requirements.

Thank you

Christopher J Kramer

President & CEO

OneName Global, Inc.

[redacted]

[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

OpenEarth Foundation

Comment to the U.S. OSTP on the Priorities for Digital Assets Research and Development

Introduction

The current climate accounting approaches are woefully inadequate to consider national, subnational, and local climate action, resulting in a fragmented and heterogeneous accounting system. Such heterogeneity and fragmentation largely prevent the integration and consideration of information from subnational and non-state actors, such as corporations, cities, and regions into the international context. Multiple authors have already highlighted this risk of increasing fragmentation and general complexities in global environmental governance (Elsässer et al., 2022), particularly among the Paris Agreement actors (Atkinson et al., 2017; Widerberg and Pattberg 2017). Here, many developing countries continue to lack the necessary institutional capacity (Aldy 2018) for adequate accounting, and the 'vast majority of locally based self-organized climate change groups' are 'fragmented and embryonic' and 'lack the capacities/resources to engage' with larger networks, preventing 'mutual learning' and 'concerted action' (Atkinson et al., 2017).

Accordingly, this area of digital development presents an opportunity for the United States to provide a trustworthy infrastructure that can facilitate information sharing, transparency, and global governance in an increasingly digitized world. This can be achieved through foundational and translational research, spanning topics from cryptography to the social, behavioral, and economic sciences to improve collaboration between actors within the US and with partnering economies. By investing in this area, the US can contribute to building a more secure and transparent digital environment that fosters innovation and growth of novel financial models and assets, while also addressing potential trust issues related to (voluntary) carbon markets, greenwashing, and data privacy concerns.

Here, emerging technologies like Distributed Ledger Technology (DLT) can play a vital role in enhancing climate action transparency, building trust through new types of record-keeping, and creating new infrastructures for managing digital assets and providing novel financial services. In this context, we have identified three interconnected areas for potential research and development, digital infrastructure, environmental assets, and financial instruments.

Digital Infrastructure

Our research highlights the urgent need to enhance interoperability for climate and environmental data and assets through the creation of an infrastructure that promotes transparency and accountability. This infrastructure should comprise both soft and hard components, such as networks of actors and digital processes, technologies, and infrastructure that facilitates the establishment of a 'Digital Information Commons.' This Commons should be built on decentralized, shared, and open infrastructure that leverages digital technology to transform data into actionable information available to researchers, policymakers, decision-makers, and the public, thereby promoting better coordination of global climate action. The Digital Commons should be guided by key principles, including the traceability and transparency of data sources and methodologies, interoperability across actors and climate data systems, open access and inclusivity of climate data, and shared ownership and governance of global commons, such as the atmosphere or oceans (NASEM 2022).

Incorporating digital technologies, such as DLT and sensors, enable alternative accounting approaches that enhance trust and transparency through decentralized data governance. The combination of these technologies with artificial intelligence and machine learning can automate the data analysis and verification process, resulting in improved efficiency and reduced analytical burden, also known as the digital monitoring, reporting, and verification (dMRV) process (Belenky et al., 2022). Nested accounting provides a logic to integrate data across different governance levels. Here, emissions are accounted for at one level of analysis, such as a specific project or facility at the local level, before being factored into higher levels, such as the municipality, region, country, and international processes like the Global Stocktake (Schletz et al., 2022). Nested accounting was already included in Article 6.4 of the Supervisory Body (UNFCCC 2022) which provides guidance for the creation and transfer of assets between national Parties to foster collaboration.

Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) can enable novel forms of identity and reputation management that increase trust through attributability while also offering privacy preservation (Schletz et al., 2022). In the context of climate accounting and environmental assets, sensitive financial data should be private, and the digital infrastructure should maintain privacy and protect against arbitrary or unlawful surveillance.DIDs and VCs can play a crucial role in this regard by providing unique, persistent, and verifiable identifiers to authenticate individuals, organizations, or other entities (Davie et al., 2019; Sporny et al., 2019a), and digital documents that contain information about an individual or entity, cryptographically signed by a trusted issuer to ensure their authenticity (Lux et al., 2020; Sporny et al., 2019b).

Environmental Assets and Financial Instruments

Nature-based digital currencies (NBDCs) could play a crucial role in financing conservation and climate action operations. Ostrom and her colleagues' approach to economics and incentives can be applied to the design of how these NBDCs are to be governed, financed, and preserved in different localities by different peoples around the world. Institutions such as central banks and regenerative finance (ReFi) DLT protocols could develop instruments that effectively "bring natural resources on the balance sheet while preserving living capital". For central banks, this could take the form of Nature-Based Central Bank Digital Currencies (NB-CBDC) that includes and supports the natural sector of the economy, which is not typically considered in the policy.

The ReFi movement encompasses various web3 and crypto-based digital currencies to transform the governance of global common pool resources. This involves utilizing approaches such as dMRV, financialization of assets through tokenization, and decentralized governance to coordinate financing, governance, and regeneration of common pool resources. By pooling and tokenizing assets such as NBDCs, ReFi aims to leverage novel finance and market applications to drive the regeneration of natural resources. The movement operates across three systems of accounting, markets, finance, and governance, employing both digital and analog processes. Tokenization, for instance, has the potential to increase transparency in the carbon offset market by converting real-world assets into digital tokens that contain all relevant information, including the metric, issuing country, project name, and year generated (Franke et al., 2020). These tokenized assets can be used for new nature-based financial instruments in environmental markets and green finance.

CLIMATE ACTION DATA 2.0

WORKING GROUP

Future of Climate Action Data from Cities, Regions, Businesses, and Investors

convenors:

Camda for credible Climate Action

DATA DRIVEN ENVIROLAB

OPENEARTH FOUNDATION

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

PayPal

March 3, 2023

Via email: ***DARD-FTAC-RFI@nitrd.gov***

Office of Science and Technology Policy
Executive Office of the President
[redacted]

Response to Request for Information: OSTP Digital Assets R&D Agenda

I. Introduction

PayPal appreciates the opportunity to provide this letter in response to the Request for Information (RFI) issued by the Office of Science and Technology Policy (OSTP) to help identify priorities for research and development related to digital assets and various underlying technologies. Outreach with industry and experts in the digital asset field is critical as the government considers developing a framework for enhancing U.S. economic competitiveness and innovation related to digital assets and infrastructure.

Digital assets and their associated technologies offer immense possibilities to create more efficient and effective payments systems. We believe digital payments, including through the use of stablecoins and CBDCs, can be a key area where the United States has a competitive advantage given the quality of technology and domestic law and regulation. Further, if properly designed, CBDCs hold promise in providing individuals and small businesses with substantial benefits, including increased access to financial services, lower costs, faster transaction speeds, enhanced privacy, and greater optionality, leading to overall improved financial health.

II. The Future of Money

Advances in technology, including the use of digital assets and smart contracts, have the potential to fundamentally change the way in which payment and financial activities are conducted. Digital asset infrastructure represents the next generation for a digital economy – bringing enhanced efficiencies, programmability, speed, accountability, and access. Through proper understanding and exploration of the benefits of tokenization, blockchain, and distributed ledger technology (DLT), we can develop modern financial infrastructure that better serves American consumers and small businesses.

We note and acknowledge at the outset, however, that the fundamental potential that digital asset technology presents can at times be obscured by high-profile failures of certain actors or specific financial assets they have developed. As with financial services and markets more broadly, some assets and platforms are well-designed, while others lack transparency or clear value propositions. It is important to separate the objectively real elements of innovation from hyperbole.

To do this, we should consider policies that unlocked past periods of digital innovation, including with respect to early Internet development. A sound combination of government collaboration, public research funding, private innovation, global attraction of talent, and appropriate regulation cemented the role of the United States at the center of the digitization of communications, media, commerce, and Internet-based financial services, but that was not inevitable. It took forward-leaning leadership, as is being demonstrated today with this RFI.

We have been learning a great deal about digital assets, establishing in early 2022 an internal cross-disciplinary advisory council for our Blockchain, Crypto and Digital Currencies unit comprised of some of the world's leading experts in cryptography, distributed technology, regulation, economics, and capital markets. And we're committed to working with governments and regulators to help responsibly shape the future of digital financial services. We believe CBDCs, digital currencies, and stablecoins could be great additions to the payment options available to businesses and consumers and complement the current retail payments system. It is critical for the U.S. government to play a leadership role in supporting the rise of domestic industry and fostering a cohesive global policy framework for the digital asset ecosystem.

III. Payments Innovation & Financial Inclusion - Clear Goals for Research & Development (Question 1)

A. Payments Innovation and US Global Competitiveness

As it stands today, the current payment rails are inconvenient and expensive, taking days to settle transactions, providing limited visibility to businesses conducting international payments, and charging high fees – especially to lower-income and underbanked segments of the population that are forced into costly check cashing, money order, payday lending, and remittance services.

New technologies and thoughtful regulation provide an opportunity to reshape the financial system to benefit the underserved; to support businesses, professionals, and creators with faster, lower cost payments as well as access to credit; and, to relieve financial stress for the general public. Responsible innovation in payment systems, lending, digital currencies, digitized protocols, digital identity and in the fight against fraud and financial crime can bring a new era of equitable, low cost, and accessible financial services. The time is ripe to modernize and upgrade the technological infrastructure of the financial system – and the United States is well-positioned to lead both in terms of private sector innovation and public sector engagement.

[redacted]

Across the globe, governments are actively studying the merits of CBDCs, with 114 countries (representing over 95 percent of global GDP) noting active exploration.[1] We accordingly believe the United States should take a leadership role in this space, especially with respect to establishing global standards.

The U.S. dollar plays a critical role not just domestically, but across the globe. As the primary global reserve currency, the dollar is used to conduct international transactions based on the availability and prevalence of financial instruments denominated in dollars as well as the depth and integrity of U.S. financial markets. The relative stability of the dollar against other currencies instills trust and confidence that dollars will serve as an effective medium of exchange and store of value. The importance of dollars in international transactions makes the Federal Reserve one of the leading central banks that can provide international liquidity.

If the U.S. dollar is to remain the world's primary reserve currency in the unfolding century, then being at the forefront of technological innovation that reduces friction in payments should be an area of focus. Accordingly, the U.S. government and the OSTP should actively explore and consider new digital forms of money that can most effectively operate in an increasingly digital world. PayPal believes that a digital dollar could be a logical next iteration to futureproof the U.S. dollar. A properly designed digital dollar could promote diversification of the payment system and spur financial innovation, inclusion, and global currency interoperability.

To maximize its benefits and reduce disruptions or causing instability, we believe a future digital dollar should embody certain key tenets, including:

- Operate alongside existing and future payment options and innovations, including but not limited to ACH, wire, credit, and private digital currency payment solutions;
- Be offered to retail and wholesale users;
- Be facilitated and distributed through accounts and digital wallets at regulated banks and financial services companies, such as trust companies and money transmitters;
- Ensure individual privacy, while satisfying law enforcement requirements;
- Promote global digital currency and network interoperability
- Be flexible in its design to account for future technology, policy, or economic changes; and
- Encourage private sector innovation and collaboration.

B. Financial Innovation Should Be Viewed through the Lens of Financial Health & Inclusion

We believe that financial health and inclusion can and should be a key goal of any research and development effort regarding blockchain technology. We believe financial innovation and access are key

[1] Atlantic Council - Central Bank Currency Tracker, accessed 03/01/23, https://www.atlanticcouncil.org/cbdctracker/.

prerequisites to maintaining the broader goal of "Financial Health." Helping people to accomplish and/or maintain strong financial health is at the heart of PayPal's mission to democratize the movement and management of money.

It is well documented that nearly 7.1 million households in America remain unbanked, with the majority of such households being Black and Hispanic. Notably, a 2021 survey found that one of the primary reasons individuals remain unbanked is due to distrust of banks given experience with surprise punitive fees, such as overdraft. [2] The underbanked represent an additional subsegment of the U.S. population that is currently underserved by the financial system. Approximately 20% of U.S. households are considered underbanked, meaning that they used alternative financial products outside the banking system.[3] A further 69% of Americans are living paycheck-to-paycheck, meaning they would experience financial difficulty if paychecks were delayed for a week.[4] And, 77% of Americans report feeling anxious about their financial situation.[5]

We firmly believe that how we pay for goods and services is fundamental to financial health, meaning that consumers must have choice in payment methods, understanding of payment options, visibility into their financial standing, financial options to achieve their goals, and the ability to exercise those needs in the coming digital age. The advent of stablecoins and CBDCs presents another option that could be widely used, as it is pegged to fiat currency and could enable faster cheaper financial transactions in the digital environment and, depending on design, could potentially fulfill currently unmet and future payments needs.

First, if crypto currencies, including stablecoins and CBDCs, were made available through a digital wallet service offered by regulated financial services firms, it is likely that a meaningful percentage of **currently un- and underbanked individuals would find benefits.[6]** There are numerous and complex causes that contribute to unbanked and underbanked populations. We need to study these and address them individually – there will be no one solution to this global problem. It is a problem that deserves thought and action, which may need to come in small doses to test solutions for effectiveness or recalibrate to achieve the desired results. While a U.S. CBDC may not succeed in converting all unbanked and underbanked persons into those that fully utilize the needed financial services, even impacting a small

[2] Federal Deposit Insurance Corporation, *How America Banks: Household Use of Banking and Financial Services 2019*, Oct 2020, https://www.fdic.gov/analysis/household-survey/2019execsum.pdf.
[3] Federal Deposit Insurance Corporation, *2017 FDIC National Survey of Unbanked and Underbanked Households,* updated Dec 2021, https://www.fdic.gov/analysis/household-survey/2017/index.html.
[4] PRNewswire, *Number of Americans Living Paycheck to Paycheck on Decline Despite Pandemic,* Sept 2020, https://www.prnewswire.com/news-releases/number-of-americans-living-paycheck-to-paycheck- on-decline-despite-pandemic-301134207.html.
[5] CNBC, *77% of Americans are anxious about their financial situation—here's how to take control,* May 2022, https://www.cnbc.com/select/how-to-take-control-of-your-finances/.
[6] *See, e.g.,* The Digital Dollar Project, *Exploring a US CBDC,* May 2020, http://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf.

percentage of the 20% of U.S. households that are underbanked is worthwhile and should be fully considered.

Digital wallets could be tailored to offer access to digital dollars, custody, and related payments services. These offerings would be in parallel with other payments services, providing competition and consumer choice. Once onboarded through a digital wallet service, a previously unbanked or underbanked individual would find herself connected to the global financial system and e-commerce platforms.

Second, the impact on G2P payments could be immense. Far too many Americans waited months to receive stimulus checks at the onset of the COVID-19 pandemic. A combination of tools like CBDCs, stablecoins, and digital identity could enable these individuals to receive their money through direct deposit in a far more timely manner. G2P payments provide a lifeline to millions of Americans and can be made far more efficient with digital assets.

The pandemic underscored the importance of access to accurate, timely, safe, efficient, and affordable payments for all Americans and the high cost associated with being unbanked and underbanked. Approximately 35 million individuals had to wait for months to receive their stimulus checks, if they received them at all.[7] PayPal was honored to participate in the disbursement of stimulus checks. In the first round alone, 100,000 payouts were made to PayPal and Venmo accounts using the Direct Deposit feature. In the second round, 117,000 were made via PayPal and Venmo using that feature. Instead of waiting for physical checks to be printed and mailed and later cashed and deposited, individuals and households could submit their PayPal account details directly to the IRS website and elect to receive their stimulus payment through Direct Deposit into a PayPal CashPlus account. The challenges of getting relief payments to these households highlighted the benefits of delivering payments more quickly, cheaply, and seamlessly through **new digital infrastructure**, and CBDCs can be a means of increasing financial inclusion and improving financial health.[8]

Third, given the likely speed, efficiency, and cost benefits of certain digital assets, low-income individuals should be able to **shift certain financial activity away from high-cost legacy providers**, including check-cashers and payday lenders, that often come with significantly higher fees.

Fourth, cross-border **remittance transactions could become more efficient and cost effective.** Many individuals face high fees sending money across borders due, in part, to numerous intermediaries; an interoperable digital dollar that could be readily exchanged across borders and converted into another digital fiat currency holds promise in connecting funds more directly, quickly, and efficiently to those who need them.

[7] CNBC, *35 million stimulus checks are still outstanding. What you need to know if you're waiting for your money,* June 2020, https://www.cnbc.com/2020/06/08/35-million-stimulus-checks-havent-been-sent- out-who-is-waiting-for-money.html.
[8] PayPal, *Addressing Your Questions About Government Stimulus Payments,* accessed May 5, 2022, https://newsroom.paypal-corp.com/covid-19-addressing-your-questions-about-government-stimulus-payments#:~:text=Elect%20to%20receive%20your%20stimulus,and%20you%27re%20all%20set.

Fifth, stablecoins, CBDCs, and related technologies could **support small business merchants** by providing them (and customers) with a new form of payment, especially given reduced physical cash dealings and the trend toward reduced cash usage. Indeed, as economies move away from physical money, it is prudent to offer the public access to a modern, digital form of cash. A digital dollar can offer important competition against other forms of payment and allow participants access to central bank money through regulated intermediaries.

Finally, digital assets would be **responsive to clearly shifting preferences** among consumers. Younger generations are increasingly reliant on mobile access to digital services, and a digital dollar meets them where they are. Offering public money in a digital format would appear to be the next step in the natural evolution of the dollar.

III. Understand Privacy and Climate Impact to Mitigate Potential Risks (Question 3)

A. Getting Privacy Right

One of the most important elements of digital assets broadly, and a U.S. CBDC more specifically, is ensuring user privacy while satisfying legitimate law enforcement requirements, and we encourage the OSTP to focus research and development efforts in this area. Many have expressed concern that CBDCs could allow for government surveillance of citizen payment transactions, especially to the extent that the digital currency transacts upon highly centralized government rails. On the other hand, some worry that treating as a pure analog to cash along with its anonymity features will facilitate illicit activity and threaten national security.

Given these important considerations, it is imperative that the United States gets privacy right. With thoughtful design and implementation, the digital dollar could enjoy competitive advantages relative to other national CBDCs that permit unchecked surveillance. One advantage the United States already enjoys is existing legal due process and protections when it comes to individual financial information. These protections, which include those under the 4th Amendment of the U.S. Constitution, should be embedded within the design of a digital dollar and associated authorizing legislation.

Notwithstanding the importance of privacy, it is also important that CBDCs, stablecoins, and digital assets more generally be capable of meeting key law enforcement requirements and objectives. A design that relies on regulated entities to serve as digital wallet service providers can ensure implementation of key KYC/AML requirements. We encourage the OSTP to actively explore leading-edge privacy technologies that can help satisfy privacy and law enforcement objectives simultaneously.

For example, zero-knowledge proofs are an area of development that allows network participants to validate certain information without having direct access to underlying, sensitive information. In the context of KYC/AML, this might mean verifying that an individual is not on a sanctions list without revealing the identity of the individual to the entity seeking verification.

B. Mitigate Climate Risk

PayPal is focused on advancing our mission of democratizing financial services, while responsibly managing and reducing our environmental impact. PayPal is proud to have supported the development of the Crypto Climate Impact Accounting Framework, co-authored by the Crypto Carbon Ratings Institute (CCRI) and South Pole.[9] This initial effort enables better understanding of how companies involved in the cryptocurrency ecosystem can begin to account for their emissions, which is a first step in determining how to reduce those emissions. We welcome to opportunity to continue this work alongside the OSTP to better research, track, and understand climate emissions associated with digital assets.

IV. Prioritize CBDC Technology in R&D Efforts (Question 4)

A. CBDC Technology

We encourage the OSTP to focus R&D research on greater automation. Digital asset technology holds the promise to drive key benefits across the payments system including increased speed and efficiency; greater security; innovative new functionality; interoperability; and programmability.

One of the central benefits of digitized modern payments rails that leverage some of the innovations in blockchain and cryptography is the ability to **automate t**he settlement of payments and maintenance of the ledger. It is this automation that can eliminate costly, time-consuming, and sometimes manual processes associated with legacy infrastructure. This advantage can reduce transaction times and costs. It can further simplify the payments system by removing siloed databases and providing access to consumers and businesses to previously closed networks.

These features can result in a dramatically **more efficient and speedy financial system**. This in turn could result in reduced costs compared to the current system. The use of a digital dollar that transacts on more efficient rails should include regulated digital wallet providers who can process payments on the designated rails (and help manage or ensure proper governance of the rails) and the central bank operator of the CBDC system. Settlement times that today take days can be reduced to minutes, and errors that can be introduced due to the many intermediaries and systems through which a payment typically flows can be significantly reduced. As a result, financial system participants will not only have greater transparency into the movement of funds but will also enjoy greater liquidity and improved cash flow, further stimulating the economy.

A properly designed CBDC can also serve as a foundation for a **safer and more secure** payments network. Because digital currencies can employ multi-layer security in addition to strong authentication and authorization assurances, they can be subject to secure processes like multiparty authentication or

---

[9] Crypto Carbon Ratings Institute and South Pole, *Crypto Climate Impact Accounting Framework*, https://www.southpole.com/reports/report-accounting-for-cryptocurrency-climate-impacts.

enhanced transaction verification. Additional features embedded in a digital currency can facilitate compliance with reporting requirements, support AML and anti-terrorist financing efforts, and assist law enforcement in the prosecution of financial crimes. Notably, emerging encryption technologies can provide these benefits while preserving consumer privacy and control in how their data is used and shared.

The third feature of CBDC technologies is the ability to **spur additional innovations** across the financial sector. At PayPal, we have seen firsthand the impact that digitization has had on the economy and society. The ability to perform many different kinds of financial transactions directly on a mobile device has improved accessibility, particularly in rural locations and banking deserts. Giving small businesses the ability to accept payments digitally has enabled them to compete on a national or global scale. With more aspects of our lives taking place online, it's easy to see that a secure and open digital dollar could power use cases that we cannot conceive of today.

The fourth key feature of CBDC-related technology is the potential for **enhanced interoperability**. Domestically, this means operating alongside, and easily convertible to, other forms of digital currency as well as digital representations of fiat currency. The system should facilitate consumer and business optionality and choice. The breaking down of silos provides an opportunity to connect digital economic systems, including other global CBDCs and financial networks. Interoperability, however, is predicated on careful coordination between the central bank issuers of CBDCs and related stakeholders, along with the development of standards. For this reason, **we urge the OSTP to research and promote interoperability standards, including with respect to privacy and security.**

The final technological benefit of a CBDC is its **programmable nature**. This refers to "smart contracts" which enable tokens or currencies to be "programmed" to perform specific functions, like paying a mortgage on a certain date. Programmable money could help to reduce money laundering and terrorist financing by embedding eKYC and sanctions screening functionality. Tied to the concept of automation, digitized money can be wrapped in smart contracts and coded to include certain features and behave in determinable ways. The programmable nature of digital money means that regulation and compliance requirements can be embedded in money itself, and that business logic can drive desired outcomes. For example, a digital dollar could be programmed for humanitarian distribution in a disaster zone and only usable for the purchase of essential food and medical supplies in the first instance. In the context of financial markets, digital dollars could be programmed to facilitate clearing and settlement of transactions at efficient intervals.

With OSTP spearheading research and development, in partnership with the private sector and industry, the United States has an opportunity to lead global efforts for the advancement of critical technology infrastructure for digital assets.

V. Advance Responsible Innovation through Standards Setting & Private Sector Participation (Question 5)

Given the potential for the technologies underpinning digital assets to form the next generation of financial services infrastructure, governments around the world are taking steps to champion domestic innovation and industry. It is well known that China is the global leader in piloting its CBDC, the digital yuan (or e-CNY), and that leading jurisdictions, including Europe, the UK, and Korea, are taking steps to support digital asset development. This accordingly marks a unique time where a “whole of government” approach is needed to support U.S. digital asset innovation that incorporates core democratic values and a focus on privacy, security, and consumer protection.

For this reason, we recommend exploring the formal development of public-private platforms to advance digital asset standards. By investing in standards and including leading U.S. private sector expertise, we can ensure that the future of global and interconnected digital infrastructure is imbued with U.S. norms, values, and know-how.

VI. The Importance of Regulated Non-Bank Financial Services Providers in Issuance and Distribution

PayPal has long worked to expand financial inclusion and health in the digital realm. We frequently work in partnership with banks and traditional financial institutions as a regulated financial services provider. We believe that digital assets hold particular promise in advancing inclusion and financial health if it recognizes the benefits of open systems and broad distribution of digital dollars by regulated entities beyond traditional banks.

The traditional banking system has faced challenges in reaching all segments of the population, especially historically disadvantaged, minority, and low-income groups. Regulated payments providers like PayPal and Venmo typically offer free onboarding and carry no minimum balance. Additionally, PayPal’s two-sided platform connects both consumers and merchants in a seamless manner. Our services provide a favorable experience for the consumer and entree into a digital marketplace that does not typically accept cash or checks.

Recent research underscores this dynamic by noting that regulated payments providers were far more effective in reaching minority-owned businesses during the COVID-19 pandemic to offer them Paycheck Protection Program (PPP) relief.[10] For example, PayPal’s PPP loan program is over- indexed in the majority of the top 30 counties that have the highest density of Black business activity and heightened incidence of COVID-19. More specifically, the coverage rate for PayPal-facilitated PPP loans is above

[10] Washington Post, *Racial bias affected Black-owned small businesses seeking pandemic relief loans, study finds,* Oct 2021, https://www.washingtonpost.com/national/ppp-bias-black- businesses/2021/10/15/b53e0822-2c4f-11ec-baf4-d7a4e075eb90_story.html.

average in 23 out of these 30 counties[11], in sharp contrast to the overall PPP, in which the coverage rate is below average in 22 out of these 30 counties.[12]

Indeed, there is clear evidence that regulated payments providers are increasingly providing key services for underserved women and minority consumers.[13] For example, PayPal Working Capital (PPWC) loans are distributed to areas with greater concentrations of minority populations, helping to close the gap in access for minority entrepreneurs. The percentage of total PPWC loans going to census tracts with greater than 25% African American population share is slightly higher than traditional SMB loans (13% vs. 11%). Also, this same group of borrowers are growing more quickly than the average SMB (22% vs. 9%).[14]

Given the ability of regulated payments providers to reach broader populations, it is critical that a U.S. CBDC be offered and distributed through both regulated banks and non-banks, including state-regulated money transmitters and trust companies. Regulated payments providers specialize in nimble, consumer-friendly applications, as well as connectivity with other service providers. A U.S. CBDC offers a unique opportunity to leverage a broader set of regulated entities to help expand access to digital financial services.

***

We appreciate the opportunity to comment on this letter and are happy to engage with you further as you consider R&D involving digital assets.

---

[11] PayPal, *Resilience and Growth During the COVID-19 Pandemic: A Study of Digital Small Businesses,* Sept 2021, https://publicpolicy.paypal-corp.com/sites/default/files/2021- 09/C19_and_Digital_SMBs_PayPal.pdf.

[12] Federal Reserve Bank of New York, Double Jeopardy: COVID-19's Concentrated Health and Wealth Effects in Black Communities, *Aug 2020,* https://www.newyorkfed.org/medialibrary/media/smallbusiness/DoubleJeopardy_COVID19andBlackOwn edBusinesses.

[13] Federal Reserve Bank of Cleveland, *Fintech Lenders and Their Potential to Reach Underserved Women- and Minority-Owned Small Businesses,* accessed 05/12/22, https://www.clevelandfed.org/newsroom- and-events/events/2017/policy-summit/coverage/fintech-lenders-and-small-business.aspx.

[14] PayPal, *Alternative SMB Financing: Fueling Underserved Entrepreneurs,* Nov 2020, https://publicpolicy.paypal-corp.com/sites/default/files/2020- 11/Alternative_SMB_Financing_Fueling_Underserved_Entrepreneurs.pdf.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

PocktBank

PocktBank™

www.fednow.cash

Engineer #0
Founder and Inventor
United States of America FinTech Research and Development Program.
Statement in support of: National Digital Assets Research and Development Agenda (88 FR 5043)

Central Bank Digital Currency (CBDC) can serve as a secondary transactions layer, complementing existing banking infrastructure for domestic and cross-border settlements. By providing an alternative means of settlement, CBDC can improve liquidity and reduce settlement risks for banks thanks to blockchain processing integrity and programmatic auditing reporting. CBDC can enable near-instant cross-border transactions, reducing the time and cost associated with existing infrastructures not capable of financing a transaction modernization upgrade. CBDC can provide a more transparent and traceable system of transactions, improving accountability and reducing the risk of fraud with Web3 enabled ID integration. The introduction of a United States application level CBDC can increase competition in the financial industry by expanding the integration layers from mobile apps, VR, and IoT endpoints. By providing an alternative means of payment and settlement on the application level, CBDC can provide a "backup" subsystem that reduces the risk of a financial crisis caused by a system-wide failure or malicious attack on the United States traditional banking system.

Please visit www.fednow.cash for a public display of our foundation of FinTech R&D work.

[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Polygon Labs

Polygon Labs' Response to the OSTP RFI Seeking Comments on Digital Assets Research & Development

March 3, 2023

For additional information about this response, please contact:

Policy Team
Polygon Labs
[redacted]

About Polygon Labs

Polygon Labs is a software development company that builds blockchain network scaling solutions and complementary software to enhance the user experience in a blockchain-based Internet (also referred to as "web3"). Our mission is to provide more efficient and open blockchain infrastructure on which developers and the community can build and bring web3 to billions globally.

Over the last several years, Polygon Labs invested significant time and resources into promising early-stage technologies that improve Ethereum by increasing transaction speeds and decreasing transaction costs. To date, these efforts have been able to reduce blockchain transaction costs to the point where transactions on the Polygon network typically cost less than one cent,[1] and Polygon Labs continues to build on and improve these technologies.

The builder and user community has shown great receptivity to the benefits of the Polygon network. As of the end of 2022, developers had deployed countless applications on top of the Polygon network. These applications span various fields and industries, including healthcare, education, social media as well as decentralized finance ("DeFi").[2]

Although the technology is still at an early stage and may present some risks and limitations, research and development ("R&D") efforts from the U.S. government - like that of the Office of Science & Technology Policy ("OSTP") through the "Request for Information: Digital Assets Research and Development" ("RFI") - will provide additional insight and assist with building evergreen legislation relating to blockchain technology. We agree with the RFI that "[r]esponsible innovation in digital assets could provide significant benefits for the American people" and believe open dialogue with industry will facilitate innovation while ensuring the technology's safety and soundness, especially as it relates to the users.

Introduction and Recommendations

As the RFI recognizes, web3 – an internet powered by blockchains – has the potential to transform the economy. Although the Internet has already made great strides in bringing more individuals and businesses into the U.S. (and global) economy, a blockchain-enabled Internet will further reinforce this trend. Digital assets coupled with the broad ecosystem of blockchain technology and attendant applications built thereon will enable this innovation to add value to the U.S. economy. For that reason, Polygon Labs' response to the RFI (the "Response") focuses on blockchain-enabled applications – many of which are powered by digital assets – and not solely on digital assets themselves.

Web1 (1980s-2005) gave us the core infrastructure ("protocols") on which the current Internet is based and is freely accessible by anyone ("open"). In web2 (2005-2020), large technology companies built proprietary, closed protocols on top of the open Internet infrastructure and monetized these business models. This made them the "gatekeepers" of the Internet and gave them an ability to "commoditize users" — *i.e.*, requiring users to relinquish control over personal data, intellectual property, and choice to access basic websites.

---

[1] Compare Polygon POS chain average gas price chart with Ethereum average transaction fee chart.

[2] See applications in Polygon's ecosystem.

Web3 (2020+) is a return to the web1 ethos, with a determination to avoid the centralization of web2. It cultivates an ecosystem of projects that use open blockchain infrastructure for building and connecting. Rather than promoting predatory big tech intermediaries, a blockchain-enabled internet allows users to be stewards of their rights, including over their personal data, personally identifiable information, intellectual property, and financial well-being. Whereas this period seems to have kicked off in earnest in 2008 with the publication of the Bitcoin Whitepaper, the development of web3 infrastructure and applications has proliferated exponentially, particularly over the last five years.

Now, instead of simply blockchain networks, web3 comprises blockchain infrastructure solutions ("layer 2 networks" or "scaling solutions"), DeFi, decentralized social media, gaming, and other applications. Since 2018, monthly active developers have increased +297% (now averaging 23,000 monthly developers), and this accounts for the drop in overall value of the market within the past year.[3] The significant growth can develop further in an economic and regulatory environment that seeks to foster innovation, while protecting users and ensuring market integrity.

<u>Questions Posed in the RFI</u>

(1) Goals, sectors, or applications that could be improved with digital assets and related technologies.

A blockchain-enabled Internet can improve significant aspects of our society. Many of these improvements have been discussed at length over the past decade – *e.g.*, financial inclusion, efficiency in transactions, etc.

One of the more recent innovations with blockchain technology is the advent of "web3 social" – social media and networking protocols that return autonomy to users over all aspects of their social media experience. For that reason, the Response highlights the ways in which web3 social will positively impact individuals' social media experience.

In the current web2 world, users must relinquish their rights – over personally identifiable information and intellectual property – to receive access to interact with a website. Blockchain-enabled applications – whether they utilize digital assets or not – will return control over these valuable rights to users, increasing autonomy over their digital footprint and presence.

Limitations in current web 2 social and networking applications.

Big Tech tracks user data through browsing history, location, emails, among other means – whether covertly (*e.g.*, search engines) or overtly (*e.g.*, forced acceptance of "cookies" for most websites). Technology companies then use and sell (for profit) this data for advertising, marketing, or personalizing the browsing experience. In certain instances, this data collection may produce some benefit to users (*e.g.*, better suggestions for shopping), but this benefit is only a byproduct of technology companies seeking to maximize their revenues. One study found that when looking at iPhone applications that may appeal to children, two thirds of those apps harvested data on how children interacted with the app and sent that information to the advertising industry.[4] This may explain

[3] "2022 Electric Capital Developer Report," January 2023.

[4] Dave Davies, "Users beware: Apps are using a loophole in privacy law to track kids' phones," NPR, June 2022.

why in 2021, the estimate for children's advertising in the U.S. grew to $2.9 billion and is expected to reach $21.1 billion by 2031.[5]

Outside of tracking personal data, Big Tech also exercises similar amounts of control over a user's generated content ("UGC"). Many individuals contribute reviews and other types of UGC to a variety of sites like social media, crowd-sourced reviews platforms, personal blogs, among others. UGC allows users to create a "database" of content (whether visual or written) while simultaneously garnering an audience and building an online presence and reputation. However, a user's online presence is tied to a specific platform because both the UGC and following are non-transferable to other platforms.

This helps Big Tech companies to build a user base through network effects (the more users join the platform, the more appealing the platform becomes, and the more users join) while maintaining control of this user base by "locking in" users to their platform. In this sense, Big Tech exercises ownership over all the user's UGC while also leveraging the user as a personal, profit-generating tool without offering any compensation.

The same is true as it applies to a user's intellectual property. Online, two forms of intellectual property come into play: "formal" and "informal." In the formal system, different types of IP (*e.g.*, trademark, patent) require different types of legal frameworks, making the system fragmented and complicated. The informal system relates to UGC, in which no legal frameworks or recognized rights exist. This allows Big Tech to "own" all a user's content, following, and therefore, the user's entire presence on a given platform.

Where blockchain provides benefits in web2 social applications.

In blockchain-based/web3 social or networking internet applications, users reclaim control over their internet experience: data, content, and following. Users do not relinquish their personal data; instead, when the user wants to engage with the Internet, they connect their personal, self-hosted wallet to any application. These self-hosted wallets are pseudonymous – meaning that they are identified only by a string of letter and numbers – and do not necessarily contain any personal data, unless the user intentionally has included a type of digital asset (*e.g.*, non-fungible tokens ("NFTs")) with such information or which represents such information.

Blockchain-enabled social applications also reshape the idea of ownership and UGC. In 2021, YouTube had total revenue of $15 billion with 37 million channels and paid out an average of $405 per channel whereas total NFT sales totaled $3.9 billion with 22,400 creators, and the creators made an average of $174,000.[6]

NFTs allow a new way for creators to monetize their contributions. In the web3 world, users own their content, while allowing others to engage with or collect it. Instead of only consuming content as with the web2 space, consumers can become active participants in the career of creators, either investing in projects directly, voting on future content, or becoming collectors, making them personally invested in the success of the creator.

Blockchains allow users to hold their intellectual property through NFTs or otherwise. Instead of relying on paperwork and documents, an individual can have digital ownership or representations of

[5] "The negative consequences of advertising to children," National Financial Educators Council.

[6] Chris Dixon, Robert Hackett, and others, "Introducing the 2022 State of Crypto Report," a16z, May 2022.

ownership tied to their identity online. This system could work both in the formal and informal contexts. In relation to the formal context, NFTs would allow individuals to obtain IP rights quickly and more efficiently, while also allowing for easier tracking and transfer of ownership. In the informal context, an individual would own all his or her contributions on a platform and could take this UGC to other parts of the Internet. If an individual has the right to "pack up and leave" a social media site in web2, the company will have to continually innovate and offer incentives for the user to stay. This reallocates power from Big Tech to the users.

(2) Goals, sectors, or applications where digital assets introduce risks or harms.

While we draw attention to the significant benefits that blockchains present for both individual users and the economy, we acknowledge that there are risks associated with emerging technologies. In particular, we are mindful of the concerns voiced by regulators domestically and globally regarding the decentralized finance system.

Notably, regulators have focused on financial stability risks, as the DeFi system grows and becomes more interconnected with current, established systems. Specifically, we acknowledge concerns connected to the price volatility of digital assets held by users and the deployment of digital assets throughout the DeFi system - such that if digital assets are used as collateral or otherwise back transactions, this may amplify selling behavior and cause compounded user losses in periods of market stress.

However, DeFi systems differ from traditional financial and "CeFi" systems - centralized, financial platforms for digital assets - where intermediaries control users' assets in times of market stress. In a DeFi system, volatility may impact the assets held by users, but these users remain empowered to take control over their own holdings rather than relying on an intermediary.

(3) Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

Classifications of digital assets.

In the U.S., there has long been a debate over whether digital assets are commodities as defined by the Commodities Exchange Act, falling under the jurisdiction of the Commodities Future Trade Commission, or securities as defined by the Securities Act of 1933, falling under the jurisdiction of the Securities Exchange Commission. This divide has hindered the ability to create a thorough regulatory regime on digital assets in the United States. Therefore, we recommend for the OSTP to research classifications of digital assets across the globe to inform the U.S. approach.

Other jurisdictions have undertaken various classifications of digital assets that recognize the realities of the technology and the nuances in different types of assets:

- The European Union's Markets in Cryptoasset Regulation ("MiCA") has created a classification of digital assets as follows: "asset-referenced tokens" (a digital asset that is not an electronic money token and that purports to "maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets"); "e-money tokens" (digital assets that purport "to maintain a stable value by referencing to the value of one official currency"), and all other tokens (including utility tokens, defined as "a type of crypto-asset which is only intended to provide access to a good or a service supplied by the issuer of that token");

- The Swiss Financial Market Supervisory Authority ("FINMA") categorized digital assets based on the following breakdown[7]: "payment tokens" (tokens intended as "a means of payment for acquiring goods or services or as a means of money or value transfer"); "utility tokens" (tokens that "provide access digitally to an application or service by means of a blockchain-based infrastructure"); and "asset tokens" (tokens that represent assets like debt or equity claims on the issuer and include tokens that "enable physical assets to be traded on the blockchain").

- On February 1, 2023, the UK's HM Treasury issued a consultation and call for evidence entitled, "Future financial services regulatory regime for cryptoassets" (the "UK Consultation") in which they posit a "glossary" for various types of "cryptoassets" that expands significantly on the framework presented by MiCA and FINMA.[8] For example, the UK Consultation defines "utility tokens" as "cryptoassets which provide digital access to a specific service or application . . . and use a technology such as DLT to support the recording or storage of data"; defines NFTs as "cryptoassets which confer digital ownership rights of a unique asset (*e.g.*, a piece of digital art), using a technology such as DLT to support the recording or storage of data . . ."; and define "crypto-backed tokens" as a "subset of asset-referenced tokens which reference their value in relation to other cryptoassets." The UK Consultation glossary also includes exchange tokens, security tokens, stablecoins, commodity-linked tokens, algorithmic tokens, governance tokens and others.

MiCA, FINMA classifications, and the UK Consultation all recognize that digital assets take many forms, not all can be classified as financial instruments, and certain digital assets may have characteristics of both a financial instrument and something entirely not financial.

To build a robust and appropriately-tailored regulatory regime for digital assets, understanding the extent and ways in which digital assets function – and the ways that other jurisdictions have been classifying digital assets as they build their own legislation – will be important to ensuring the U.S. can build regulation that protects users, provides market stability, and promotes innovation.

DeFi risk mitigation.

There are significant benefits to a financial system based upon or buttressed by DeFi and its ecosystem. We understand that other responses to the RFI will address these benefits and refer the OSTP to those responses. We recognize, however, that there are risks that may arise in the DeFi system.

Financial stability risk. A number of technological solutions may be deployed to mitigate against financial stability risk, including implementing systems and controls. For example, creating a control designed to mitigate the risk of leverage and liquidity mismatches. This could include a protocol that uses indicators of available capital within a liquidity pool to calibrate liquidity risk and optimize utilization, which impact interest rates that could also be calibrated to address a variety of digital assets and their respective levels of risk. Other measures could include protocols that provide additional

[7] See "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)"

[8] See "Future financial services regulatory regime for cryptoassets: Consultation and call for evidence" at pp. 16-17.

liquidity during times of stress or volatility, create siloed assets (restriction on borrowing to isolated stablecoins), or implement caps (upper bounds for reducing exposure to certain assets).

Cyber risk. DeFi systems may face cyber risks, including economic exploits by bad actors (*e.g.*, hacks). And, because DeFi is an emerging technology, code errors and bugs may occur, posing technological risk. However, continual improvements are being made to the code underlying such systems, meaning they are becoming increasingly more secure from technological risks. The most critical tool for mitigating these risks is the creation of uniform code audit and cyber-security standards for the deployment of DeFi protocols (*i.e.*, a set of pre-deployment standards). The OSTP's research into the way code audits are conducted, how to standardize such audits, and the benefits of a disclosure regime relating to such audits will benefit the DeFi ecosystem and its users. In addition to this, the OSTP could consider how the concept of self-regulatory organizations (SROs) could fit in the context of decentralized technology. Although other jurisdictions have developed digital asset related SROs,[9] the U.S. is uniquely positioned to support and assist in developing SROs. For example, FINRA and NFA provide robust examples of SROs with regulatory authority that form a basis for standard setting regimes across the digital asset sector.

(4) R&D that should be prioritized for digital assets.

Benefits to the U.S. Economy. Blockchain increases efficiency (*i.e.*, less intermediaries, lower fees, faster processing times) and transparency (*i.e.*, information availability), which has immense potential to improve current systems, especially around record keeping and tracking in areas such as supply chains, healthcare, and government. Per PwC's estimates, by 2030, blockchain technology could boost global gross domestic product by $1.76 trillion (1.4% of global GDP), while adding 40 million jobs.[10] The U.S. would reap $407 billion of that added value. However, software developers in the blockchain technology sector have been leaving the U.S. for international jurisdictions at an increasing rate.[11] Research about the number of jobs, revenue, and economic benefit lost due to this phenomenon will be critical in assessing how to create policy that promotes innovation, protects users, and ensures market integrity.

Remittances. With decreased transaction costs and more efficient transaction processing, blockchain technology may allow for cheaper and faster remittance payments. In particular, blockchain infrastructure solutions (*i.e.*, layer 2s like the Polygon network) significantly reduce the cost of remittances and allow for even greater volume and speed of transactions. If money becomes more liquid globally, then what shifts would occur with local currencies? How will this affect the U.S. Dollar as the global reserve currency? In addition to considering those questions, there should be research on quantifying how much money could be saved in remittance payments if blockchain technology is used. If blockchains are used for remittances, then what does that system look like, and would any individual be able to access it?

Privacy. As mentioned above, blockchains are open and transparent. Further, zero-knowledge proofs - an area in which Polygon Labs has dedicated significant R&D resources - will allow people and entities to prove a specific piece of information without disclosing that information to a third party. Although this offers benefits, blockchains should not force users to expose their private information. Research efforts could concern the individual right to retain privacy on blockchains. How should

[9] For example, see Japan's Crypto Asset Trading Association, one of the country's official SROs for digital assets.

[10] "Time for trust: The trillion-dollar reasons to rethink blockchain," PwC, October 2020.

[11] See this Twitter thread by Electric Capital that produced the developer report cited in footnote three.

individuals retain privacy on transparent blockchains? Should individuals be required to be able to reveal all their information available on blockchains?

Operational Resiliency of Decentralized Finance. DeFi will have the ability to improve the operational resiliency of the financial system (assuming the risks associated with DeFi are addressed appropriately). Notwithstanding certain seismic events from centralized players in the digital asset ecosystem in the last half of 2022, DeFi protocols did not experience volatility that mirrored the shifts in the centralized system.[12] Understanding DeFi protocols from both a technical and operational standpoint will be critical in understanding the benefits of DeFi and the economic incentives and structures within these protocols. By further understanding why and how decentralized, software-based financial systems can withstand market volatility, we may be able to provide more robust underpinnings for our financial system that are not subject to failures or extreme volatility from large players in the system (*e.g.*, the 2008 financial crisis).

Conclusion

The U.S. has been and can remain a center for technological innovation, while also ensuring responsible development of blockchain-based technology. The U.S. can be well-positioned to develop an effective R&D strategy for digital assets and related technologies.

We welcome the opportunity for further discussion and engagement on these issues.

[12] Jesus Rodriguez, "DeFi is the way forward, but it needs to evolve," CoinDesk, December 2022.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

R3

R3 RESPONSE TO THE FAST TRACK ACTION COMMITTEE ON DIGITAL ASSETS RESEARCH AND DEVELOPMENT, REQUEST FOR INFORMATION

MARCH 2023

R3 welcome the opportunity to respond to the request for information by the White House Office of Science and Technology Policy (OSTP) on behalf of the Fast Track Action Committee on Digital Assets, Research and Development in contribution to these activities.

Our response contains an overview of R3, our work in central bank digital currency (CBDC) and our offer of support to the activities of the United States as it explores the utility of digital assets. The contents of this submission are a compliment to the evidence presented by Richard Gendal Brown, Chief Technology Officer and Jack Fletcher, Government Relations Manager (Digital Currencies) to the Technical Sub-Committee during a session held on Friday February 17.

Introducing R3

R3 is an enterprise software firm enabling digital transformation through our trust technology, connected networks, and regulated markets expertise. R3's Corda is the world's leading distributed application platform trusted by regulated institutions to connect networks, automate complex business processes, streamline workflows, drive faster settlement, and manage digital assets and currencies. Battle-tested by regulated networks operating at scale, Corda delivers a permissioned, smart contract-enabled ledger.

To ensure our customers derive the greatest value from our products, we provide services to shorten time-to-market, as well as guidance on implementation, integration and developing ecosystems on our platforms. Our customers and partners also have access to a network of leading systems integrators, cloud providers, technology firms, software vendors, corporates, and banks.

Learn more at r3.com, and corda.net

R3 is headquartered in New York, and has offices in London, Singapore, Dublin, India, and São Paulo.

Our Work in CBDC

R3 Corda has been used in world leading CBDC projects. These include projects conducted by: the Banque de France, Swiss National Bank, and Bank of International Settlements (BIS) in Project Jura; the Monetary Authority of Singapore, South African Reserve Bank, Bank Negara, Reserve Bank of Australia, and BIS in Project Dunbar; the Swedish Riksbank in their retail eKrona project, and in Project Icebreaker; South African Reserve Bank in Project Kholka; and Swiss National Bank and BIS in Project Helvetia; and the Central Bank of Kazakhstan in their Digital Tenge retail CBDC project. Corda has also been used in Project Jasper (Canada); Project Ubin (Singapore); Project Inthanon (Thailand), and by the European Central Bank in the Eurochain project and in Project Stella (in coordination with the Bank of Japan).

Our involvement in these activities has enabled R3 to establish world-leading technical expertise in CBDC. We have used this to support innovative projects across the world, raise the bar of thought leadership on digital currencies and increase understanding of CBDC within the both the public and private sector. In 2021, we ran a CBDC Working Group, with participants from over 140 entities from across the public and private sector. The findings of our Working Group, and expertise developed from our participation in CBDC projects, resulted in the design and functionality of our CBDC sandbox. The sandbox allows users to quickly establish a virtual environment for experimenting with CBDC, guiding them through the lifecycle of a token from issuance to redemption using a two-tier distribution model. It also provides the tools for the implementation of policy decisions through programmability.

Supporting the work of the United States

We believe that the development of CBDC should not a technology led exercise, but that technology solutions should be built to implement a policy led design. As such, we believe that our role in CBDC development is to illustrate and demonstrate what is possible through technology and work with stakeholders to implement a solution designed around their requirements. As our body of work indicates, Corda has established itself as the platform of choice for CBDC work across wholesale, retail, domestic and cross-border activities. We stand ready to support the work of the United States in developing its stance on CBDC.

If you have any questions relating to our submission, please contact Jack Fletcher, Government Relations Manager (Digital Currencies) [redacted]

CBDC Landscape and Motivations for Issuance

We view retail CBDC as a payment settlement medium issued by a central bank, which operates alongside cash in the retail payments landscape. CBDC would therefore become the third type of M0, alongside cash and central bank reserves. Motivations for the development of CBDC vary globally and typically reflect a response to a specific issue or collection of issues in the payments landscape, be they domestic, cross-border, wholesale, or retail. Common motivations also encompass macro-economic and geopolitical factors, along with pro-innovation policy initiatives. With respect to retail CBDC, seeking a digital replacement for cash is also high on the agenda and an area that this response will focus on with respect to privacy.

In pursuit of cash-like CBDC

Cash is arguably one of the world's most successful products. Whilst CBDC should be considered a compliment to cash in the near-medium term, it might be wise in the design of CBDC to consider which properties of cash it might (or might not) incorporate, should it establish itself as the long-term successor. Cash has unique properties as a settlement medium which no digital offering can currently provide. Those include:

- Anonymity: the respective identities of payee and payer are not required to initiate or settle a transaction
- Censorship resistant: there is no third-party dependency in the settlement of a transaction or third-party visibility in a transaction
- Confiscation resistant: holders can only be parted from their cash via a physical interaction
- Universally available: there is no barrier to holding cash, thereby providing broad financial inclusion
- Offline functionality: transactions can be settled without digital connectivity
- Bearer-instrument with settlement finality: transactions are final and instant
- Symmetric settlement instrument: it is as easy to pay as to be paid

When we consider the potential for cash-like CBDC, it feels necessary to examine these characteristics and explore whether they can be technically implemented into a potential CBDC design. Where conflicts appear between the characteristic being implemented in a digital solution and existing legislation, it is our role to support policy makers in highlighting the *extent* to which a specific feature can be replicated and report the trade-offs this might entail. For instance, were absolute universality a core of requirement for CBDC, it would be highly challenging (if not impossible) for every citizen to meet the threshold requirements to satisfy current AML/KYC compliance requirements for electronic transfers. It is not for technology vendors to determine the path forward in such an example but to illustrate the possible technical pathways in support of the policymakers work in determining which of the conflicted sides needs to accommodate the other.

A benchmark for privacy

When we consider the matter of privacy, we consider it in two regards: 1) privacy *of what,* and; 2) privacy *from whom*. When considering the privacy *of what* it is useful to consider the assets themselves and the transaction details as two components that might contain data that should be access restricted. When considering the *from whom* our consideration should extend to the network operator and issuer, the transaction counterparties, and network participants at large. In our current payment landscape, digital payments and cash payments provide deep contrasts in both respects.

If we are seeking to build a cash-like CBDC we must acknowledge that cash's benchmark for privacy is higher than that provided by current digital payments. Cash's privacy standard is not that the operator *will not* reveal the identity of the payer but *cannot* reveal the identity of the payer. It may well be that this standard is deemed inappropriate for digital payments at large, but we might choose to consider whether we allow such freedoms with limitations – such as holding caps. This is undoubtedly a point of social and political consideration that should be explored by the United States, as it has been in jurisdictions overseen by the European Central Bank and the Bank of England. With physical cash, there is a practical self-limitation to its use (you can only carry/store so much of it) and this reduces the risk that the freedoms of cash might be unacceptably abused. In the design of CBDC, we could implement technical constraints on holdings to replicate this practical consideration of cash and integrate it with sybil resistance techniques to prevent one individual from holding multiple wallets and circumventing those constraints. We would be happy to discuss this further.

Censorship Resistance

A noted political consideration in the development of retail CBDC, has been the concern by some lawmakers that transactions must be free from the potential of state surveillance. Were such a design requirement be adopted for a US retail CBDC, we must accept that it's delivery points towards a solution that emphasizes one of the key features of physical cash – that of censorship resistance. By extension of the argument, we should also acknowledge that it also champions the freedom for us as citizens to buy something that society might not approve of. This presents one of the first challenges for such a design requirement and arguably the more difficult end of the requirement to publicly justify.

We will discuss how such a design might be achieved in the next section, but it is relevant to state here that establishing confidence in that solution across a potentially sceptical public is not trivial. The path towards civil confidence and understanding in this feature is likely to require demonstration and attestation from trusted entities to assure the public that their payment activity was free from observation and censorship. In this sense, there may well be a strong role for the state to play in convening suitable parties to review solutions.

Advanced Privacy Techniques

We welcome the recent announcement by the National Science Foundation of its multi-million dollar funding of the Center for Distributed Confidential Computing. We believe that confidential computing is a vital component of digital solutions that unlock digital innovation whilst preserving privacy.

Corda is a private-permissioned platform that shares data on a need-to-know basis by default. In the design of a CBDC using DLT infrastructure, we have several techniques for providing transaction privacy, including confidential identities, public key rotation, chain-snipping, and burn and reissuance. We discuss some of these techniques in more detail in this externally published blog.

A core issue faced by all IT solutions, however, is that we must design solutions to reflect that it is not possible to trust another actor's computer. We must therefore put in place steps to satisfy that a given digital asset is what it claims to be. In CBDC, this requires the holder of a claimed US retail CBDC token to prove that the token is truly a liability of the US Fed. In token-based distribution systems, this validation is done based on the token's provenance. An inspection of the chain of historic transactions attached to a token ultimately reveals its issuer, the Fed. Such an examination, however, can also expose sensitive data to the inspecting entity, like general transaction behaviour in the system or hashes of information with the potential to be linked back to a real-life entity. The solution lies in techniques that can provide the attestation and assurance that the CBDC really is a liability of the US Fed, without exposing sensitive data to anyone.

We believe that there are several potential techniques for solving this problem. There are software techniques: zero knowledge proofs, fully homomorphic encryption, and secure multi-party computation; and hardware techniques: special purpose secure enclaves, and general-purpose trusted execution environments. In our view, research and development in these areas could lead to significant leaps in the implementation of solution with the United States uniquely placed, certainly in respect to hardware solutions, to capitalise on the work of its domestic industrial and academic research base. In respect to CBDC, we believe that we were work undertaken to advance the security of general-purpose trusted execution environments, it would unlock privacy preserving services for implementation within a cash-like privacy CBDC design and deliver a potentially compelling product offering.

Concluding remarks

We believe that it is important to consider a retail CBDC offering as a product seeking market adoption in a competitive domestic market. It is therefore important for the designers of such an offering to consider which attractive features it might have that make it distinct from other products available to consumers, and how American values and standards should be reflected in a retail CBDC offering.

R3 has proven world-leading credentials in CBDC and we stand ready to support our home nation in the United States in the development of its analysis and formulation of its plan ahead on the subject of digital currencies.

-ENDS-

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

R3 Research

CBDC and Digital Assets: Open Research Questions

FTAC-DARD Tech Group

Richard G Brown, February 2023

Chief Technology Officer, R3

Introduction

ABOUT US

We exist to enable an open, trusted and enduring digital economy •

R3 is leading the future of digital finance by powering multi-party solutions that deliver digital trust and unlock greater potential for regulated businesses everywhere.

R3's CBDC Central Bank Projects

- **Jasper** (Bank of Canada – 2016+)
- **Ubin** (Monetary Authority of Singapore – 2017+)
- **Inthanon** (Bank of Thailand – 2018+)
- **LionRock** (Hong Kong Monetary Authority – 2019+)
- **Stella** (ECB and Bank of Japan – 2019)
- **E-Krona** (Sveriges Riksbank [Sweden] – 2020+)
- **Banque de France** (2020+)
- **Project Khokha** (South African Reserve Bank – 2020+)
- **Project Helvetia** (Swiss National Bank; BIS – 2020+)
- **Project Jura** (Banque de France, Swiss National Bank, BIS, SIX – 2020+)
- **Project Dunbar** (Monetary Authority of Singapore; Bank Negara; Reserve Bank of Australia; South African Reserve Bank; BIS - 2021+)
- **Project eTenge** (Central Bank of Kazakhstan – 2021+)

r3.

Agenda

- Introduction
- Open Questions With Concrete Actions
  - CBDC: Resolving the Privacy and Oversight Tension
  - Advanced Privacy Techniques: Unhelpful incentives?
  - The Role of Standards

CBDC Roadblock: Privacy with Control

Rep. Tom Emmer Says Fed Must Not Create Digital Currency 'Surveillance State'

Emmer has introduced legislation that seeks to limit the Fed's ability to issue a digital currency without additional oversight.

https://www.wsj.com › articles › surveillance-risks-shape-...

Surveillance Risks Shape How Central Banks T

22 Mar 2022 — Dozens of governments are exploring whether digi
central banks can bring benefits without the instability of ...

https://cointelegraph.com › news › uk-think-tank-launc...

UK think tank launches a crusade against 'surveillance' CBDCs

14 Feb 2023 — The Tax Reform Council believes implementing a **CBDC** would lead to increased government **surveillance**, greater intrusion from tax authorities and ...

UnHerd

The tyranny of digital currencies

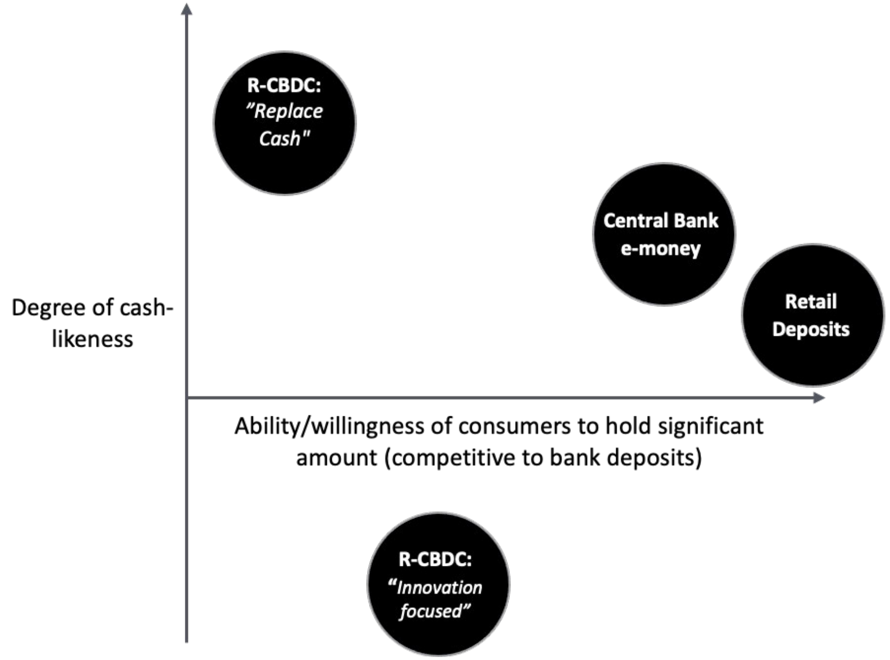
Where a CBDC would change things, however, is that the digital ... CBDCs, after all, would give governments sweeping powers of surveillance...

1 week ago

Reverse-engineering the requirements for privacy and identity

To what question might a retail CBDC be the answer?

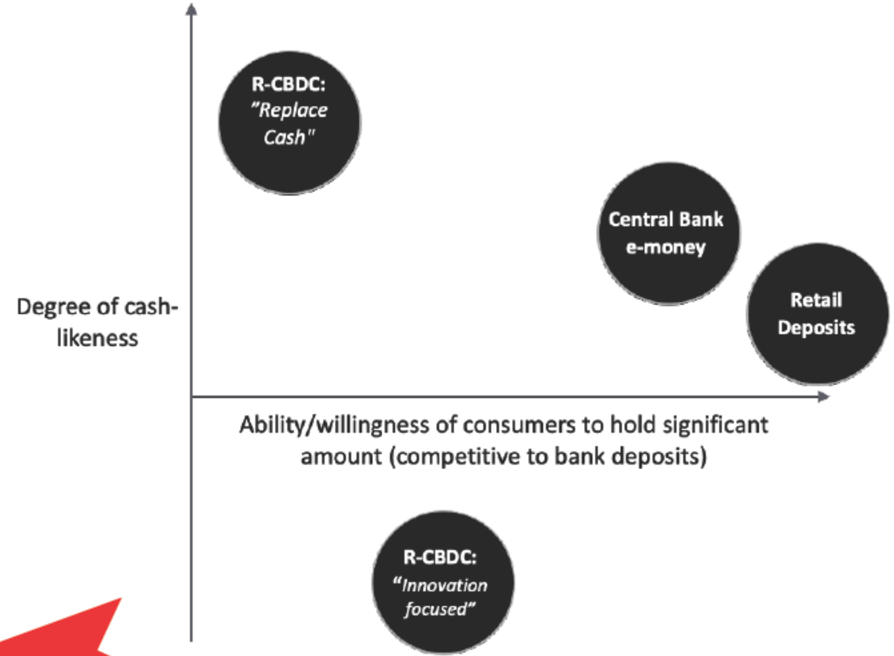
- “Promote Innovation”?
  - Access, Programmability, APIs, etc
- “Monetary Sovereignty”?
- “Democratise Payments”?
  - Make it as easy to be paid as it is to pay?
  - Point-of-Sale transformation?
- “Provide a digital replacement for physical cash”?
- Other?



Reverse-engineering the requirements for privacy and identity

To what question might a retail CBDC be the answer?

- “Promote Innovation”?
  - Access, Programmability, APIs, etc
- “Monetary Sovereignty”?
- “Democratise Payments”?
  - Make it as easy to be paid as it is to pay?
  - Point-of-Sale transformation?
- “Provide a digital replacement for physical cash”?
- Other?



This leads to hard questions so let’s start here and see where it takes us…

r3.

Can we foresee the “architecturally significant” requirements of a true ‘cash-like’ CBDC, were that to be the objective?

- Privacy?
- Censorship-resistance?
- Confiscation-resistance?
- Universally inclusive?
- Offline support?
- No recourse / finality?
- Symmetric payer-versus-payee?

Privacy

- **Question:** Privacy of *what* from *whom*? *Let's focus here on "what = who made a payment"*
- **Table stakes:** "I can make a payment without vendor learning who I am"
  - Payment cards provide this so it's a reasonable starting point
- **But what about:** "There are some payments for which the 'operator' will not learn or reveal the payer"
  - Absent a warrant? If that's the bar, no advanced technology required to meet this requirement. But that's not really a true equivalent to physical cash…
- **What about:** "There are some payments for which the state ***can not*** learn the payer"
  - Implication: privacy-enabled wallets become *highly* desirable to 'bad' people so we need some notion of 'limits'
    - Cash gets more inconvenient the more you hold. What is a digital analog?
  - How do you stop one person creating multiple wallets if you don't know who they are?
    - Can we design a solution where one human can only possess ~1 wallet? ("anti-sybil")?
    - Can we do it in a way that is inclusive?
    - Can we do it in a way that a paranoid citizen would *believe?*

Remember: cash is censorship-resistant; this is not just about privacy
"I can pay for things that society may not approve of"

- **Assumption:** Society will not permit this without *limits (if at all)*
- **Implication:** Limits on: wallet size; transaction size; tx count; tx type?
- **Requirement:** Sybil resistance
  - "Proof of unique human"
  - Note: limited censorship resistance alone does not imply a need for *identity**
    - (ie anonymity is not precluded by the need for limits)

** I use 'identity' deliberately loosely to capture the notion that **some** actor knows with **some** degree of confidence **who** controls a wallet*

Open Question #1

How do you design a *credibly private*, *quasi-censorship-resistant* CBDC which facilitates no more crime than physical cash?

Advanced privacy techniques

Depressing fact of life:
You can't trust somebody else's computer

Data sharing is risky

A control is only as strong as your trust in the party implementing it

If you could trust somebody else's computer, so many 'multi-party' problems would be SO MUCH easier!

Software Techniques	Hardware Techniques
Zero Knowledge Proofs	Special Purpose Secure Enclaves
Fully Homomorphic Encryption	General Purpose Trusted Execution Environments
Secure Multi-Party Computation	

Software Techniques	Hardware Techniques
Zero Knowledge Proofs	Special Purpose Secure Enclaves
Fully Homomorphic Encryption	General Purpose Trusted Execution Environments
Secure Multi-Party Computation	
Academia-led	Industry-led

Open Question #2

- If General Purpose Trusted Execution Environments could be made sufficiently secure, and if it were generally *accepted* that they were sufficiently secure, we could see a step-change in adoption of privacy-preserving services and an entire class of 'hard problems' would become 'easy problems'
- **The United States has a (near) monopoly on TEE capabilities (Intel SGX, AMD SEV)**
- What would an academia/government/research-led programme focused on validating and improving TEE tech, with a mandate to drive adoption, look like?

Interoperability Standards

OCTO-053 Interoperability Landscape for Atomic Swaps on Permissioned DLTs

Created by Richard Brown
Last updated: Jan 30, 2023 • 17 min read • 38 people viewed

Introduction

2022 witnessed a surge of interest in techniques for connecting d
industry has long known that interoperability between DLT-based
different technologies, would be necessary but it was only in 2022
on multiple platforms, that the question moved from the theoretic

The specific interoperability requirement we hear most often is th
between parties on one network if and only if another asset is tra
direction on another network. This requirement is often described
(sometimes 'Payment versus Payment' when both assets are c
...metimes also hear a requirement to 'move' or '

Contents

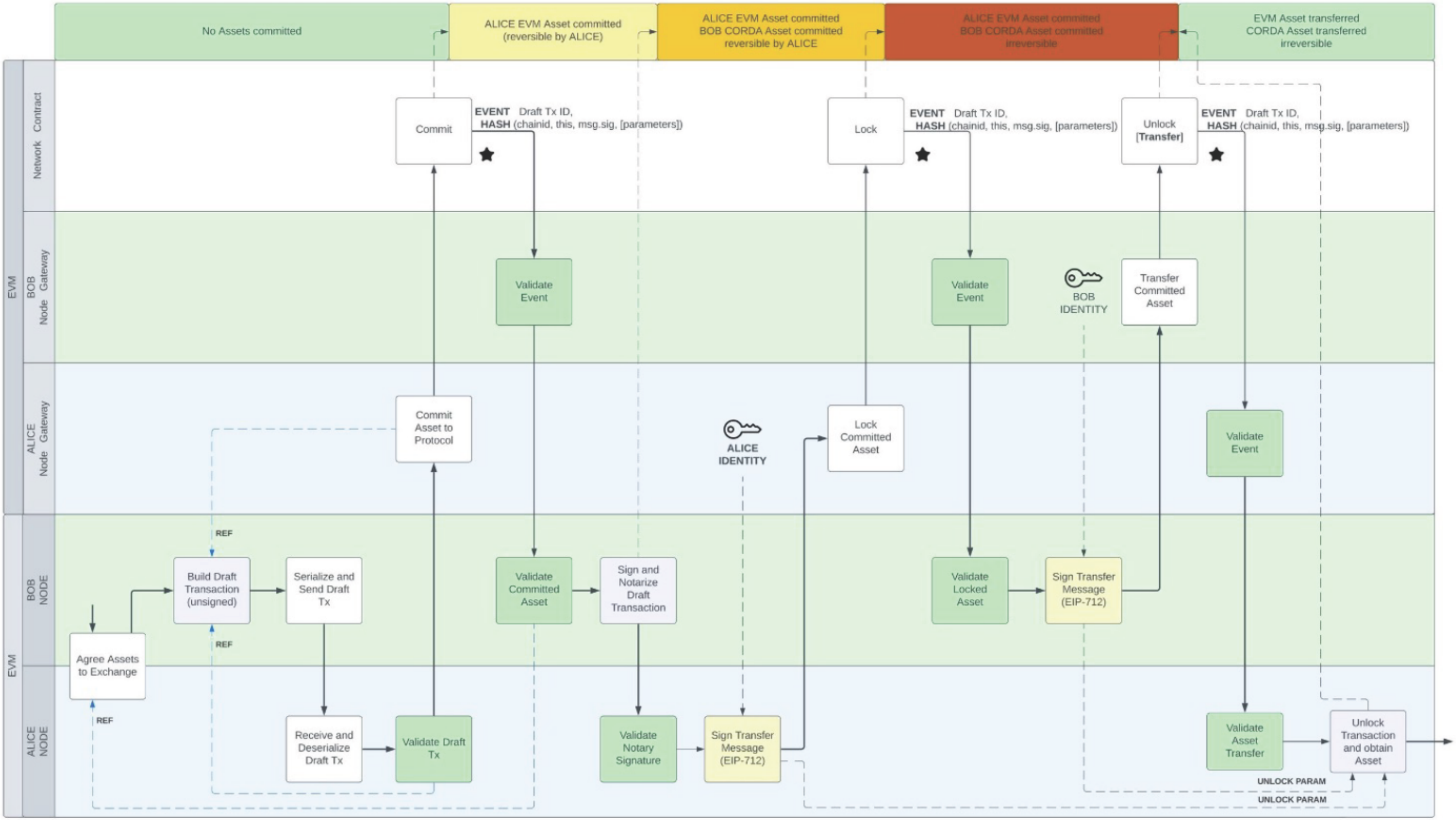
Fnality and HQLAX run PoC of cross-chain repo swap settlement

05 December 2022 0 0 0

Source: Fnality

Fnality and HQLAX announce the successful completion of the first proof of concept (PoC) delivery versus payment (DvP) repo settlement across the Fnality Payment System (FnPS) and HQLAX's Digital Collateral Registry, bridging the distributed ledger technologies (DLT) of Enterprise Ethereum and R3 Corda, respectively.

The proof of concept was support...
...nco Santander, Goldman S...


No Assets committed
ALICE EVM Asset committed (reversible by ALICE)
ALICE EVM Asset committed BOB CORDA Asset committed reversible by ALICE
ALICE EVM Asset committed BOB CORDA Asset committed irreversible
EVM Asset transferred CORDA Asset transferred irreversible
EVM
Network Contract
BOB Node Gateway
ALICE Node Gateway
EVM
BOB NODE
ALICE NODE
Commit
EVENT Draft Tx ID,
HASH (chainid, this, msg.sig, [parameters])
Lock
EVENT Draft Tx ID,
HASH (chainid, this, msg.sig, [parameters])
Unlock [Transfer]
EVENT Draft Tx ID,
HASH (chainid, this, msg.sig, [parameters])
Validate Event
Validate Event
BOB IDENTITY
Transfer Committed Asset
Commit Asset to Protocol
ALICE IDENTITY
Lock Committed Asset
Validate Event
REF
Build Draft Transaction (unsigned)
Serialize and Send Draft Tx
Validate Committed Asset
Sign and Notarize Draft Transaction
Validate Locked Asset
Sign Transfer Message (EIP-712)
REF
Agree Assets to Exchange
REF
Receive and Deserialize Draft Tx
Validate Draft Tx
Validate Notary Signature
Sign Transfer Message (EIP-712)
Validate Asset Transfer
Unlock Transaction and obtain Asset
UNLOCK PARAM
UNLOCK PARAM

Open Question #3

- What happens if the blockchain interoperability protocols designed for public chains turn out to be ill-suited for corporate/enterprise usage? How do we ensure there is academic/theoretical rigor to underpin the custom/bespoke protocols being developed by clients or for client engagements in the regulated space?

- Threat models
- Conceptual correctness
- Communicating and validating trust assumptions

Thank you

www.r3.com | corda.net

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Rather Labs

Office of Science and Technology Policy (OSTP)

Request for Information; Digital Assets Research and Development

Rather Labs

Contents

From:

Rather Labs
RFI #: 2023-01534
Respondent type: Private Industry
[redacted]

RATHER LABS

March 2, 2023
Via Electronic Mail Only: DARD-FTAC-RFI@nitrd.gov
Dr. Arati Prabhakar, Director of the Office of Science and Technology Policy (OSTP)

Attn: Digital Assets R&D RFI

Dear Dr. Prabhakar,

Rather Labs appreciates the opportunity to respond to the Request for Information from the The White House Office of Science and Technology Policy (OSTP), and actions related to strengthening community health through digital health technologies. Rather Labs is a global blockchain tech hub, whose elite team of engineers makes new ecosystems come to life: helping more than 30 founders & startups, and enterprises design, build and launch Web3 products. Rather Labs brings the solution for tech startups that want to create their MVPs from scratch, raise investment and scale their products.

We appreciate this opportunity to bring to your attention issues of great importance to the United States and world. If you have any questions, please contact me, Federico Caccia, at [redacted]

Sincerely yours,

[redacted]

Federico Caccia, CEO at Rather Labs

1. Opportunity to decrease Tax Evasion through CBDC and Blockchain Technology

Tax collections through CBDC with economic incentives for its use is a possibility that not only decreases tax evasion but also provides more transparency to the system by registering all transactions in the Blockchain with the possibility of automation through Smart Contracts.

By leveraging the unique features of CBDCs coupled with economic incentives for their use, taxpayers can be incentivized to comply with tax regulations.

Government Blockchain: Tax and Royalties Payment with CBDC

The implementation of Blockchain technology has the potential to revolutionize the relationship between Government, Enterprises, and Citizens. The development of a collaborative Blockchain infrastructure that enables the tracking and processing of CBDC payments for taxes or royalties through Smart Contracts, presents an opportunity to streamline financial transactions while incentivizing adoption.

All tax transactions can be recorded in a secure and immutable ledger, ensuring that every transaction is transparent and tamper-proof. This not only enhances the efficiency of the tax collection process but also provides a greater level of accountability and trust within the system.

Furthermore, using Smart Contracts can enable the automation of tax payments and ensure that all obligations are met in a timely and accurate manner. This can help to reduce administrative costs and increase compliance while decreasing the potential for human error or fraudulent activity. Additionally, by offering discounts or other economic incentives for using CBDCs to make payments, the Government can encourage greater adoption of this innovative payment system.

The transition from physical assets to digital assets presents a unique set of challenges that require careful consideration to ensure the successful implementation and adoption of this innovative payment system. To achieve this, a modular, flexible, and scalable payment technology capable of supporting a simple and user-friendly mode of operation must be developed.

One of the key considerations in the development of CBDCs is the need to strike a balance between control and privacy. While digital assets offer a high degree of control and transparency for governments and financial institutions, they can also raise concerns about individual privacy and data protection. It is essential to establish a framework that addresses these concerns while still providing the necessary controls and oversight to ensure the integrity of the payment system.

Another critical factor to consider is the need to incentivize adoption. Unlike physical assets, digital assets are a new and unfamiliar concept for many individuals and businesses. Therefore, it is essential to provide a simple and usable mode of operation that is easy to understand and accessible to all. By providing a seamless user experience and offering economic incentives, such as discounts or loyalty programs, the adoption of CBDCs can be accelerated, leading to greater efficiency and security in financial transactions.

Furthermore, the scalability of the payment technology must be considered to accommodate the anticipated increase in demand for digital payment systems. As more individuals and businesses adopt CBDCs, the payment infrastructure must be able to handle large volumes of transactions in real time. Developing a scalable and modular payment system will ensure the payment infrastructure can adapt to changing needs and demands.

Connect to Blockchain Production Mesure Equipment.

By integrating CBDCs with Blockchain production measurement equipment, it is possible to accurately measure the production of goods and estimate the royalties payable in real-time. This enhances transparency and efficiency in the collection of royalties while providing real-time data for both the government and relevant parties.

Automatizate Payments through Smart Contracts and IoT

The automation of payments through Smart Contracts and the Internet of Things (IoT) can streamline royalty payments, reduce administrative overheads and errors, and ensure prompt payment to the appropriate parties. By creating events that trigger payments through Smart Contracts, the payment process can be fully automated eliminating the need for manual intervention, thereby reducing the likelihood of errors, and providing a high level of auditability. Additionally, by auditing productions, it is possible to ensure that royalty payments are accurate and comply with regulations.

Incentivize Royalty and Tax Payments through CBDC

One potential approach is to offer discounts to industries that use CBDC to pay royalties. This can serve as a specific way to empower CBDC usage and promote adoption, especially for industries that may be initially hesitant to use this alternative payment method.

To ensure transparency and accountability, all payments made using CBDC would be registered in the blockchain. This allows for real-time auditing and monitoring, ensuring that all transactions are recorded and can be traced back to their source.

In addition, it is also possible to integrate this technology with other relevant tax data. By digitizing paper-based documentation into non-fungible tokens (NFTs), it is possible to streamline the tax payment process and make it more efficient. This can help to reduce paperwork and improve accuracy in tax record keeping.

Citizens can also be integrated into the blockchain to pay their taxes using CBDC. Similar to the incentive for industries, citizens could receive a direct discount for using CBDC to pay their taxes. To ensure the privacy and security of citizen tax data, this information could be encrypted and integrated into the blockchain system.

The adoption of CBDC can help to fight fraud by moving tax payments closer to digital transactions. It is important that blockchain solutions be compatible with the accounting and computer systems used by taxpayers to ensure seamless integration and minimize potential errors or complications in the payment process.

2. Toxic waste traceability with Blockchain

As we continue to grapple with the environmental impacts of waste disposal, it has become increasingly clear that effective waste management demands a comprehensive approach that accounts for the entire lifecycle of waste. One crucial aspect of this approach is traceability, which involves the tracking of waste from its generation to its final destination, whether that be reuse, recycling, or recovery. Moreover, data tracking is essential for ensuring compliance with existing laws and policies governing waste management, as well as for incentivizing the development of new regulations and policies that prioritize waste reduction, prevention, and diversion away from landfilling or incineration.

Against this backdrop, we propose the integration of blockchain technology into waste traceability systems. Blockchain's unique features, including its decentralized, tamper-proof ledger and its ability to provide secure, transparent, and immutable data storage and transfer, make it an ideal solution for addressing many of the challenges facing waste traceability today. With blockchain, we can create a system that is resistant to fraud, resistant to tampering, and provides a complete, real-time record of waste movement and disposal. By doing so, we can enhance accountability, transparency, and trust among all stakeholders in the waste management ecosystem, including businesses, government agencies, and the public.

We believe that incorporating blockchain technology into waste traceability systems will not only help us better manage our waste but also pave the way for a more sustainable, circular economy. By enabling the efficient tracking and reuse of waste, we can reduce the environmental impact of waste disposal, conserve natural resources, and create new economic opportunities.

Create a Green Blockchain with the main objective of tracking toxic waste.

The creation of a Green Blockchain with the primary objective of tracking toxic waste. Such a blockchain system can leverage the immutability and transparency of Blockchain technology to create a shared ledger database that automatically registers and tracks toxic waste using GPS and proof of view.

To ensure compliance with regulations and encourage responsible behavior, an automatic penalty fee charged in CBDC can be implemented through a Smart Contract. The Smart Contract can be designed to enforce penalties based on predefined criteria, such as a time deadline penalty or location penalty. For example, if a shipment of toxic waste is not delivered within the stipulated time or is found in a location where it is not authorized, a penalty fee can be automatically charged in CBDC, providing an incentive for compliance and responsible behavior.

Moreover, the public registry of activity regarding toxic waste transportation can be maintained and made available to the public to expose polluters. This registry will provide an audit trail of all toxic waste transportation activities, including the responsible parties involved, the quantity of waste transported, and the location of the waste. This will ensure accountability and encourage responsible behavior, thereby promoting a cleaner environment.

- **Traceability:** Blockchain can provide an immutable and transparent record of every transaction in the waste management process. This means that all parties involved in the handling of toxic waste can be held accountable for their actions, and any unauthorized or illegal activity can be quickly identified and addressed.

- **Supply chain management:** Blockchain can be used to track the movement of toxic waste from its source to its final destination. This can help to ensure that the waste is handled safely and responsibly at every stage of the process and that all regulatory requirements are met.

- **Smart contracts:** Smart contracts can automate the process of toxic waste management by enforcing predetermined rules and conditions. For example, a smart contract could automatically trigger the release of funds once a certain amount of toxic waste has been safely disposed of.

- **Tokenization:** Tokenization is the process of creating digital tokens that represent physical assets. This can be applied to toxic waste, where each token represents a specific quantity and type of waste. These tokens can then be traded on a blockchain-based marketplace, allowing waste generators and handlers to buy and sell waste in a transparent and secure manner.

- **Incentivization:** Blockchain can be used to incentivize responsible behavior in the handling of toxic waste. For example, waste handlers could be rewarded with tokens for meeting or exceeding regulatory standards, while waste generators could be penalized for not properly managing their waste.

Overall, blockchain technology has the potential to greatly improve the safety, efficiency, and transparency of the toxic waste management process. However, its adoption will depend on regulatory and industry support, as well as the development of user-friendly blockchain-based platforms and applications.

References

- National Institute of Standards and Technology
- World Economic Forum
- Blockchain Research Institute

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Rethinc. Labs

Over the past four years, Rethinc. Labs, an initiative of the Kenan Institute of Private Enterprise at the Kenan-Flagler Business School at the University of North Carolina at Chapel Hill, has been engaged in research and development, teaching and engagements with entrepreneurs and government pertaining to several of the goals laid out in this request for information-

1. *Goals, sectors, or applications where digital assets introduces risks or harms*
2. *Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets*
3. *Opportunities to advance responsible innovation in the broader digital assets ecosystem.*

In what follows is a summary of our efforts in these areas.

Curriculum

New educational initiatives at both the undergraduate and MBA levels were implemented at the Kenan-Flagler Business school at UNC Chapel Hill during the 2019-2020 academic year. Two new undergraduate classes were offered—the first was delivered jointly with UNC's computer science department on data science, and the second covered blockchain technology and current cryptocurrency markets. The MBA fintech course that first premiered in 2019 was redesigned by new faculty member Donghwa Shin.

The first new undergraduate course, "Introduction to Fintech: Blockchain Technologies and Cryptocurrencies," was designed to introduce the recent advances in blockchain technologies and cryptocurrencies to senior undergraduate students. This course is being taught by Donghwa Shin. Starting with the mechanics of Bitcoin and blockchain, the course broadly covers Bitcoin mining, Ethereum and smart contracts, initial coin offerings, security versus utility tokens, market manipulations, and stablecoins. More specific topics such as Ripple (XRP) and IBM blockchains were covered in group presentations, where students conducted in-depth analyses based on the techniques they learned in the course.

Research

A new research project led by Eric Ghysels (UNC-Chapel Hill), Giang Nguyen (Penn State), Donghwa Shin (UNC-Chapel Hill), and Zhe Wang (postdoc UNC-Chapel Hill) uses textual analysis of cryptocurrency blogs to study their impact on Bitcoin. The purpose of this research is to study the impact of social media on cryptocurrency price dynamics. There is no observable fundamental information to help understand the valuation and pricing of Bitcoin. A common belief is that the value of Bitcoin is dependent on market sentiment and risk factors that are pertinent to cryptocurrencies (such as hacking, theft, and regulatory constraints). However, measuring market sentiment is not a trivial undertaking. The research team is overcoming this challenge by employing a new machine learning technique to perform textual analysis of the blog forum initially created by Satoshi Nakamoto. With this technique, the team can capture the sentiment and information content of blog posts and differentiate bloggers by their insights. They then study how the online activities of different bloggers affect Bitcoin returns. Their methodology helps shed light on the heterogeneity of beliefs and insights among bloggers and its implications on Bitcoin pricing. The paper "**The Wisdom of Crowds in FinTech: Evidence from Initial Coin Offerings" was published at Review of Corporate Finance Studies** and was selected as an Editor's Choice.

Another research project, which resulted in the paper, "**Longand Short-term Cryptocurrency Volatility Components: AGARCH-MIDAS Analysis," by Christian Conrad (Heidelberg University), Anessa Custovic (UNC-Chapel Hill), and Eric Ghysels**, received the 2019 *Journal of Risk and Financial Management* Best Paper Award. Custovic and Ghysels also started a new joint project with Amin Shams (Ohio State University) on long- and short-term components of cryptocurrency co-movements. This new research is an extension of the earlier work, focusing on the sources of correlation instead of volatility.

Donghwa Shin recently completed the project, **"The impact of derivatives on cash markets: Evidence from the introduction of bitcoin futures contracts," jointly with Patrick Augustin (McGill University) and Alexey Rubtsov (Global Risk Institute).** In this study, the authors exploit a unique feature of cryptocurrency markets to provide new evidence on how derivatives affect cash markets. In December 2017, the CME and the CBOE both introduced futures contracts on Bitcoin (BTC) against the U.S. dollar (USD), but not on any other cryptocurrency exchange rate pairs.
Because identical cryptocurrencies trade on multiple exchanges, the researchers were able to examine how the introduction of Bitcoin futures changed various attributes of BTC-USD relative to other cryptocurrency pairs, keeping exchange characteristics constant. Following the futures introduction, the authors observe a significant increase in cross-exchange BTC-USD price synchronicity relative to other exchange rate pairs, as demonstrated by an increase in price correlations and a reduction in arbitrage opportunities.

The authors also find evidence in support of an increase in market efficiency, market quality, liquidity, and market stability. In the most conservative specification, the authors control any unobservable time-varying exchange specific factors find that the effects stay statistically and economically significant. Multiple subsequent analyses make the results more appealing. The effects are more pronounced at around the settlement time of the Bitcoin futures. The authors find no effects of the introduction of the Bitcoin futures in other cryptocurrencies like Ethereum. Overall, the results support the view that the BTC-USD futures was beneficial to the Bitcoin cash market by marking the underlying prices more informative. This research sheds light on the current debates on the introduction of cryptocurrency investment vehicles including cryptocurrency ETFs and Ethereum futures, and therefore provides an important policy implication. In addition to this project, Shin is also working on a project on DeFi (Decentralized Finance).

Dongwha Shin studied the impact of news on cryptocurrency markets around the world. While a large body of literature documents the impact of macroeconomic news on financial markets, far less is known about the impact of news on the cryptocurrency market. We use a unique and comprehensive data set to study the impact of news on different cryptocurrency markets located in Asia, Europe and North America. We found that: (1) the price of cryptocurrency is highly correlated across exchanges, so the same news triggers the same price responses on different exchanges; and (2) trading activities are exchange-specific, so the same news triggers quite different trading activities in different exchanges. The empirical setting in this project is unique: geographically segregated investors with different cultures and languages are trading one same asset on sparse exchanges. This is very unique from our traditional financial markets where people trade the same assets in the same exchanges. Due to this, our studies will not only improve our understanding of newly emerged cryptocurrency markets, but also has the potential to answer some of the economic questions that are not easy to study in traditional financial markets. This project was co-authored by Lucia Alessi (European Commission), Marco Petracco (European Commission) and Zhe Wang (UNC Chapel Hill).

Donghwa Shin's current research seeks to characterize the risk and return characteristics of yield farming investment strategies on PancakeSwap, one of the largest automated market makers among the emerging ecosystem of decentralized financial services. PancakeSwap provides opportunities for earning passive income by pledging pairs of cryptocurrency tokens in liquidity pools and harvesting governance tokens in yield farms, a practice called `yield farming.' Yield farming generates performance through several components related to capital gains, trading fee revenue and farm yields, and is exposed to impermanent losses that are driven non-linearly by differential return performance in the underlying cryptocurrency token pairs. Findings show that yield farming delivers positive Sharpe ratios that are comparable to those of other cryptocurrency investments and the S&P500 index. However, investment performance declines significantly after accounting for transaction costs and price impact that is largest for farms with the highest headline yields, leading possibly to negative risk-adjusted returns. Evidence shows that flows to high-yield farms chase past performance and high yields and predict negative future returns. These patterns are similar to investment behaviors and risk return characteristics observed in traditional markets, despite the absence of financial intermediaries. Since yield farming is easily accessible to retail investors, our analysis has important implications for the current debate about the regulation of decentralized financial services.

PhD student Kim Chan's project, Periodicity in Cryptocurrency Volatility and Liquidity, Chan examines recurrent patterns in volatility and volume for major cryptocurrencies, Bitcoin and Ether, using data from two centralized exchanges (Coinbase Pro and Binance) and a decentralized exchange (Uniswap V2). He finds systematic patterns in both volatility and volume across day-of-the-week, hour-of-the-day, and within the hour. These patterns have grown stronger over the years and are presumably related to algorithmic trading and funding times in futures markets. He also documents that price formation mainly takes place on the centralized exchanges while price adjustments on the decentralized exchanges can be sluggish.

Zhe Wang, a postdoctoral research associate, is studying flight-to-safety and Bitcoin/equity co-movements. In his work he examines the correlation between equity and the Bitcoin market. He finds a significant and positive correlation between the two markets over short horizons (15-min and 30-min return in the morning or daily return) but not over longer horizons (1 week or longer). Separating regular times from crises in the equity market by a simple flight-to-safety (FTS) indicator shows that the correlation over the short horizon is much stronger during equity market crises. These findings are consistent with the hypothesis that both equity and the bitcoin market are subject to some common short horizon fluctuations but over the long run the two markets have a low correlation because of their different fundamentals implying that Bitcoin is not a good diversifier/hedger for traditional assets over the short horizon.

Conferences

On Friday, March 4th Rethinc. Labs Faculty Director and UNC Kenan-Flagler Business School Professor of Finance, Eric Ghysels and Cam Harvey, Professor of Finance at Duke Fuqua School of Business co-hosted the first academic conference on Decentralized Finance (DeFi). Sponsored by UBRI and Ripple, this was Rethinc. Labs first event to be held in person, taking place at UNC Kenan-Flagler's Rizzo Center in Chapel Hill.

PAPERS PRESENTED
Decentralization through Tokenization
Michael Sockin (UT Austin) and Wei Xiong (Princeton)

Blockchain Analysis of the Bitcoin Market
Igor Makarov (LSE) and Antoinette Schoar (MIT)

Decentralized Exchanges
Alfred Lehar (University of Alberta) and Christine Parlour (UC Berkeley)

The Conceptual Flaws of Constant Product Automated Market Making
Andreas Park (University of Toronto)

An Economic Model of Consensus on Distributed Ledgers
Hanna Halaburda (NYU), Zhiguo He (University of Chicago) and Jiasun Li (George Mason)

Staking, Token Pricing, and Crypto Carry
Will Cong (Cornell), Zhiheng He (Tsinghua University) and Ke Tang (Tsinghua University)

On March 2, 2023 we co-hosted the Future of Digital Assets Symposium joint with the Milken Institute at the Gallup Building, Washington DC.

Future of Digital Assets Symposium Speaker List and Program
Session #1: *A Conversation with US Representative French Hill, Chairman, US House Financial Services Subcommittee on Digital Assets, Financial Technology and Inclusion*
• The Honorable French Hill, US Representative, Arkansas; Chairman, US House Financial Services Subcommittee on Digital Assets, Financial Technology and Inclusion
• Moderator: Nicole Valentine, FinTech Director, MI Finance, Milken Institute

Session #2: *Crypto Policy: New Rules for a New Paradigm*
• Scott Bauguess, VP, Global Regulatory Policy, Coinbase
• Jonathan Jachym, Global Head of Policy, Kraken
• Brian Quintez, Head of Policy, a16z Crypto
• Sandra Ro, CEO, Global Blockchain Business Council
• Moderator: Brian Brooks, CEO, BitFury

Session #3: *Digital Assets, DeFi and Institutional Adoption: A Conversation with David Mercer, CEO of LMAX Group*
• David Mercer, CEO, LMAX Group
• Moderator: Kailey Leinz, Anchor, Bloomberg TV

Session #4: *Digital Innovation and Security: Compatible or Competing?*

• Cody Carbone, VP of Policy, Chamber of Digital Commerce
• Ric Edelman, Founder, Digital Assets Council of Financial Professionals (DACFP)
• Kathy Kraninger, VP of Regulatory Affairs, Solidus Labs
• Erin Plante, VP, Investigations, Chainalysis
• Justin Stottlemyer, Director of Crypto Center of Excellence, Intuit
• Moderator: Casey Wagner, Reporter, Blockworks

Session #5: *The Digital Currency Global Revolution*
• Darrell Duffie, Adams Distinguished Professor of Management and Professor of Finance, Stanford Graduate School of Business
• Moderator: Campbell R. Harvey, Professor of Finance at the Fuqua School of Business, Duke University

Session #6: *A New Regulatory Framework for Digital Assets Built Upon Innovation, Transparency, and Consumer Protection: A Conversation with US Senators Kirsten Gillibrand and Cynthia Lummis*
• The Honorable Kirsten Gillibrand, US Senator, New York
• The Honorable Cynthia Lummis, US Senator, Wyoming
• Moderator: Michael Piwowar, Executive Vice President, MI Finance, Milken Institute

Session #7: *The Future of Innovative Finance: A Conversation with Brad Garlinghouse, CEO of Ripple*
• Brad Garlinghouse, CEO, Ripple
• Moderator: Michael Piwowar, Executive Vice President, MI Finance, Milken Institute

Session #8: *Global Crypto Regulatory Outlook*
• Noach Hacker, Minister of Economic Affairs, Embassy of Israel
• Bryan Stirewalt, Senior Managing Director, K2 Integrity
• Moderator: Milken Institute FinTech Team

Session #9: *Public-Private Partnerships for Innovations in Payments and Financial Contracting with Tobias Adrian, IMF*
• Tobias Adrian, Financial Counsellor and Director of the Monetary and Capital Markets Department, International Monetary Fund (IMF)
• Moderator: Eric Ghysels, Research Director, Rethinc.Labs, Distinguished Professor, University of North Carolina, Kenan-Flagler Business School

Session #10: *The Crypto Opportunity: The View from Chief Executives*
• Dave Siemer, CEO, Wave Financial Group
• Sheila Warren, CEO, Crypto Council for Innovation
• John Wu, President, AVA Labs
• Moderator: Daniel Gorfine, Founder and CEO, Gattaca Horizons, LLC

Session #11: *Inclusive FinTech*
• Ashley Bell, CEO and Founder, ReadyLife
• Corey Carlisle, Head of Policy and Social Impact, Varo Bank

• Nicole Elam, President & CEO, National Banker's Association
• Moderator: Greg Brown, Professor of Finance, UNC, Executive Director, Kenan Institute of Private Enterprise, Research Director, IPC

Session #12: *Privacy and Central Bank Digital Currencies*
• Jennifer Lassiter, Executive Director, Digital Dollar Project
• Alexandra Steinberg Barrage, Partner, Davis Wright Tremaine
• Mark Young, Chief Risk Officer/Data Advisor, ConsenSys
• Moderator: Sarah Wynn, Reporter, The Block

Session #13: *Venture Capital and Investing in Digital Assets*
• Barbara Iyayi, Founder and Managing Partner, Unicorn Growth Capital
• Colin Jones, Head of Strategic Investments, Horizen Labs
• Adam Mastrelli, Partner, Investments, Woodstock US
• Alex Simpson, Founder, Openstock, Angel Investor, Milken Young Leader
• Moderator: Saif Ishoof, Founder, Lab 22C

Session #14: *Can Web3 Help Build a Better Internet?*
• Les Borsai, Co-Founder and Chief Strategy Officer, Wave Financial
• Falon Fatemi, CEO & Co-Founder, Fireside
• Alex Pruden, CEO, Aleo
• Moderator: Tomicah Tilleman, Chief Policy Officer, Haun ventures

Papers Presented

Automated Market Making and Loss-Versus-Rebalancing
Ciamac C. Moallemi - Columbia University

Reaching for Yield in Decentralized Financial Markets
Patrick Augustin - McGill University

Systemic Fragility in Decentralized Markets
Alfred Lehar- University of Calgary

Scaling Smart Contracts via Layer-2 Technologies: Some Empirical Evidence
Luofeng Zhou- Columbia University

Stablecoin Runs and the Centralization of Arbitrage
Yao Zeng- University of Pennsylvania

Anatomy of a Run: The Terra Luna Crash
Igor Makarov- LSE

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Rewired.one

RFI Response:
Digital Asset R&D Agenda

A Rewired.one deliverable

3 March, 2022

Author: Torben Anderson MSc Blockchain and Digital Currencies

Response Type: Other - Organisation - Professional Services Firm

Rewired Consulting LLC
[redacted], United States of America
www.rewired.one

[redacted]

Table of Contents

Introduction

As we navigate through the 21st century, the world is becoming increasingly interconnected and reliant on technology. Decentralized technologies, such as cryptocurrencies, blockchain, and digital identity systems, have emerged as critical components of this technological revolution.

The United States has long been a leader in technological innovation, and we cannot afford to fall behind in this rapidly evolving landscape. Our ability to harness the power of digital assets will be a key determinant of our economic success and global influence in the years to come.

By embracing digital assets, we can create new opportunities for innovation, entrepreneurship, and job creation. We can streamline and enhance our financial systems, making them more efficient, transparent, and secure. We can empower individuals to have greater control over their personal data and digital identities, while also protecting national security interests.

Competition is fierce. Other nations around the world are already investing heavily in digital asset technology and positioning themselves for dominance in the global marketplace. We cannot afford to lag behind.

Digital assets are critical to the future growth and global leadership of the United States of America. We must embrace this new era of technological innovation and ensure that we remain at the forefront of the digital revolution. Failure to do so would be a disservice to our nation and future generations.

The tokenization of everything

The process of tokenisation enables the creation of a unique digital representation of a physical or intangible asset, allowing it to be traded, exchanged, and transferred in a secure and transparent manner on a blockchain network. This trend has the potential to disrupt a wide range of industries, from finance and real estate to gaming and sports. In short, the tokenization of everything is rapidly transforming the way we perceive, interact with, and derive value from the world around us.

In recent years, we have witnessed an explosion in the creation and adoption of digital tokens that represent a wide variety of assets, from traditional securities and commodities to more unconventional items such as art, real estate, and even personal data. The potential applications and implications of this trend are vast, and it is essential that we understand its significance for our economy, society, and way of life. According to a report by PwC, the total value of tokenized assets was estimated to be around $1.5 trillion in 2020. This is a small fraction of the total value of global assets. The report also notes that future potential for tokenization is much larger. Estimates range from $24 trillion to $640 trillion in the long term.

Opportunities to advance responsible innovation in the broader digital assets ecosystem:

Introduction

Responsible financial innovation entails the development of novel financial products and services that cater to the well-being of individuals and communities at large, while also keeping in check any potential risks and negative consequences.

This implies crafting innovations with a customer-centric approach, with full transparency and an adequate comprehension of customers' needs, preferences, and financial literacy. Additionally, complying with relevant laws and regulations is paramount to developing innovations that safeguard stakeholders' interests.

Furthermore, sustainability must be at the forefront of any responsible financial innovation, considering the impact of such innovations on environmental, social, and governance issues. To ensure the effectiveness of responsible financial innovation, risk management should also be factored in, including credit, market, operational, and reputational risks.

Finally, ethical considerations and values, such as integrity, fairness, and privacy, must be the bedrock of any innovation that has a positive impact on customers, without exposing them to harm.

Here are some key focus areas that are supported and are necessary for a holistic approach responsible for innovation for digital assets.

Workforce Enablement

For the USA to quantum leap and become a forbidale leader in safe Digital Asset innovation, deployment and regulation, significant and focused investment is needed. We recommend the USA invest in educational programs that teach digital asset skills, such as blockchain technology, cryptography, and programming languages. Not focusing on foundational aspects of digital assets, like these, puts the USA at risk of developing a shallow understanding of digital asset systems.

We recommend the USA invest in reskilling and upskilling programs to help existing workers develop the skills needed for the digital asset industry. This includes partnering with small businesses that can offer niche training programs and resources to help workers transition to new roles and industries, and by prompting diversity and inclusion in the digital asset industry by providing opportunities for underrepresented groups and minorities.

Collaboration with industry is critical to ensuring that the US workforce is prepared for the digital asset industry. Industry means not just large multinationals, but also grassroot startups and small and medium enterprises that can offer faster times to market. We highly recommend the federal and state governments work with the private sector to identify the skills needed for the digital asset industry, and indeed partner to develop educational programs to meet the needs.

In addition the government can provide support to the digital asset industry by offering tax incentives and other forms of support to businesses and individuals working in the industry. This can help attract top talent and encourage innovation.

Digital assets standards board

We recommend the setup of a new equally represented standards board. A new board that is made up of government bodies, private sector industry and consumer both public, exchanges, banking and investors. Government agencies can include, but are not limited to the FED, SEC, CFTC, FDIC, OCC, NCUA, CFPB, FSOC, Treasury Dep. and State-level regulatory bodies, led by the Office of Science and Technology Policy (OSTP), or associated body.

The goal of a standards board is to promote and educate where digital assets can solve a pain point that could not otherwise be addressed through centralized systems and provides true utility of digital asset deployment. This will result in the use of sustainable business practices, and the value is captured through use, not through the perpetual addition of new speculative token buyers. Code is audited and standards and testing practices are developed that meet or exceed industry norms.

Embrace transparency and accountability.

Blockchain can help create an immutable and transparent record of government transactions and activities, thereby increasing accountability and reducing the potential for bad actors that bring about corruption. We recommend that blockchain itself is used to help integrate regulatory processes directly into the digital asset landscape. This is an innovation in and of itself and positions the federal government as not only as a participant, but indeed also a user of the technology. This will drive innovation at the highest level. It also builds governance of digital assets directly into the framework of the US financial system, not to mention supply chains and other critical processes that can be secured through digital asset transactions and exchange.

Prioritize data and process security

By providing a secure and decentralized platform for sharing information, blockchain can help streamline bureaucratic financial processes and reduce an almost infinite number of costs for the

US government and US economy as a whole. We recommend the development of a blockchain based computation platform, that can be used to secure critical government information and infrastructure, that can be integrated with other private and public blockchain networks. This will give digital asset projects and financial institutions the opportunity to self regulate by providing regulatory data feeds directly to government agencies like SEC etc.

Voting and reducing election fraud

Blockchain can be used to create secure and transparent voting systems, which could help reduce the risk of election fraud and improve the integrity of the democratic process.

Securing citizen data and citizen services

Blockchain can provide a secure and tamper-proof method of storing sensitive data, on real-world data and assets, such as citizen information or land records.

Government accounting

Blockchain can help governments track tax payments and reduce tax evasion by providing a transparent and tamper-proof record of financial transactions, by leveraging the programmable nature of digital assets.

Promote inclusivity

Digital assets can empower individuals by enabling them to participate in new financial ecosystems and empowering them to take control of their financial futures.

Regulatory Collaboration

Driving regulatory collaboration is key to ensuring the long-term sustainability of digital assets. Developing common standards across regulatory bodies is critical to ensuring that digital assets can operate across borders, and international cooperation is essential in promoting regulatory collaboration.

Regulatory bodies must work together to establish common goals and develop regulatory frameworks that support innovation while protecting consumers. Regulatory bodies must share information to develop effective regulatory frameworks. This includes sharing best practices, regulatory approaches, and emerging risks associated with digital assets.

Regulatory sandboxes can facilitate regulatory collaboration by providing a safe space for businesses and emerging marketplaces to test innovative ideas and products while adhering to regulatory requirements. This enables regulatory bodies to gain insights into new business models and technologies and develop more effective regulatory frameworks, in partnership with the private sector.

Funding Innovation

Crowdfunding: Crowdfunding is an effective way to fund digital asset projects at the grassroots level. Crowdfunding platforms enable individuals to contribute small amounts of money to fund projects they believe in. This allows grassroots projects to bypass traditional funding channels and reach a wider audience.

Grants: Grants from government agencies, non-profit organizations, and private foundations can provide critical funding for digital asset projects at the grassroots level. These grants often prioritize projects that promote innovation and inclusivity.

Angel Investors: Angel investors are high net worth individuals who provide funding to startups and early-stage projects. Angel investors are often more willing to take risks and invest in emerging technologies than traditional venture capitalists.

Community Funding: Community funding models, such as community shares, allow individuals to invest in local projects they believe in. This can be particularly effective for grassroots digital asset projects that have a strong local following.

Incubators and Accelerators: Incubators and accelerators provide funding, mentorship, and resources to early-stage projects. These programs can be particularly effective for grassroots digital asset projects that lack the resources and expertise to bring their ideas to market.

Digital Asset Education

Digital Asset Fundamentals: Education on the basics of digital assets is imperative. People must have a comprehensive understanding of what digital assets are, their various types, associated benefits, risks, and regulations.

Blockchain Technology: In-depth knowledge of blockchain technology is a vital component of digital asset education, given that it's the underlying technology of most digital assets. People need to comprehend how blockchain works, the different types of blockchain, and their applications.

Security and Privacy: Digital asset education should place an emphasis on security and privacy considerations when utilizing digital assets. People need to know how to safeguard their digital assets from theft, cyberattacks, and hacking, as well as how to ensure their personal data is secure when using digital assets.

Investment Strategies: Understanding the various investment strategies and their associated risks is an essential aspect of digital asset education. People should be familiar with different approaches to buying, trading, and holding digital assets. They should also know how to assess the value of digital assets and evaluate potential risks.

Business Applications: Digital asset education should concentrate on the various business applications of digital assets, such as supply chain management, real estate, and healthcare. People need to comprehend how digital assets can be utilized to enhance business operations and leverage the advantages of blockchain technology.

Securing Supply Chains

Digital assets can be employed to verify the authenticity of goods and materials by creating an infallible record of their origin and provenance. This helps prevent fraudulent activities and ensures only genuine products are distributed to customers.

Smart contracts can also be implemented to automate certain processes in the supply chain, such as payment processing, quality assurance checks, and delivery confirmation, leading to increased efficiency and reduced risk of errors.

In addition, blockchain technology's shared digital ledger allows for improved transparency and accountability between suppliers, manufacturers, and customers. It promotes trust and helps to mitigate disputes and conflicts.

Fundamentally all components of a supply chain can be considered to be an asset, or stream of interconnected assets that deliver a particular service, supply chain or other critical outcome e.g. Food security. Rewired invision that these processes themselves will be traded as digital assets in newly formed digital marketplaces.

References

- RESPONSIBLE ADVANCEMENT OF U.S. COMPETITIVENESS IN DIGITAL ASSETS U.S. Department of Commerce
- CBInsights - State of Blockchain - Global - Q3-2022
- Digital Switzerland Strategy 2023
- Digital Assets Competitiveness Report (US)
- Remote Election Technology Report
- Global Blockchain Survey: Blockchain momentum continues to grow

About Rewired

At Rewired we know that you want to be an organization with trustworthy data and efficient processes. In order to do that, you need secure, transparent, and traceable data and automated systems. The problem is that data can be untrustworthy, and processes can be archaic. This makes an organization experience vulnerability to chaos and become out-of-date.

We believe it is your organization's right to have the safest and most efficient data systems available in the world. We understand that modern businesses operate with big data. It can be difficult to secure and manage data in a world that has increasing access to it. This is why our experts use the most modern technology, blockchain, to offer you the highest efficiency processes and trustworthy data available.

Our mission is to empower pioneers within government agencies, organizations and enterprises, to rewire our nation for a freer and fairer economic system.

Believing that emerging technologies including blockchain would be a major part of the solution, Torben co-founded rewired.one in 2018 with a vision for personal, economic, and systemic freedom.

Torben Anderson - MSc Blockchain and Digital Currencies. Torben has been a management consultant for more than 25 years working with some of the world's biggest financial firms, regulators and central banks, specializing in digital transformation. Believing the consulting model was broken, Torben was searching for a better way for supporting, and doing, business.

Torben was instrumental in delivering new regulatory systems at the Bank of England (BoE) after the 2008 banking crisis, and has also led other major change programmes in financial services and energy sectors.

He is passionate about making the impossible possible and committed to developing the future of blockchain solutions. Torben has a Bachelor's degree in Computer Science and Economics and his Master of Science in Blockchain and Digital Currencies.

Contact information

Principle Lead: Torben Anderson, Chief Executive Office,[redacted]

Organization: Rewired Consulting LLC, [redacted]

Rewired.one has office in United States, United Kingdom and Australia.

Legal Disclaimer

This paper and the associated research is conducted based on public information sources, such as White Papers, Internet Resources and previous knowledge gained. Rewired.one cannot guarantee the validity of the information in this paper. The contents of this paper do not constitute any legal or financial advice in any way whatsoever.

The information provided in this paper does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this paper are for general informational purposes only. Information in this paper may not constitute the most up-to-date legal or other information. This paper contains links to other third-party websites. Such links are only for the convenience of the reader, and Rewired.one does not recommend or endorse the contents of the third-party sites.

Readers of this paper should contact their attorney to obtain advice with respect to any particular legal matter. No reader of this paper should act or refrain from acting on the basis of information in this paper without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation. Use of, and access to, this paper or any of the links or resources contained within this paper do not create an attorney-client relationship between the reader and authors, contributors, contributing law firms, or Rewired.one and their respective employees.

All liability with respect to actions taken or not taken based on the contents of this paper are hereby expressly disclaimed. The content is provided "as is;" no representations are made that the content is error-free. Rewired.one is not liable for any damages arising in using the data out of this paper or from any action or decision taken as a result of using this paper.

This paper offers links to other sites. Rewired.one is not responsible for the content of these linked sites, nor for the proper functioning of these links in the future.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Riot Platforms, Inc.

Riot Platforms' Response to the OSTP RFI Seeking Comments on Digital Assets Research and Development

March 3, 2023

For additional information about this response, please contact:

Brian Morgenstern
Riot Platforms, Inc.
[redacted]

[redacted]

About Riot

Riot Platforms, Inc. (NASDAQ: RIOT) is an American construction, manufacturing, and data center company that builds and operates infrastructure for the Bitcoin network. As of December 31, 2022, Riot employs 489 professionals in Colorado and Texas. Riot's facility in Rockdale, Texas is the largest Bitcoin mining data center in North America with 700 megawatts in total capacity. Additionally, Riot is beginning development of a second large-scale Bitcoin mining data center in Corsicana, Texas which is expected to have approximately one gigawatt of available capacity.

Submitted electronically to DARD-FTAC-RFI@nitrd.gov
Subject: **RFI Response: Digital Assets R&D Agenda**

Deputy General Counsel Rachel Wallace,

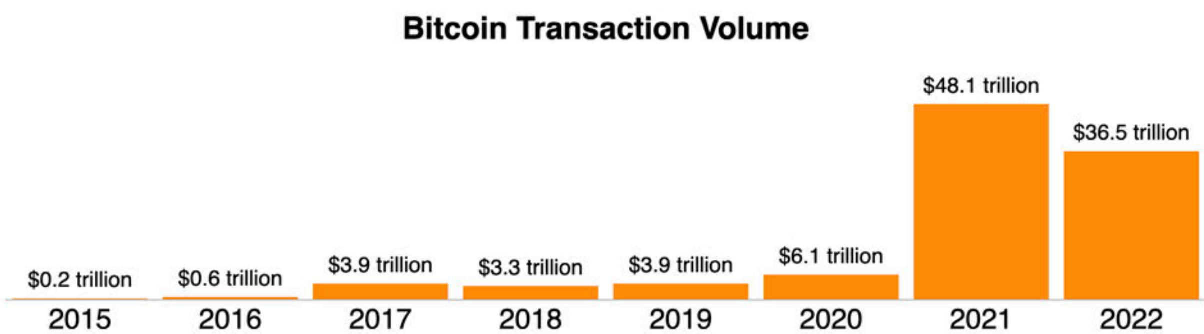
The following comments are submitted by Riot Platforms, Inc. in its capacity as a member of the Bitcoin industry. Riot is grateful to have the opportunity to comment on a National Digital Assets Research and Development Agenda. Thank you for your engagement of the public on this important matter.

Very truly yours,
Riot Platforms, Inc.

1. The value of Bitcoin

Satoshi Nakamoto summarized his reason for inventing Bitcoin in this way: "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. […] Bitcoin is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending."[1]

Bitcoin (BTC) provides access to payments without relying on financial intermediaries. The benefits of transacting with Bitcoin include 24/7 availability, global electronic final settlement in less than one hour, open-source programmability and auditability, and cryptographic security. These benefits provide value to the public and have grown the transactional use of Bitcoin from zero in 2009 to $36.5 trillion worth of bitcoin transacted on its decentralized ledger in 2022.



In addition to its medium-of-exchange transactional users, Bitcoin has accrued a significant base of long-term investors. Investors value the Bitcoin network's predictable issuance schedule[2]. The quantity of BTC units on the ledger can be independently verified using open-source node software[3].

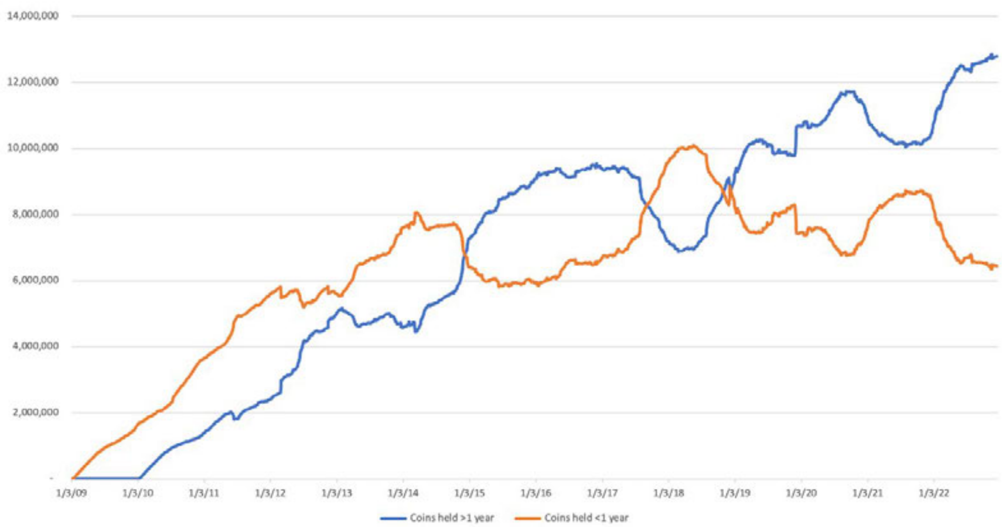
Node software is like internet browser software, it enables a user to access the network. Unlike a web browser, a Bitcoin node downloads and verifies all the network's data to independently re-calculate the ledger of all Bitcoin transactions and thus audit the supply of BTC. The majority of the BTC are held by long-term investors as a store-of-value often described as "digital gold",

[1] Nakamoto, Satoshi. Bitcoin Open Source Implementation of P2P Currency. Satoshi Nakamoto Institute, 11 Feb. 2009, https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

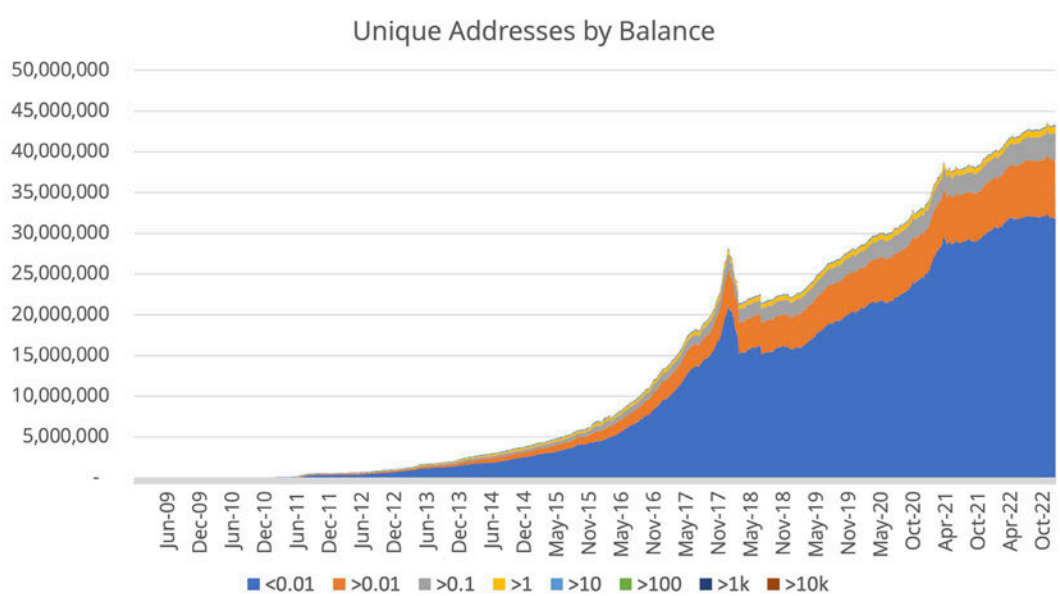
[2] Jones, Paul Tudor. "The Great Monetary Inflation." Market Outlook – Macro Perspective, 10 May 2020, https://www.lopp.net/pdf/BVI-Macro-Outlook.pdf.

[3] Rochard, Pierre. "Auditing Bitcoin Supply." PierreRochard.com, 8 Oct. 2020, https://www.pierrerochard.com/auditing-bitcoin-supply/.

a hedge against fiscal and monetary risks[4] of proprietary centralized systems. Data from the blockchain indicates that the majority of BTC has been held as long-term savings, not as a short-term speculation.



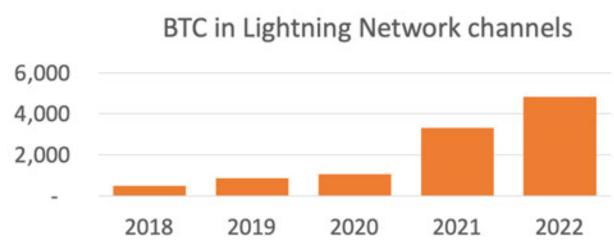
Small and large balances of BTC are treated equally by the Bitcoin network. Wealth does not influence the Bitcoin protocol's operations, unlike the proprietary fiat system where wealth can waive fees, raise limits, and give access to exclusive perks[5]. Most of the Bitcoin addresses, analogous to accounts, hold less than 0.01 BTC (roughly $200 based on the current exchange rate).



[4] Roy, Avik. "How Bitcoin Protects Americans from Inflation." Bitcoin Policy Institute, 26 Oct. 2021, https://www.btcpolicy.org/articles/how-bitcoin-protects-americans-from-inflation.
[5] Dimon, Jamie. "Chase Private Client Checking." Chase, https://www.chase.com/personal/checking/private-client.

Creating a Bitcoin address (a “wallet”) is just cryptographic math, and it's free and instant. Though it is still unfamiliar to most people, anyone can learn to use Bitcoin today. The option to use Bitcoin is available to everyone equally, the powerful and the marginalized, the banked and the unbanked. As a public network, Bitcoin is a beacon of global empowerment and financial inclusion[6].

To speed up small Bitcoin payments, open-source protocol developers invented an overlay network called Lightning[7]. This network routes payments through channels anchored in the Bitcoin blockchain. Lightning enables small transfers of BTC to be instant and almost free, while still benefiting from the Bitcoin protocol’s security and stability. The Lightning network’s openness and programmability has attracted successful fintech entrepreneurs like Jack Dorsey[8] and David Marcus[9] to build Lightning-integrated products. The quantity of BTC committed to the Lightning network has been increasing[10] over the past five years:



2. Realities of Bitcoin

No system can be or is perfect. While Bitcoin has fewer risks and harms than proprietary centralized fiat systems, it should be closely evaluated.

Software Limitations

The public can independently verify Bitcoin transactions and audit the Bitcoin ledger to ensure compliance with the Bitcoin protocol rules by using node software. This software connects with the Bitcoin p2p network to download the blockchain data from peers, independently verify each accounting entry, and reproduce the entire Bitcoin ledger. The user’s wallet can query this ledger to summarize balances and transactions. Anyone with a high-speed internet connection and a contemporary computing device can use node software.

---

6 Hernández, Carlos. “Bitcoin Has Saved My Family.” The New York Times, The New York Times, 23 Feb. 2019, https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html.
7 “What Is the Lightning Network?” River Learn - Bitcoin Technology, River Financial, https://river.com/learn/what-is-the-lightning-network/.
8 Namcios. “Jack Dorsey's Cash App Integrates Bitcoin's Lightning Network.” Nasdaq, 7 Feb. 2022, https://www.nasdaq.com/articles/jack-dorseys-cash-app-integrates-bitcoins-lightning-network.
9 Betz, Brandy. Libra Creator David Marcus Begins New Lightning Network Venture, Lightspark. CoinDesk, 12 May 2022, https://www.coindesk.com/business/2022/05/12/libra-creator-david-marcus-begins-new-lightning-network-venture-lightspark/.
10 “Bitcoin: Lightning Network Capacity.” Glassnode Studio - On-Chain Market Intelligence, https://studio.glassnode.com/metrics?a=BTC&category=&m=lightning.NetworkCapacitySum.

The primary source of risks for users of Bitcoin is potential flaws in their node software that mis-apply the protocol rules. The first major incident was in 2010 when an inflation bug in the software enabled anyone to create an infinite amount of bitcoin[11]. This bug was solved by users of node software as they rolled the blockchain back to the last known valid block.

The second and most recent major incident was in 2013[12], when a flawed new version of the node software caused the block size limit to accidentally be increased. To resolve this bug the node operators changed their software back to the previous version. Those are the only two times Bitcoin has a significant consensus-level risk materialize, and in both cases Bitcoin the issue was promptly solved by the users of the software. There have been many minor flaws discovered and resolved of Bitcoin's history. Satoshi Nakamoto's now-famous white paper itself has many known problems that have been discovered[13] and resolved in the 14 years since its publication.

Custody Experiences

With freedom comes responsibility. There are cases of Bitcoin users losing their private keys[14] or getting their wallet hacked[15]. In response to these risks and harms, secure products and best practices have emerged.

Users are encouraged to keep only small amounts of BTC on mobile and desktop software wallets[16]. Keys that control large amounts of BTC should be held in specialized devices known as hardware wallets. The latest generation of devices from leading manufacturers like Coinkite, Ledger, and Trezor have not had a successful private key extraction by security researchers - meaning no one has been able to hack into a wallet and access a user's funds. While critical vulnerabilities may emerge in the future, hardware wallets are currently considered to be secure if properly setup by the user[17].

---

[11] "CVE-2010-5139 Detail." NIST, 6 Aug. 2012, https://nvd.nist.gov/vuln/detail/CVE-2010-5139.

[12] Narayanan, Arvind. "Analyzing the 2013 Bitcoin Fork: Centralized Decision-Making Saved the Day." Freedom to Tinker, 27 Mar. 2019, https://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day/.

[13] Harding, David. "Bitcoin Paper Errata and Details." Gist GitHub, 6 Aug. 2018, https://gist.github.com/harding/dabea3d83c695e6b937bf090eddf2bb3.

[14] Hamilton, Isobel Asher. "The Quest to Find $181 Million in Bitcoin Buried in a Dump." Business Insider, Business Insider, 24 July 2022, https://www.businessinsider.com/james-howells-threw-away-bitcoin-dump-masterplan-get-back-2022-7.

[15] "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency." The United States Department of Justice, 8 Feb. 2022, https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[16] Lopp, Jameson. "Recommended Bitcoin Wallets." Lopp.net, https://www.lopp.net/bitcoin-information/recommended-wallets.html.

[17] Stevens, Robert. "How Do Hardware Wallets Keep Crypto Safe?" CoinDesk, CoinDesk, 22 Nov. 2022, https://www.coindesk.com/learn/how-do-hardware-wallets-keep-crypto-safe/.

To further reduce risk and harms from holding private key material, users are encouraged to use Bitcoin's multi-signature ("multisig") functionality[18]. This functionality can be thought of as a form of two-factor authentication; it removes any single point of failure by requiring a quorum of signers from a set of private keys, for example 2-of-3 or 3-of-5. Decentralization and redundancy of cryptographic key material in different geographic locations with the multisig feature creates unique value for users, unavailable with physical and financial assets.

In addition, hardware wallets can be backed-up on metal as 12 to 24 words, called a "seed plate". This enables private keys to be resilient to fire and flood[19]. Alternatively, these 12 to 24 seed words can be memorized.

The dematerialization of value as private keys is new and unfamiliar to the public, creating risks of harm, but education and new products are bridging the gap to enable the public to secure their Bitcoin. Third-party custody adds risks of harm to the public, as evidenced by the failures of FTX, Celsius, Voyager, and BlockFi[20]. Federal policymakers and researchers should identify ways to encourage the public to self-custody their Bitcoin and avoid trusting third parties.

Illicit Activity

Almost all Bitcoin transaction volume reflects lawful usage by the public. In 2022, only an estimated 0.24% of transaction volume was associated with illicit usage[21] whereas the UN estimates that traditional fiat money laundering is 2.7% of global GDP[22]. To improve their investigative capabilities, law enforcement and prosecutorial agencies can familiarize themselves with Bitcoin through education[23] and usage. The Justice Department has a proven track-record of effectively combating illicit use of Bitcoin[24].

Fiat-crypto exchanges have had guidance on their Bank Secrecy Act AML/KYC obligations since FinCen issued an administrative ruling in 2014[25] to define "virtual currency". Generally, criminals want to convert crypto-currencies to fiat and their activity at regulated exchanges can contribute evidence for prosecution. An industry has emerged to assist law enforcement in

---

[18] "Operational Security Guide." Unchained Capital, Unchained Capital, May 2020, https://unchained.com/wp-content/uploads/2022/01/Unchained-Operational-Security-Guide.pdf.

[19] Lopp, Jameson. "Metal Bitcoin Seed Storage Stress Test." Cypherpunk Cogitations, Lopp.net, 24 Jan. 2020, https://blog.lopp.net/metal-bitcoin-seed-storage-stress-test/.

[20] Olinga, Luc. "FTX, BlockFi, Voyager, Celsius: Awful Year for Crypto Investors." TheStreet, 29 Nov. 2022, https://www.thestreet.com/investing/cryptocurrency/ftx-blockfi-voyager-celsius-awful-year-for-crypto-investors.

[21] The 2023 Crypto Crime Report. Chainalysis, Feb. 2022, https://go.chainalysis.com/2023-crypto-crime-report.html.

[22] "Tax Abuse, Money Laundering and Corruption Plague Global Finance." United Nations, United Nations, https://www.un.org/development/desa/en/news/financing/facti-interim-report.html.

[23] Bhasker, Sanjeev, et al. "Carpe Crypto: Prosecuting Cases Involving Digital Assets and Blockchain Technology." DOJ Journal of Federal Law and Practice, Dec. 2022, pp. 105–116.

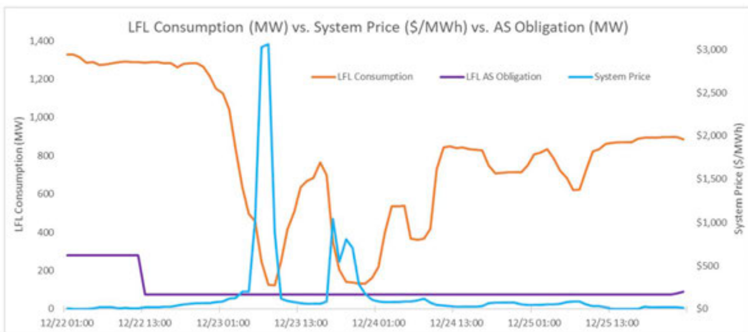
[24] Mallin, Alexander. "DOJ Seizes Millions in Ransom Paid by Colonial Pipeline." ABC News, ABC News Network, 7 June 2021, https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821.

[25] "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System." FinCEN.gov, Financial Crimes Enforcement Network, 27 Oct. 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf.

countering illicit financial activity using digital assets, for example Coinbase, Ciphertrace, and Chainalysis have received government contracts[26].

Energy Facts

Electricity is a dynamic market with volatile supply and demand. On the supply side, volatility is driven by natural gas prices and the intermittency of wind and solar power generation. On the demand side, consumption of electricity is highly seasonal with wide daily oscillations. Bitcoin mining's electricity consumption is highly interruptible, it can quickly and granularly shed load to stabilize the electricity grid and decrease price volatility[27]. Bitcoin contributes to grid resilience and energy security. Texas' ERCOT grid operator illustrated this inverse relationship between electricity prices and Bitcoin mining electricity consumption during the December 2022 Texas freeze[28]:



ercot

Computing cryptographic hashes ("Bitcoin mining") does not directly emit any EPA criteria air pollutants or greenhouse gases (GHG). From a Scope 1 emissions[29] perspective, Bitcoin mining is fully electrified and zero-emissions. Indirectly, Bitcoin mining may reduce electricity grids' greenhouse gas emissions by replacing natural gas and coal peaking power plants[30]. Peaker plants only turn on for short periods of time when there is temporarily high demand, their use is avoided when Bitcoin miners temporarily curtail power usage. This enables the grid to have more zero-carbon electricity producers.

[26] Ehrenhofer, Justin. "Coinbase, Ice and Bitcoin Blockchain Surveillance - Bitcoin Magazine ..." Bitcoin Magazine, 14 July 2022, https://bitcoinmagazine.com/business/coinbase-ice-and-bitcoin-blockchain-surveillance.

[27] Mellerud, Jaran, and Anders Helseth. "How Bitcoin Mining Can Transform the Energy Industry." Arcane Research, 1 Sept. 2022, https://arcane.no/research/how-bitcoin-mining-can-transform-the-energy-industry-new-report.

[28] Woodfin, Dan. "December 2022 Cold Weather Operations: Preliminary Observations." ERCOT Public. ERCOT Public, 24 Jan. 2023.

[29] "Scope 1 and Scope 2 Inventory Guidance." EPA Center for Corporate Climate Leadership, Environmental Protection Agency, https://www.epa.gov/climateleadership/scope-1-and-scope-2-inventory-guidance.

[30] Ibañez, Juan & Freier, Alexander. (2023). Can Bitcoin Stop Climate Change? Proof of Work, Energy Consumption and Carbon Footprint (SoK).

Bitcoin mining's unique controllable load profile was recognized as a benefit to the ERCOT grid by the Texas Work Group on Blockchain Matters Report[31]. Electricity and water consumption, noise pollution, and electronic waste from Bitcoin mining can all be reduced using innovative immersion cooling technology[32].

Benefits of Consensus

The central benefit of Bitcoin's use of proof-of-work ("mining") is the network's decentralized consensus on the order of transactions that are recorded on the ledger. Satoshi Nakamoto's breakthrough was a solution to the "double-spending" problem that did not rely on trusting a third-party[33]. The central benefit of Bitcoin's use of proof-of-work is freedom and inclusion for users[34]: anyone can run a Bitcoin node at a very low cost to verify the miners' work, anyone can earn the block reward by mining[35], and anyone can use the ledger by paying a transaction fee.

Bitcoin miners generate cryptographic hashes using SHA-256. Bitcoin nodes require the miners to provide a hash with a minimum number of leading zeros, called the difficulty. Since each hash is random, miners must generate many hashes to probabilistically find one with enough leading zeros. The difficulty is updated every 2,016 blocks to average a winning hash, and thus a block, every 10 minutes.

Proof-of-stake relies on signatures from a set of token-holders, or "stakers." Unlike proof-of-work hashes, proof-of-stake signatures are not probabilistically anchored in time. Blockchains that use proof-of-stake are therefore more vulnerable to ledger re-writes that compromise their transaction settlement finality, and therefore, the overall integrity of the ledger[36]. Computer science researchers refer to this flaw in proof-of-stake as the "nothing at stake" or "costless simulation" problem[37] and it increases the risk of fraud on the network. A potential solution to this security vulnerability would be to checkpoint proof-of-stake blockchains in

[31] Texas Work Group on Blockchain Matters. "Texas Work Group on Blockchain Matters Report: TX BCWG." Texas Work Group on Blockchain Matters Report | TX BCWG, 15 Nov. 2022, https://portal.bcwg.texas.gov/General-Documents/Texas-Work-Group-on-Blockchain-Matters-Report/wbtp-2m5k.

[32] Economics of Immersion Cooling for Bitcoin Miners. Braiins, 9 May 2022, https://braiins.com/blog/economics-immersion-cooling-bitcoin-miners.

[33] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." To, 31 Oct. 2008, https://nakamotoinstitute.org/bitcoin/.

[34] Huberman, Gur and Leshno, Jacob and Moallemi, Ciamac C., Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System (September 30, 2020). Columbia Business School Research Paper No. 17-92, Available at SSRN: https://ssrn.com/abstract=3025604 or http://dx.doi.org/10.2139/ssrn.3025604

[35] Prat, Julien and Walter, Benjamin, An Equilibrium Model of the Market for Bitcoin Mining (February 05, 2018). CESifo Working Paper Series No. 6865, Available at SSRN: https://ssrn.com/abstract=3143410 or http://dx.doi.org/10.2139/ssrn.3143410

[36] Tas, E. N., Tse, D., Yu, F., & Kannan, S. (2022). Babylon: Reusing Bitcoin Mining to Enhance Proof-of-Stake Security. doi:10.48550/ARXIV.2201.07946

[37] Poelstra, A. (2016, May 25). A Treatise on Altcoins. WP Software. Retrieved September 9, 2022, from https://download.wpsoftware.net/bitcoin/alts.pdf.

Bitcoin's proof-of-work history using Taproot, a recent upgrade to Bitcoin's smart contract scripting language[38].

Bitcoin's use of a proof-of-work system in combination with a difficulty adjustment is at the cutting edge of computer science and software engineering. Bitcoin empowers the public to earn, save, and spend their money freely in a peer-to-peer process, without relying on trusted third-party intermediaries.

3. Federal research opportunities in Bitcoin

Federal research in semiconductor efficiency[39], immersion cooling technologies, and renewable electricity production[40] would increase the competitiveness of Bitcoin mining in the United States. Increasing domestic production of Bitcoin hashrate is in the national security interest of the United States as it reduces hard currency revenues to adversaries[41].

Regulators can help protect consumers from fraud by educating the public about how to securely use Bitcoin node software, hardware wallets, and multisig. Regulators should re-use and elaborate on common phrases that have emerged over the past decade relating to safe Bitcoin use such as "not your keys, not your bitcoin" and "don't trust, verify". In particular, regulators should be cautious not to conflate Bitcoin with knockoff "altcoins" or allegedly unregistered securities in "digital assets".

To effectively improve Bitcoin usability for underserved communities, Federal research opportunities should be directed towards open-source Bitcoin projects with the guidance of organizations like Bitcoin Design[42] and Summer of Bitcoin[43].

4. Federal research priorities for Bitcoin

Federal research opportunities should be introduced to:

---

[38] Azouvi, S., & Vukolić, M. (2022, August 10). *Pikachu: Securing proof-of-stake blockchains from long-range attacks by checkpointing into Bitcoin proof-of-work using Taproot*. arXiv.org. Retrieved September 9, 2022, from https://arxiv.org/abs/2208.05408.

[39] "Efficiency of Bitcoin Mining Hardware." IEA, https://www.iea.org/data-and-statistics/charts/efficiency-of-bitcoin-mining-hardware.

[40] Sigalos, MacKenzie. "Tesla, Block and Blockstream Team up to Mine Bitcoin off Solar Power in Texas." CNBC, CNBC, 8 Apr. 2022, https://www.cnbc.com/2022/04/08/tesla-block-blockstream-to-mine-bitcoin-off-solar-power-in-texas.html.

[41] Orcutt, Mike. "North Korea Appears to Have Expanded Its Crypto-Mining Operation." MIT Technology Review, 22 Mar. 2022, https://www.technologyreview.com/2020/02/11/844871/north-korea-cryptocurrency-mining-monero/.

[42] "Open-Source Design for Bitcoin Products." Bitcoin Design, July 2020, https://bitcoin.design/.

[43] "Summer of Bitcoin." Summer of Bitcoin, Oct. 2021, https://www.summerofbitcoin.org/.

- Verify estimates that Bitcoin's indirect emissions of 62 $MtCO_2e$ per year are orders of magnitude less than tourism's indirect emissions of 4,500 $MtCO_2e$ per year[44].
- Build on existing research to quantify reduced GHG emissions from Bitcoin miners replacing peaker plants[45].
- Compare the low cost of Bitcoin's open-source Lightning network[46] protocol versus the high cost of closed proprietary fiat card fees[47]. Lowering the cost of payments and removing the Visa/Mastercard duopoly as gatekeepers of commerce would advance U.S. competitiveness and leadership in the world.
- Study the potential effect of a de minimis tax exemption[48] on consumer choice for the 19% of Americans who are unbanked or underbanked[49]. Putting Bitcoin and the Lightning network on a level playing field with traditional payment incumbents that are not subject to capital gains tax could help the U.S. catch up to countries that already have a tax exemption for Bitcoin[50].
- Assess how accumulating BTC in a Bitcoin Strategic Reserve can strengthen the US Dollar, increase Federal resilience, reduce Bitcoin's price volatility, and diversify the nation's gold reserves. The U.S. Federal government is already a leading holder[51] of Bitcoin due to past seizures of the asset, but auctions of seized Bitcoin would cede this leading position.
- Evaluate the national security interest in out-competing adversaries with Bitcoin mining[52]. China, North Korea, Iran, Russia, and Venezuela are all mining Bitcoin, the more market share of hashrate the United States can take, the less profitable it is for others to mine. Domestic Bitcoin mining helps advance U.S. competitiveness and leadership in the world.
- Examine the risks and harms of growing authoritarian CBDC networks[53]. CBDCs may enable human rights abuses by authoritarian regimes and undermine economic

---

[44] "Comparisons of Greenhouse Gas Emissions." Cambridge Centre for Alternative Finance, https://ccaf.io/cbeci/ghg/comparisons.
[45] How Bitcoin Mining Can Support the Energy Transition. Wood Mackenzie, 7 Apr. 2021, https://www.woodmac.com/news/opinion/how-bitcoin-mining-can-support-the-energy-transition/.
[46] Ogawa, Yuya. Lightning Network's Advantages as Payment Technology. Bitcoin Magazine, 8 Aug. 2022, https://bitcoinmagazine.com/technical/lightning-network-payment-technology-advantages.
[47] Durbin, Marshall Introduce Bipartisan Credit Card Competition Act: U.S. Senator Dick Durbin of Illinois. 28 July 2022, https://www.durbin.senate.gov/newsroom/press-releases/durbin-marshall-introduce-bipartisan-credit-card-competition-act.
[48] Brito, Jerry. "Congress Takes a Step toward a De Minimis Capital Gains Exemption for Everyday Cryptocurrency Transactions." Coin Center, 26 July 2022, https://www.coincenter.org/congress-takes-a-step-toward-a-de-minimis-capital-gains-exemption-for-everyday-cryptocurrency-transactions/.
[49] "Economic Well-Being of U.S. Households in 2021." Board of Governors of the Federal Reserve System, May 2022, https://www.federalreserve.gov/publications/files/2021-report-economic-well-being-us-households-202205.pdf.
[50] "Crypto Tax Free Countries 2023." Koinly, 3 Jan. 2023, https://koinly.io/blog/crypto-tax-free-countries/.
[51] "Bitcointreasuries.net." BitcoinTreasuries.NET, https://bitcointreasuries.net/.
[52] Lowery, Jason. Softwar: A Novel Theory on Power Projection and the National Strategic Significance of Bitcoin. Massachusetts Institute of Technology, 2023.
[53] Kimani, Michael. "China Leads Africa's Digital Currency Race." CoinDesk, 14 Sept. 2021, https://www.coindesk.com/policy/2021/02/03/china-leads-africas-digital-currency-race/.

growth[54]. The introduction of this foreign technology in the United States could enable adversaries to fully control and surveil domestic economic activity, directly undermining U.S. leadership and competitiveness.

- Identify and responsibly disclose vulnerabilities, as well as suggest usability improvements, in the MuSig family of cryptographic protocols[55] to increase security for Bitcoin users.

Federal R&D for software and hardware development should be focused on open-source contributions to existing projects, rather than creating duplicative new projects. Furthermore, research should be oriented towards solving real Bitcoin user problems. These problems can be identified in existing UX research[56], through new research initiatives, with first-hand experience using Bitcoin in various contexts, and by working directly with Bitcoin stakeholders.

5. Bitcoin education in the United States

Regardless of warnings from skeptical adults, children of all ages are going to experiment with Bitcoin because the technology is freely available. To protect children from risks and harms of Bitcoin, educational curriculums at all age levels should be updated to include how to use Bitcoin and Lightning wallets securely and responsibly. In higher education, Texas A&M University has introduced a Bitcoin Protocol course[57] for computer science students to familiarize themselves with the technical underpinnings of Bitcoin. Workforce training at technical colleges should include opportunities to learn how to repair Bitcoin mining rigs. The unfamiliarity of Bitcoin indicates that a significant national competitive advantage can be developed through education.

Conclusion

Bitcoin's freedom and inclusion benefits have resulted in significant adoption by the public over the past decade. The Bitcoin community[58] and industry have developed educational material and products to successfully mitigate the risks and harms of Bitcoin. The National Digital Assets Research and Development Agenda should build on this track-record to help advance U.S. competitiveness and leadership in the world.

---

[54] Smolenski, Natalie. "Why the U.S. Should Reject Central Bank Digital Currencies." Bitcoin Policy Institute, 27 Sept. 2022, https://www.btcpolicy.org/articles/why-the-u-s-should-reject-central-bank-digital-currencies.

[55] "Musig." Bitcoin Optech, https://bitcoinops.org/en/topics/musig/.

[56] Estevão, Patrícia. "Bitcoin UX Research." Patrícia Estevão, 15 Aug. 2021, https://patestevao.com/work/bitcoin-ux-research/.

[57] Henton, Lesley. "New Class Explores Technical and Economic Foundations of Bitcoin." Texas A&M Today, 3 Feb. 2023, https://today.tamu.edu/2023/01/20/new-class-explores-technical-and-economic-foundations-of-bitcoin/.

[58] Rizzo, Pete. "Why Bitcoin Maximalism Is Critical." Bitcoin Magazine, 12 July 2022, https://bitcoinmagazine.com/culture/why-bitcoin-maximalism-is-critical.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Ripple Labs Inc. (Ripple)

March 3, 2023

The White House
Office of Science and Technology Policy
[redacted]

Email: DARD-FTAC-RFI@nitrd.gov

To whom it may concern:

Ripple Labs Inc. (Ripple) welcomes the opportunity to comment on the White House Office of Science and Technology Policy's (OSTP) request for information entitled "Request for Information; Digital Assets Research and Development" (the RFI). The RFI was issued in response to President Biden's Executive Order, "Ensuring Responsible Development of Digital Assets," and following OSTP's report, "Technical Evaluation for a U.S. CBDC System", which prompted further questions regarding digital assets research and development (R&D).

Ripple strongly believes that the United States can and should be a leader in the digital assets space. This requires not only implementation of a proper regulatory framework, but also robust investment in developing and applying the technology underlying digital assets. As identified in the RFI, there are myriad opportunities to leverage digital assets to achieve key policy objectives, ranging from advancing financial inclusion and equity goals to supporting environmental and sustainability objectives. A coordinated, comprehensive and strategic approach to digital assets R&D will allow the United States to leverage these technologies and apply them in ways that will benefit the nation and its citizens.

Introduction

Using blockchain technology, Ripple allows financial institutions to process payments instantly, reliably, cost-effectively, and with end-to-end visibility anywhere in the world. Our customers are financial institutions that want tools to effect faster and less costly cross-border payments, as well as eliminate the uncertainty and risk historically involved in moving money across borders using interbank messaging alone. All this is done in compliance with AML/BSA regulations.

Some customers, in addition to deploying Ripple's "blockchain" based software solution (RippleNet), leverage a digital asset known as XRP. Just as Bitcoin is the native asset to the open-source Bitcoin ledger, and Ethereum is the native asset to the open-source Ethereum ledger, XRP is the native asset to the open-source XRP Ledger. XRP, given its unique design, can serve as a near instantaneous bridge between fiat currencies (or any two representations of value), further reducing the friction and costs for commercial financial institutions to transact across multiple global markets.

Although Ripple utilizes XRP and the XRP Ledger in its product offerings, XRP is independent of Ripple. The XRP Ledger is decentralized, open-source, and operates on what is known as a "consensus" protocol, eliminating the need for mining and making it one of the most environmentally-friendly ledgers in the digital asset space. While there are well over a hundred known use cases for XRP and the XRP Ledger, Ripple leverages XRP for use in its product suite because of XRP's suitability for cross-border payments. Key characteristics of XRP include speed, scalability, energy efficiency, and cost efficiency, all of which benefits the consumer and helps reduce friction in the market for cross-border payments.

***

With this overview, Ripple respectfully submits the following response to the OSTP's RFI.

Sincerely,

Ripple Labs Inc.

Response to RFI

Goals, sectors, or applications that could be improved with digital assets and related technologies

Ripple's vision is the Internet of Value, where value flows over the internet as easily, freely, and cheaply as information does today. Digital assets, as defined in the RFI, play an instrumental role in allowing us to pursue this vision as discussed below. As adoption of digital asset applications and development of blockchain technology continues to increase, the benefits and positive impacts likewise trend upward.

Cross-border payments

Cross-border payments are costly, full of friction, and slow. Much of this friction is the result of processes followed in cross-border payments, long the domain of incumbent or correspondent banks. Correspondent banking has been described as "the provision of current or other liability account and related services to other financial institutions (including affiliates), used for the execution of third-party payments and trade finance as well as its own cash clearing, liquidity management, short-term borrowing and investment needs in a particular currency."[1]

As this definition highlights, banks use correspondent relationships – a network of bilateral, accounts-based relationships – spread across the world to process payments originating from their corporate and retail clients. Although widely proliferated, the market structure of correspondent banking injects significant friction, delay and costs in processing payments for the respondent banks, primarily due to the need to pre-fund accounts. In various instances, these costs are also then passed down to retail customers.

This is best exemplified in the case of remittances. U.S. workers with relatives overseas are often saddled with high transaction fees when sending money home, which are sometimes so egregious that senders are disincentivized to make the transaction.[2] This is because remittance providers have historically enabled payments through the cumbersome correspondent account ecosystem, which not only traps enormous amounts of capital, but also creates compliance costs and foreign exchange and counterparty risks that often must be hedged. Additionally, these remittance corridors are sometimes too small to warrant adequate attention from major financial institutions, and therefore cannot reach the economies of scale needed in order to reduce costs. As a result, the process can limit the reach of efficient payment solutions to only

[1] https://www.bis.org/cpmi/publ/d136.pdf.

[2] According to an IMF Working Paper, How do Transaction Costs Influence Remittances, between 5 and 15 percent of remittances are "lost" due to high transaction costs, depending on the country and the amounts sent home.

high-volume currency pairs, adding further opacity to the fees charged to remittance-sending customers.[3]

Digital assets specifically designed for payments have the potential to reduce these limitations by enabling payments without the need to pre-fund accounts overseas. For example, Ripple's software leverages the digital asset XRP as a bridge between currencies. This allows financial institutions to access liquidity on demand through digital asset exchanges without having to pre-fund accounts in the destination country. The payer and payee continue to use fiat currency for their payment, with XRP incorporated as a bridge between the regulated financial institutions that are facilitating the remittance transaction. This is particularly helpful for smaller institutions with limited capital.

Micropayments

Digital assets are also helpful for the facilitation of micropayments (i.e., payments made for very small amounts - sub $5), the increase of which could well enable new business models. Currently, the transaction costs associated with micropayments made in fiat currency are often too high to support their execution. Enabling the ability to pay for a single news article or television episode - or even to pay per second or per page of content - rather than a full subscription service has the ability to fundamentally transform commerce.

The facilitation of micropayments similarly has the power to transform remittances. The World Bank estimates that remittances to low- and middle-income countries will reach a high of $630 billion in 2022, following an almost record recovery of 8.6 percent in 2021.[4] At the same time, the average cost of sending $200 to lower and middle income countries was estimated to be as high as 6 percent in the fourth quarter of 2021, double the Sustainable Development Goal target of 3 percent by 2030.[5] These costs reduce in tangible and measurable ways the impact of money being sent to populations for which literally every dollar matters. Digital assets like XRP can help solve these problems based on its speed, scalability, energy efficiency, and cost.

Digital wallets

It is worth noting that one of the bigger drivers of financial inclusion over the past decade has been the rise of financial services from outside the banking sector, including

[3] In announcing the final rule that would revise the Electronic Fund Transfer Act ("EFTA") as it relates to remittance transfer providers, the Consumer Financial Protection Bureau stated it "believe[d] that expanded adoption of … Ripple's suite of products could … allow banks and credit unions to know the exact final amount that recipients of remittance transfers will receive before they are sent" contrary to the current state of play. *See* 85 Fed. Reg. 34870, 34880 (final rule); *see also* 84 Fed. Reg. 67132, 67142 (proposed rule).

[4] World Bank, Remittances to Reach $630 billion in 2022 with Record Flows into Ukraine (May 11, 2022).

[5] *Id.*

digital wallets. These services are pioneering new offerings and alternative experiences for traditional banking users. The creation of digital wallets offer consumers ownership of digital assets and allow for a faster and more efficient method of distribution of money.[6] Digital wallets that enable payments, whether made domestically or cross-border, without requiring a bank account could succeed in promoting financial inclusion for the unbanked and underbanked population, which may not be adequately served by the traditional banking system.

Energy efficiency and environmental use cases

As we continue to experience the severe impacts of climate change, it is critical to understand how digital asset technologies and services can be leveraged to increase economic activity and achieve goals like financial inclusion without putting additional strain on the environment. Globally, the damages from climate change are projected to amount to almost 3% of GDP by 2060.[7]

Ripple strongly believes, however, that digital assets can be compatible with a low-carbon economy that emphasizes renewable energy and reduces its environmental footprint. As an example of how digital assets can align with climate change goals, in 2020, Ripple partnered with Energy Web (EW) and the Rocky Mountain Institute (RMI) to decarbonize public blockchains — starting with the XRP Ledger, the first major global blockchain to do so.[8] Ripple as a company has also pledged to achieve carbon net zero by 2030 or sooner.

Additionally, Ripple is a supporter of the Crypto Climate Accord[9] (CCA) — an initiative organized by EW, RMI and the Alliance for Innovation Regulation (AIR) focused on decarbonizing cryptocurrencies to ensure the global financial system is less harmful and more sustainable. Key objectives of the CCA, which counts over 200 companies and individuals as supporters,[10] include:

- Enable all of the world's blockchains to be powered by 100% renewables by the 2025 UNFCCC COP Conference
- Develop an open-source accounting standard for measuring emissions from the cryptocurrency industry
- Achieve net-zero emissions for the entire crypto industry, including all business operations beyond blockchain and retroactive emissions by 2040

[6] Wallets are the leading e-commerce payment method in several Asian countries; a McKinsey survey reported that more than 70% of respondents said they use digital wallets. Sustaining digital payments growth: Winning models in emerging markets (October 13, 2022).
[7] OECD, Economic interactions between climate change and outdoor air pollution at 3 (July 3, 2019).
[8] https://ripple.com/ripple-press/ripple-leads-sustainability-agenda-to-achieve-carbon-neutrality-by-2030/.
[9] https://cryptoclimate.org/.
[10] https://cryptoclimate.org/supporters/.

While many currencies (whether digital or physical) are not environmentally friendly, the XRP Ledger processes transactions through a unique "consensus"[11] mechanism that consumes negligible energy. Specifically, the XRP Ledger utilizes a distributed agreement protocol which establishes super-majority agreement, or consensus, around a given transaction without the need for energy intensive mining characteristic of other digital assets. Further, XRP itself was designed with sustainability in mind; it is an inherently green currency. All XRP is already in existence, meaning no unsustainable mining practices or additional energy is ever required to produce more.

Finally, as OSTP researches the climate impact of digital asset-related technologies and services, there is an emerging consensus among digital asset industry members and climate advocacy organizations that blockchain is an important, potentially transformative technology with respect to helping global carbon markets modernize and scale to accelerate progress toward globally agreed climate goals (e.g., the Paris Agreement).

Blockchain's native characteristics make it a natural fit to address persistent pain points in carbon markets, including unclogging supply bottlenecks, reducing time to market for carbon credit producers, and bringing about dramatically higher transparency and data integrity. Blockchain can also help enable fairer price discovery and deliver a more equitable return to those engaged in high quality carbon removal activity (i.e., additive, permanent, verifiable removals). Finally, blockchain can improve the tracking and tracing of carbon removal activity and carbon market transactions, making it easier for buyers to meet their ESG commitments and both shareholder and regulatory reporting requirements.[12] Far from exacerbating global emissions problems, blockchain can help solve them by creating a more powerful market infrastructure to accommodate the needs of both suppliers and buyers of carbon credits.

R&D that should be prioritized for digital assets

Each of the above identified areas where digital assets have the potential to provide significant value to the public and warrant further focus and study by OSTP. Additionally, we would highlight the following technical areas as worthy of attention by OSTP:

- *Custody:* Regulated institutions and their technology partners having been practising key management for over 20 years, whereby they or the associated system issue a key and can reissue where required. Standards and practices will need to be extended that remove risk from this process when leveraging keys

[11] David Schwartz, The Environmental Impact: Cryptocurrency Mining vs. Consensus (July 8, 2020).
[12] For example, Ripple has partnered with Xange, a climate focused fintech backed by the UN, which is building its carbon credit verification, tokenization and exchange functionality on XRPL. Xange chose to build on the XRP Ledger given its performance, scalability and inherently green attributes. Key focus points of Xange.com include the prevention and mitigation of illicit financial transactions and on carbon emission initiatives using blockchain technology to bring transparency to carbon accounting by avoiding double counting of emission reductions or removals.

generated by a public ledger allowing recoverability, ensuring the highest levels of security are maintained whilst preventing a user from being barred access to an asset or account in the event of a key loss or issue.

- *Identity and Privacy:* Identity and privacy are tightly coupled and can greatly impact the user experience. Existing proxy identifiers such as cell numbers or email addresses can be used to create a better identity framework for end users, however clear standards and possible technology developments need to be introduced to ensure this does not compromise privacy when a public ledger is leveraged. Consideration should also be made against existing privacy frameworks or standards and the ‘right to be forgotten.’ This becomes harder in a world where there are public ledgers and data is immutable, but needs to be taken into account with any new standards or changes to existing frameworks.

- *Interoperability:* Standards currently exist for the transfer of data related to a payment transaction (e.g., ISO 20022). These can be utilised (where appropriate) to provide a consistent format for passing data between participants and also where existing systems require data in order to record transactions correctly and ensure any compliance or regulatory frameworks can be adhered to. New protocols or standards may be required to pass this information between parties to remove all information being shared on a public ledger while ensuring that the benefits of the settlement model enabled by blockchain technology are still realized.

- *Participation / Security:* Unlike traditional centralised systems where there are clear governance and participation standards and rules, new standards will need to be developed to accommodate a distributed or decentralised approach which incorporates roles and responsibilities for running the network, service level agreements and network updates. Approaches to additional innovation such as programmability will need to be clearly defined so that any introduction of changes is carefully managed whilst ensuring the impact of these is maximised without compromising the integrity of the network. Standards will also need to be defined as to who can perform the various roles to ensure bad actors are not able to compromise the integrity of the network.

Opportunities to advance responsible innovation in the broader digital assets ecosystem

In addition to directly advancing R&D in digital assets, their underlying technology, and relevant applications, responsible innovation in the United States can also be furthered in other ways. First, establishing a clear regulatory framework for digital assets and digital asset ecosystem participants would be a monumental step toward ensuring responsible innovation remains onshore in the United States and is not driven to other countries. While not within OSTP’s direct remit as related to digital asset R&D, the provision of clear jurisdictional boundaries for regulators and establishment of common sense rules for businesses would help foster responsible U.S. innovation, which OSTP should support.

There is perhaps no greater obstacle to U.S. digital asset businesses' global competitiveness than the current U.S. regulatory landscape. To date, federal agencies have deployed what can only be described as an uncoordinated, piecemeal approach to regulation.[13] Positions at times conflict, jurisdictional boundaries are unclear, and rules are subject to constant change, often with inadequate input from stakeholders.[14] The resulting ambiguity makes it difficult, if not impossible, for U.S. digital asset companies to operate effectively given the constant threat of enforcement action from multiple federal authorities.

By contrast, several foreign jurisdictions have now established comprehensive frameworks with respect to digital assets, including Singapore (the Payment Services Act) and the European Union (Markets in Crypto-Assets Regulation). These laws, among other things, establish taxonomies covering cryptocurrencies and stablecoins, create clear oversight regimes, and seek to protect consumers from the risks associated with digital assets. Other jurisdictions taking meaningful steps toward establishing credible, comprehensive regulatory frameworks include the UK,[15] Australia,[16] and Brazil.[17]

While President Biden's Executive Order is a welcome first step toward establishing a clear path forward on the regulatory front, the United States must act now or else risk ceding its place as a digital assets leader to other jurisdictions. Like its foreign counterparts, the United States should move decisively in establishing a holistic framework governing digital assets, drawing upon the knowledge of industry and other market participants in doing so. Regardless of how much R&D in the technology or applications for digital assets is done, failure to resolve the regulatory gaps means risking the migration of U.S. talent, investment, and innovation offshore to jurisdictions that have not only declared their openness to the digital assets industry, but demonstrated their willingness to nurture and encourage development of the same.

---

[13] An October 2020 report from the Department of Justice named at least seven federal agencies with some sort of regulatory authority over digital assets. Department of Justice, Cryptocurrency: Enforcement Framework at 22. Additional agencies are named in President Biden's Executive Order.

[14] *See* Hagerty, Colleagues Push Back on SEC's Back-Door Attempt to Restrain Crypto Market.

[15] https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets.

[16] https://treasury.gov.au/sites/default/files/2023-02/c2023-341659-cp.pdfhttps://treasury.gov.au/sites/default/files/2023-02/c2023-341659-cp.pdf.

[17] https://www.coindesk.com/policy/2022/12/22/brazils-president-signs-crypto-regulations-into-law/.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Sardine

Sardine is pleased to respond to the Digital Assets R&D Agenda for the Office and Science of Technology Policy.

About Sardine

Sardine is a fraud prevention and payments company specializing in cryptoassets and digital assets. Clients like Coinbase, Blockchain.com, and DeFi projects like Metamask and wallets like Ledger rely on Sardine to be the most effective tool to detect and manage fraud risks associated with digital assets. Sardine is headquartered in Miami, FL, employs 90 people, and recently raised a $51.5m Series B led by Andreessen Horowitz.

This experience has taught Sardine where the risks are for our clients (exchanges, wallets, VASPs, and CASPs). Sardine, therefore, has a unique dataset of the market, an understanding. of the key risks and potential harms but also the benefits for consumers, businesses, the economy, and the wider opportunities for government to enhance its R&D agenda.

Additionally, Sardine, in Q2 2023, will launch an industry utility to share data about on-chain and off-chain (cryptoasset, digital asset, and traditional financial services) risks like fraud and AML. Sardine has a patent pending for its approach to tying on-chain and off-chain data to an individual citizen or entity in a way that preserves privacy.

Sardine would be delighted to follow up with the OTSP or government colleagues at their convenience.

RFI Question 1: Goals or applications that could be improved with digital assets or related technologies.

Cross border payroll
One area where value is already provided to the public is international payroll. During the pandemic, US businesses must pay US nationals, and non-resident employees cross border. This helps make US businesses more competitive in a global marketplace, but using the existing financial system is highly expensive and challenging. An employee can easily be paid into a US bank account, but often getting that cash to spend it where they reside may take weeks and cost up to 10%.

Data from the Payroll platform company Deel says that 5% of their users currently use Bitcoin and dollar-backed Stablecoins (like USDC) to receive their paycheck. They also note that demand is much higher than 5%, but many payroll platforms have not widened their offering due to security and regulation concerns. Note, Sardine sells KYC, AML, and fraud prevention solutions and sees substantial pipeline demand for this offering to be made more compliant from both payroll platforms.

Financial inclusion
Stablecoins or a CBDC can be the same as cash. A CBDC, in particular, may help solve the grey economy and low-income sectors that remain stubbornly reliant on cash. Manual labor workers often have limited job security and rely on cash for savings. With un-even income patterns, they often struggle to receive formal rental or credit contracts and may have no permanent address. They exist “outside the system” to some extent.

An example where this worked well is Brazil’s PIX payment system or India’s UPI. By creating a universal, accessible, and standard payment system free for the smallest merchants, they achieved transformational growth in digital adoption. Neither system is a CBDC, but the factors that created their success are lessons for an R&D agenda. This “acceptance of the informal market” is a pragmatic policy that achieved a net positive outcome while limiting overall risk to the system by creating sensible limits on the values that can be transferred before formal KYC is required. Note that the government sets KYC and AML thresholds and levels but must be implemented by the wallets.

Click here for a full, longer read on the future of wallets by Sardine head of content Simon Taylor (written in a personal capacity but relevant to this R&D agenda)

Ticketing and Memorabilia
The concert and event ticketing sector has seen limited innovation, with recent moves considering anti-trust to increase competition. However, digital assets present a form of “ticket ownership” where the consumer is given more control over their ticket. Innovators can also use the ticket to add new functionality.

Today an NFL or NBA franchise has no easy way to send a message to everyone who attended a memorable game at the end of the season or a music artist to everyone who attended their concert. But if those consumers had a digital ticket (like an NFT or Non-Fungible Token), they could send messages, exclusive content, or discounts to future events. Brands like Nike and Starbucks continue to invest and innovate in this space because it creates new forms of consumer engagement.

RFI Question 2: Goals or sectors that introduce harm.

Scams
An unfortunate consequence of the cryptoasset price increase through 2021 was that consumers became especially vulnerable to scams involving digital assets. Fraud in the sector grew by more than 70% in a year, as consumers with limited knowledge were encouraged by

scammers to use cryptoassets to send money. At Sardine, we often see that scams involving fake invoices, elderly, romance, or phishing may end in the fraudster encouraging the victim to send money via cryptoassets.

Compared to traditional technologies, cryptoassets are an irreversible push payment type that fraudsters use to move money off-shore and across borders. Users are encouraged to open "self-custodial" wallets and avoid the use of centralized exchanges (like Coinbase) that have fraud controls in place and require KYC (for beneficiary and sender under FATF R16 and FinCen guidance).

Theft

The programmable nature of digital wallets in cryptoassets means users can be tricked into clicking a link that can drain their wallet. Users can approve smart contracts (software automatically interacting with assets). This emerging attack vector is being mitigated in two ways by the industry. 1) Wallets voluntarily create warnings for users, and 2) Other initiatives for well-known and established smart contract protocols (e.g., DeFi projects like Compound and Uniswap) are considering standards for certificates and audits. Certificates could work similarly to HTTPS for web browsing but for audited and approved smart contracts.

RFI Question 3: Federal research opportunities could be introduced with digital assets.

Fraud prevention data sharing

The US has no mechanism for cryptoasset businesses or digital wallets that support cryptoassets to support fraud and AML information sharing. Sardine is launching an industry utility to close this gap with early members, including companies such as Coinbase, Blockchain.com, Visa, Experian, banks, and large Fintech companies like Airbase and Novo.

Sardine is in active conversation with FinCen to build this under GBLA compliance and in full accordance with the patriot act to ensure the data can be shared and privacy risks managed accordingly. An opportunity for federal research might be to understand how emerging standards (like IVMS1010), and new technologies (like device and behavior biometrics) can create orders of magnitude improvements over traditional approaches to fraud and AML (namely, KYC and transaction monitoring).

Sardine's patent-pending approach to building a risk model for a single citizen or legal entity that is privacy enhancing may be particularly valuable to the OTIS R&D agenda for CBDCs and broader standard-setting agenda.

The goal will be to provide a single platform and dashboard for the industry to collaborate on fraud, credit, and AML risk. Sardine invites OTIS to evaluate the SardineX approach and understand how this impacts the R&D agenda.

Regulatory oversight (Supervisory Tech)
For cryptoassets, tokenized real-world assets, and a future CBDC, the transparent nature of DLT lends itself to supervisory policy objectives but raises privacy implications. In the existing financial system, financial institutions, MTL-licensed entities, and Fintech companies must KYC their customer and collaborate with government agencies in the event of risk. However, this task is not aligned with existing regulatory reporting requirements or the suspicious activity report (SAR) process.

Regulators see conflicting information in the form of PDFs and CSVs and have a limited window on both market and systemic risk. At its best, DLT is an auditor. It can confirm the state of a transaction has been agreed upon by multiple stakeholders and provides cryptographic proof a given fact is still true. The implication of this (with advanced new technology like federated machine learning) could allow a much more digital approach to supervision, but that would require broad coordination by government agencies. Each agency is limited by its mandate, perimeter and privacy constraints as set by law. However, whether it is a consumer, compliance officer or supervisor, they're querying the same underlying data.

Regulatory think tanks like AIR (Alliance for Innovation in Regulation) are running tech sprints to demonstrate how this can work in practice. The challenge of government is providing an incentive for the private sector to invest in and commercialize these opportunities when historically, government procurement has been exceptionally challenging to access.

This suggests areas of opportunity for R&D

1. Investigating the use of DLT and Federated learning for enhanced supervision (e.g., Proof of reserves and disclosures in cryptoassets)
2. Developing alternative mechanisms for the procurement of innovative technologies (perhaps involving non-profits)
3. Investigating further the work Sardine is doing under fraud data sharing (per the previous answer)

RFI Question 4: R&D that should be prioritized.

The role of wallets
"Wallets" are becoming central to consumers' financial lives. Venmo, CashApp, and Zelle potentially offer a multi-asset private sector alternative to the traditional bank account, and the Apple Wallet is playing a larger role in consumer identity. Wallets are at the front line of managing consumer harm and risk, and any standards or approaches to managing these risks would be a compelling area for R&D.

RFI Question 5: Opportunities to advance innovation more broadly.

Cryptoasset standards
The OTSP should actively investigate what standards the US should support and how best to do so.

- **AML:** Numerous standards have emerged in the past decade as the industry has evolved, like IVMS101 (a standard for VASPs and CASPs to share sender and recipient information to prevent AML securely). *R & D opportunities include how this could work in a DeFi context without breaking its underlying privacy and security model.*

- **Emerging standards** exist for cryptoasset custody and smart contract audit. *An R&D opportunity might be to do a landscape assessment of these standards and partner with the industry to create a standard that benefits from digital technology and can be widely adopted.*

- **Standard harmonization:** One of the largest frustrations for the industry is the inconsistency of regulations and policies at the global level. *As a global leader, the US has an opportunity to set the policy objectives but also have these managed through G20 and OECD and pushed to become a global standard (much like it has with AML or accounting standards).*

- **Institutional standards:** In private markets, there are also attempts by large global FIs to develop standards such as GFIC (Global Financial Institutions operating in Cryptoassets), Digital Custody, and attempts at self-regulation like the GDCA.

Leveraging global best practice

Organizations such as Global Digital Finance allow regulators to discuss challenges they're seeing in the "reg-only forum" but also provide a way for the industry to respond to challenges supervisors see. A similar initiative for technology and R&D could be a compelling development. Global Digital Finance is in addition building an "Open Standards Council"

RFI Question 6: Other information that should inform the R&D Agenda

The true properties of digital assets
The OTSP must recognize what distinguishes digital assets from traditional financial services and other technologies. Confusion about these properties can lead to bad outcomes for

consumers, the government, and the economy. Well-meaning practitioners often support or criticize the technology without understanding it from first principles.

Other technologies may have some of the same properties, and these properties can be removed or managed from digital assets. However, no other technology can offer all 6 in combination.

Digital assets are (or could be).

1. **Default global:** The technology is available to anyone with an internet connection at its basic level. This has led to humanitarian agencies like the UN looking to use it to disperse aid to Ukraine and see digital assets used as a way for consumers to donate directly to causes. Contrast with traditional financial technology, which always has a jurisdiction or home location.
2. **Default 24/7:** Modern financial infrastructure can be 24/7; the existing system moves as slowly as the slowest participant or system. For example, SWIFT member banks can now move money cross borders in real-time, but many banks have not upgraded their systems or processes to cope. Digital assets are born to be 24/7 and global.
3. **Default transparent:** Every transaction is a matter of public record and cannot be deleted. For this reason, law enforcement has been able to investigate and prosecute crimes substantially more effectively than the opaque existing financial system. This raises privacy implications but could be a significant upgrade to create a "golden source of truth" for the financial system(s). While the Federal Reserve may not know the precise amount of dollars in circulation, a Stablecoin issuer does (and so does any observer of a DLT network).
4. **Default Programmable:** Digital assets can include automation in the asset or smart contract enabling new functionality. This could include simple use cases of digital cash that can automatically pay sales tax for merchants to more complex use cases like automating multi-party contracts in financial markets (like ISDA-based interest rate swap agreements)
5. **Default Permissionless:** Anyone can create a wallet or interact with the infrastructure (and write code).
6. **Default Composable:** Most smart contracts can be called by other smart contracts and used to make a higher-level system. Much as two wheels and a box are "composed" to create a car picture, a stablecoin + a trading platform + a pricing protocol can quickly create a decentralized lending market. This could solve major interoperability problems if the infrastructure is permissionless and composable by default as designed by a CBDC and then limited by wallets or the private sector to a given use case.

One key consideration for R&D is how a software engineer can easily create code with positive intent but may create consumer harm they are naive to. There is no simple "GitHub repository for regulation." Such an initiative would be a powerful challenge for non-r

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Satoshi Action Education

Bottom-up Bitcoin research priorities and researcher capacity-building

Submission to the Office of Science and Technology Policy – RFI response (88 FR 5043)

Dennis Porter

President & Founder

Satoshi Action Education

[redacted]

SATOSHI ACTION EDUCATION

Introduction

The Federal Government is developing a National Digital Assets Research and Development Agenda and recently posted a request for information (RFI) soliciting public comments to help identify priorities for research and development related to digital assets.

This response, submitted by Satoshi Action Education, focuses on research and development priorities for Bitcoin. In particular, our focus is on energy, social, and environmental research needs in the USA-based Bitcoin mining space, and on the process of undertaking policy-salient transdisciplinary Bitcoin research (i.e., involving collaborative, cross-disciplinary, and cross-sectoral engagement that incorporates the experiences and practical knowledge of industry and local stakeholders).

Satoshi Action Education is a 501(c)(3) non-profit dedicated to researching Bitcoin and the Proof-of-Work consensus mechanism. This response was prepared by Dr. Murray Rudd (https://orcid.org/0000-0001-9533-5070), a former environmental economics and policy professor, now a Science Advisor for Satoshi Action Education.

Our comments, while having implications across RFI topics, are specifically aimed at Topic 4, R&D that should be prioritized for digital assets. In this RFI response, we draw on Dr. Rudd's recent publication (Rudd, 2023) and want to highlight further Bitcoin research agenda prioritization efforts that Satoshi Action Education is now facilitating. While the results from that process will not be ready prior to the RFI submission deadline, they should be available within a few months for government agencies seeking further industry-oriented perspectives about USA-specific Bitcoin research priorities.

Bitcoin research needs

Rudd (2023) recently outlined 100 potentially important research questions relating to Bitcoin's production, adoption, and impacts. That exercise, a first step in refining and articulating a Bitcoin-oriented research agenda, drew on some 88-hours of transcripts from interviews with Bitcoin experts with diverse expertise on energy use and environmental, social, and governance impacts. A partial selection of questions most salient for Bitcoin mining is included below.

Bitcoin energy use – the big picture

How much of the world's currently wasted and stranded energy could be used for Bitcoin mining without increasing CO2e emissions?

How will Bitcoin mining affect the flow of investment funds to renewable energy infrastructure, beyond what would happen through organic growth in renewable energy demand?

SATOSHI ACTION EDUCATION

Mitigating methane emissions

How much methane can be mitigated by Bitcoin mining operations co-located with oil and gas wells?

How could Bitcoin mining be used to most effectively reduce methane emissions from landfill sites and agricultural operations?

Electricity grid transition

How does the addition of Bitcoin mining affect the economic viability, net carbon emissions, and risk profile of electricity grids transitioning to renewable energy?

How do mandates about grid objectives and management responsibilities vary, and when and how can different types of Bitcoin mining strategies best help fulfill those mandates?

How does Bitcoin mining affect electricity grid resilience in the face of extreme weather events or other shocks?

Bitcoin mining – site choices and costs

What is the marginal abatement cost of reducing greenhouse gas emissions by Bitcoin mining and how does that compare to other mitigation options?

How can waste heat from Bitcoin mining best be used as a resource for other purposes?

Retail, institutional, and national Bitcoin adoption

How will the adoption of Layer 2 technological advances (e.g., Lightning Network's capacity to bundle and process small bitcoin transactions off-chain) affect Bitcoin's electricity consumption and ESG performance?

What are the economic and ESG opportunity costs for nations not adopting Bitcoin?

Governance

How do different government regulatory and non-regulatory intervention options affect Bitcoin mining profitability and behavior?

When and how might Bitcoin mining and adoption be strategically supported by governments in order to build prosperous national and regional economies resilient to external shocks?

Adaptive Capacity

How does Bitcoin adoption affect resiliency and adaptive capacity of households, communities, firms, and governments?

Narratives

How and why do organizations with differing worldviews and core values cooperate to advance or oppose Bitcoin mining and adoption?

To what extent do Bitcoin critics and advocates have undisclosed conflicts of interests that would compromise the credibility and legitimacy of their messaging?

Knowledge creation and communication

How can Bitcoin research results be framed and disseminated to ensure that key findings are available for integration in international energy and climate change syntheses?

What resources could best help communications professionals to ensure the veracity of their reporting on Bitcoin's energy use and ESG impact?

Social issues

How does Bitcoin mining and adoption influence human migration, rural regeneration, and regional economic development?

The questions outlined above provide a preliminary snapshot of some of the research needs explicitly or implicitly raised in interviews with Bitcoiners. The paper highlighted:

- the need to consider the net impact of Bitcoin mining and adoption on carbon emissions;
- the potential for Bitcoin mining to contribute rapidly to mitigation (especially via mitigation of methane emissions); and
- Bitcoin's potential in improving the economic viability of renewable energy facilities and speeding the build-out of renewable infrastructure needed for the coming energy transition.

Satoshi Action Education has initiated further policy-oriented research to better articulate Bitcoin mining-oriented research needs in the USA. Rudd's 100 research questions are being used as a baseline from which to collaboratively winnow and refine Bitcoin research questions that would, if answered, support North American policy-makers', investors', and research funders' decision-making.

SATOSHI ACTION EDUCATION

Credible evidence is necessary for informed decision-making about the economic, social, and environmental impacts of Bitcoin mining and adoption in the USA. Peer-reviewed evidence, however, is generally not yet sufficiently available (or credible) to support informed policy decisions: research that is truly transformative needs to be scientifically credible, socially relevant, and policy-salient (Figure 1).

In the Bitcoin field, where expertise from across academic disciplines and sectors will be required to produce new knowledge, this suggests that transdisciplinary processes (Hirsch Hadorn *et al*., 2006; Pohl, 2008) will be needed. Substantive transdisciplinary research engagement has the potential to help better define research needs, expand the bounds of the set of credible evidence, and both help remedy factual errors and facilitate the co-creation of new knowledge unavailable through traditional siloed approaches.

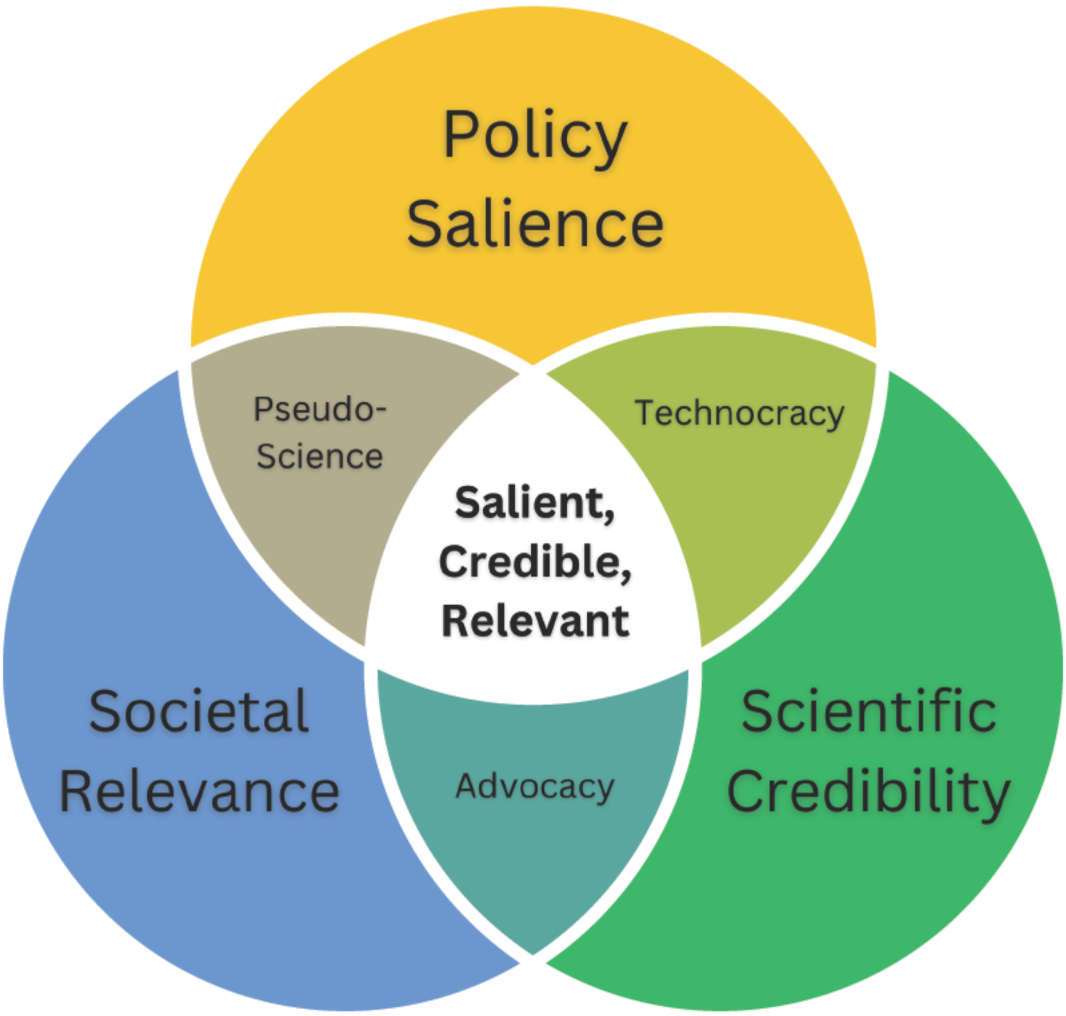


Figure 1 – Scientifically credibility, societal relevance, and policy-salience are all needed for transformative research that serves society's interests. Venn diagram adapted from Sutton & Rudd (2016) and based on Cash et al. (2003).

SATOSHI ACTION EDUCATION

The boundaries between sets are, in reality, fuzzy. In the past, academic researchers have marginalized many industry experts (and, of course, local and traditional knowledge holders even more so), maintaining tight bounds on the set of accepted scientifically credible knowledge. Expanding the scope of credible evidence by engaging industry and local research partners and non-academic experts can help increase the quality and quantity of the transformative research 'sweet spot.' Likewise, better engagement by scientists with the public and with policy-makers opens up opportunities for further expanding the scope of transformative, co-produced Bitcoin research.

This new Satoshi Action Education initiative involves:

1. using a virtual working group, comprised of a mix of industry participants, government officials, and academics, to narrow and refine the 100 Bitcoin questions into a more compact list of research priorities focusing on North American Bitcoin mining and adoption; and
2. conducting follow-up interviews with public sector and elected officials to help identify research needs that contribute most rapidly and substantively to informing public policy, regulation, and investment (i.e., identifying the 'low-hanging fruit,' the important questions that are most feasible to fund and implement in the near-term).

Bottom-up approach to identifying and prioritizing research needs

While the cryptography research underlying Bitcoin has a history going back to the 1980s, much of the recent academic literature on Bitcoin focuses on time series pricing models. There have been no large Bitcoin cross-disciplinary, funded research projects in academia that have studied the broad implications of widespread mining and adoption. There are not any established Bitcoin research epistemic communities in place because research is in such an early stage. Similarly, Bitcoin expertise within government agencies is limited.

The deep expertise on Bitcoin currently exists within the Bitcoin industry. The speed of development thus makes it challenging for academics, government agencies, and research funders to develop research priorities with a top-down approach (e.g., high-level foresight working groups, Grand Challenge reports, blue-ribbon panels, etc. – see Hicks, 2016, for a history of Grand Challenges in the USA) and highlights the importance of instead using a bottom-up approach.

Bottom-up horizon scanning efforts (Sutherland & Woodroof, 2009) have been used extensively to identify research needs in the environmental sciences over the past 15-years. Two main types of bottom-up exercise fall under the 'horizon scanning' rubric:

1. annual horizon scans of emerging issues with potentially high impact (e.g., Sutherland *et al.*, 2013a; Herbert-Read *et al.*, 2022; Sutherland *et al.*, 2023); and
2. 'key questions' exercises that identify policy-salient, intermediate-term research needs for a particular field (Sutherland *et al.*, 2009; Pretty *et al.*, 2010; Boxall *et al.*, 2012; Sutherland *et al.*, 2013b; Foulds et al., 2022) or within particular regions (Fleishman *et al.*, 2011; Rudd et al., 2011; Kennicutt *et al.*, 2014; Rudd *et al.*, 2018; Fairbrother *et al.*, 2019).

The methodology is well-established (Sutherland *et al*., 2011) and these exercises provide benefits beyond the lists of important research needs they produce. For example, collaborative key questions working group research can: help increase legitimacy and buy-in from industry (increasing compliance and reducing transaction costs of policy interventions); increase the credibility of research results; reduce values-laden policy contestation and allow for smoother policy implementation; and facilitate communication and collaboration across sectors and disciplines, helping to lay the groundwork for future transdisciplinary research. Further, survey research can be used to follow-up and quantify how priorities vary across regions or epistemic communities (Rudd *et al*., 2014; Rudd & Fleishman, 2014; Rudd, 2015), and for syntheses across key questions exercises that can help identify or quantify approaches for bridging the science-policy interface (Rudd, 2014; Wisz *et al*., 2020).

For the current American Bitcoin research prioritization process, Satoshi Action Education is structuring a tripartite effort with engagement from industry, academia, and governments. This structure is similar to a global key questions initiative inspired by Boxall *et al.* (2012) and implemented by the Society of Environmental Toxicology and Chemistry (SETAC) (Brooks *et al*., 2013). The SETAC initiative published results from five international research prioritization exercises (Furley *et al*., 2018; Van den Brink *et al*., 2018; Fairbrother *et al*., 2019; Gaw *et al*., 2019; Leung *et al*., 2020) and had substantial academic and policy impact.

Currently, the first step in the Bitcoin research prioritization exercise (Rudd, 2023) is complete and, after the next step, the Satoshi Action Education initiative should result in publication of another article focusing specifically on Bitcoin research needs in the USA. While beyond the mandate of Satoshi Action Education, note that our approach has the potential to be used as a template for international research on Bitcoin (or digital asset) research prioritization. International Bitcoin adoption could have important impacts on regional renewable energy transitions, poverty alleviation, household and regional adaptive capacity, and human rights (Gladstein, 2022; Hallinan *et al*., 2023; Rudd, 2023), all issues with international development and security implications for the USA.

---

1 Networks of knowledge-based experts who share: normative beliefs regarding the rational for social action; causal beliefs commonly held within their research domain and which link policy action and outcomes; notions of what comprises credible knowledge; and views on policy practices or interventions that enhance societal well-being (Haas, 1992).

2 The US EPA played a key role in both the research (core team member G.A. Ankley) and funding roles for the SETAC initiative.

3 The Rudd paper was an expansion of an optional first phase for key question exercises, in which interviews with thought leaders set the scope for subsequent working group collaborations prioritizing research needs.

SATOSHI ACTION EDUCATION

Using Bitcoin key questions results for high-level research prioritization

We envision our work at Satoshi Action Education as providing support for high-level decision-making processes relating to digital asset research priority setting and funding, not as an end in itself. All of our results will be published in peer-reviewed journals and Satoshi Action Education staff will be available to address questions about our process and/or results.

Having a list of Bitcoin-oriented research priorities will, we hope, help decision-makers to better understand and immediately eliminate poorly conceived alternatives from the pool of candidate policy solutions (e.g., Rigby, 2005) and/or identify research needs that help build knowledge about policy solutions on which consensus might be possible (e.g., Lawton and Rudd, 2016). Key question exercises can sensitize decision-makers to emerging challenges, helping them to take informed decisions when the need arises.

Recommendations

- **Take full advantage of industry expertise by pro-actively engaging firms and individuals with data and/or high levels of expertise in future Bitcoin research design, implementation, reporting, and policy analysis**

Widespread Bitcoin production and adoption in the USA raises important questions across a range of academic disciplines and with implications across a variety of industrial sectors and government agencies. Given the recent emergence of Bitcoin, top-down research prioritization needs to be supplemented by the bottom-up participation of industry in shaping and defining a research agenda, and in the co-creation and communication of new knowledge. Satoshi Action Education is facilitating the next step in the process but over the long-term, this process will require pro-active engagement and outreach by established knowledge creators, agencies, and funders. Further, technical and funding support will also be needed for the long-term efforts needed to establish trust, common language, and collaboration among transdisciplinary research participants (Pennington *et al*., 2016).

- **Encourage, facilitate, and fund credible scientific research that takes account of the broad social and environmental impacts of Bitcoin mining**

Bitcoin mining and adoption has the potential to impact many different parts of the energy system in the USA. Early academic research critical of Bitcoin mining has been very narrowly focused on direct energy use, often ignoring either the realities of mining (see point 3) or the potentially positive impacts on energy use and carbon emission reduction in other systems. Bitcoin research needs to take a wide view on the net impacts of mining or, at a minimum, frame tightly-focused research results within the wider context.

Bitcoin production and adoption should properly be conceived of as part of a newly emerging complex system. From a research perspective, this would imply adopting a coupled human-natural system (Liu et al., 2007) or socio-ecological systems (Ostrom, 2009) approach, accounting for interactions across geographic scales in the USA and beyond, and accounting for interactions among energy, ecological, technological, social, and governance systems. There are abundant opportunities for undertaking real-world policy experiments, exercises in adaptive governance (Chaffin *et al*., 2006), to accelerate knowledge creation about Bitcoin's impact on system dynamics and how its technological/financial innovation affects societal well-being.

- **Critically vet academic information that is used to inform policy-making and regulatory decisions**

In the nascent Bitcoin research space, several high-profile academic papers have made wildly uninformed assumptions about how Bitcoin mining works (Mora *et al*., 2018, being the most obviously egregious example). Despite peer-reviewed critiques (Houy, 2019; Masanet *et al*., 2019), such work continues to be cited in academic articles and policy reports (e.g., OSTP, 2022). Given the current sparsity of academics with real-world Bitcoin experience, the challenges currently plaguing the current peer review process (Dance, 2023), and the opaque nature of editorial processes at some high-impact journals, industry actors now view the academic peer review process as fundamentally flawed. Until such time as there is sufficient expertise within academia to credibly edit and review cross-disciplinary Bitcoin research, we suggest that government agencies (1) use contracted professional peer review consultants or expert panels to vet academic Bitcoin research and (2) allow for industry and public input prior to that research being considered credible enough to be used to inform policy decisions.

- **Establish capacity and pathways for incorporating Bitcoin research work packages into large energy and environmental research funding opportunities**

The modern energy and environmental science enterprise involves high-level research priority setting and funding, the establishment of focused funding opportunities for research projects that align with high-level goals, and, within projects, prescriptive and accountable scientific activities and training programs. The little Bitcoin research that currently is undertaken is virtually all ad hoc and independent, outside the established energy-environment mainstream. We recommend that efforts be made to help Bitcoin researchers build capacity for engagement in modern research projects – for example, efforts that can help early-career researchers to create or contribute to Bitcoin-oriented research work packages within larger energy and environment-oriented research projects and programs. That could involve diverse efforts such as, for example, Bitcoin awareness-building opportunities for senior researchers who are likely to lead large research proposals, and targeted funding for transdisciplinary research planning and synthesis grants that connect industry, government, and academic researchers.

SATOSHI ACTION EDUCATION

- **Ensure Bitcoin experts have opportunities to participate in high-level international research syntheses**

Bitcoiners believe that mining and adoption hold great potential to contribute substantively to climate change mitigation efforts, particularly in the near-term by reducing methane emissions. Bitcoin has not yet, however, managed to get on the radar screen for the large international syntheses (i.e., IPCC, IEA) that play a crucial role in articulating potential solutions that can help reduce the current carbon emissions gap.

Part of the solution obviously has to be based on results flowing from new research efforts on Bitcoin's impacts but there also needs to be means of flagging Bitcoin potential within high-level syntheses. This might involve, for instance, awareness building activities (e.g., side events at major international conventions) highlighting emerging research opportunities and their potential impacts, or the inclusion and active engagement of Bitcoin industry experts into the synthesis report writing process (with the recognition that their time is not covered by academic salaries).

Conclusion

We hope that the information from the Bitcoin key questions exercise will be timely and useful in the internal government discussions regarding digital asset research needs.

Our current initiative at Satoshi Action Education will extend research prioritization discussions within the Bitcoin space but there is an obvious need for a much broader program of research and knowledge mobilization in the future. Government support, facilitation, and funding will be necessary to help fully integrate existing Bitcoin expertise into the broader energy, climate, and social research space. This could help capture a variety of environmental and economic benefits within the USA, bolster American leadership in Bitcoin research, and have positive global externalities arising from methane mitigation, electrification in developing countries, and other associated social and economic benefits that may help bolster global democracy.

We welcome federal government participation within our efforts to refine Bitcoin research needs.

References

Boxall, A.B.A., Rudd, M.A., Brooks, B.W., Caldwell, D.J., Choi, K., Hickmann, S., *et al*. (2012) Pharmaceuticals and personal care products in the environment: what are the big questions **Environmental Health Perspectives** 120: 1221–1229. http://dx.doi.org/10.1289%2Fehp.1104477

Brooks, B.W., Ankley, G.T., Boxall, A.B.A. & Rudd, M.A. (2013) Toward sustainable environmental quality: a call to prioritize global research needs. Integrated Environmental Assessment and Management 9:179-180. http://dx.doi.org/10.1002/ieam.1411

Cash, D.W., Clark, W.C., Alcock, F., Dickson, N.M., Eckley, N., Guston, D.H., *et al*. (2003) Knowledge systems for sustainable development. **Proceedings of the National Academy of Science** 100: 8086-8091. https://www.pnas.org/doi/10.1073/pnas.1231332100

Chaffin, B. C., Garmestani, A. S., Gunderson, L. H., Benson, M. H., Angeler, D. G., Arnold, C. A., *et al*. (2016) Transformative environmental governance. **Annual Review of Environment and Resources** 41: 399-423. https://doi.org/10.1146/annurev-environ-110615-085817

Dance, A. (2023) Stop the peer-review treadmill. I want to get off. **Nature** 614, 581-583. https://doi.org/10.1038/d41586-023-00403-8

Fairbrother, A., Muir, D., Solomon, K.R., Ankley, G.T., Rudd, M.A., Boxall, A.B.A., *et al.* (2019) Toward sustainable environmental quality: priority research questions for North America. **Environmental Toxicology and Chemistry** 38:1606-1624. https://doi.org/10.1002/etc.4502

Fleishman, E., Blockstein, D.E., Hall, J.A., Mascia, M.B., Rudd, M.A., Scott, J.M., *et al*. (2011) Top 40 priorities for science to inform US conservation and management policy. **BioScience** 61: 290-300. https://doi.org/10.1525/bio.2011.61.4.9

Foulds, C., Royston, S., Berker, T., Nakopoulou, E., Bharucha, Z.P., Robison, R., *et al.* (2022) An agenda for future Social Sciences and Humanities research on energy efficiency: 100 priority research questions. **Humanities and Social Sciences Communications** 9: 223. https://doi.org/10.1057/s41599-022-01243-z

Furley, T.H., Brodeur, J., Silva de Assis, H.C., Carriquiriborde, P., Chagas, K.R., Corrales, J., *et al*. (2018) Toward sustainable environmental quality: identifying priority research questions for Latin America. **Integrated Environmental Assessment and Management** 14: 344-357. https://setac.onlinelibrary.wiley.com/doi/abs/10.1002/ieam.2023

Gaw, S., Harford, A., Pettigrove, V., Sevicke-Jones, G., Manning, T., Ataria, J., *et al.* (2019) Towards sustainable environmental quality: priority research questions for the Australasian region of Oceania. **Integrated Environmental Assessment and Management** 15: 917-935. https://doi.org/10.1002/ieam.4180

Gladstein, A. (2022) **Check Your Financial Privilege**. BTC Media, LLC, Nashville.

Haas, P.M. (1992) Introduction: epistemic communities and international policy coordination. **International Organization** 46: 1-35. https://doi.org/10.1017/S0020818300001442

Hallinan, K.P., Hao, L., Mulford, R., Bower, L., Russell, K., Mitchell, A. & Schroeder, A. (2023) Review and demonstration of the potential of bitcoin mining as a productive use of energy (PUE) to aid equitable investment in solar micro- and mini-grids worldwide. **Energies** 16: 1200. https://doi.org/10.3390/en16031200

Herbert-Read, J. E., Thornton, A., Amon, D. J., Birchenough, S. N. R., Côté, I. M., Dias, M. P., *et al.* (2022) A global horizon scan of issues impacting marine and coastal biodiversity conservation. **Nature Ecology & Evolution** 6: 1262-1270. https://doi.org/10.1038/s41559-022-01812-0

Hicks, D. (2016) Grand Challenges in US science policy attempt policy innovation. International Journal of Foresight and Innovation Policy 11: 22-42. https://doi.org/10.1504/ IJFIP.2016.078379

Hirsch Hadorn, G., Bradley, D., Pohl, C., Rist, S. & Wiesmann, U. (2006) Implications of transdisciplinarity for sustainability research. Ecological Economics 60: 119-128. http://dx.doi.org/10.1016/j.ecolecon.2005.12.002

References

Houy, N. (2019) Rational mining limits Bitcoin emissions. **Nature Climate Change** 9: 655-655. https://doi.org/10.1038/s41558-019-0533-6

Kennicutt, M.C.I., Chown, S.L., Cassano, J.J., Liggett, D., Peck, L.S., Massom, R., *et al.* (2014) A roadmap for Antarctic and Southern Ocean science for the next two decades and beyond. **Antarctic Science** 27: 3-18. http://dx.doi.org/10.1017/S0954102014000674

Lawton, R. N., & Rudd, M. A. (2016) Scientific evidence, expert entrepreneurship, and ecosystem narratives in the UK Natural Environment White Paper. **Environmental Science & Policy** 61: 24-32. https://doi.org/10.1016/j.envsci.2016.03.015

Leung, K.M.Y., Yeung, K.W.Y., You, J., Choi, K., Zhang, X., Smith, R., *et al*. (2020) Toward sustainable environmental quality: priority research questions for Asia. **Environmental Toxicology and Chemistry** 39: 1485-1505. https://doi.org/10.1002/etc.4788

Masanet, E., Shehabi, A., Lei, N., Vranken, H., Koomey, J. & Malmodin, J. (2019) Implausible projections overestimate near-term Bitcoin CO2 emissions. **Nature Climate Change** 9: 653-654. https://doi.org/10.1038/s41558-019-0535-4

Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M. & Franklin, E.C. (2018) Bitcoin emissions alone could push global warming above 2°C. **Nature Climate Change** 8: 931-933. https://doi.org/10.1038/s41558-018-0321-8

OSTP (2022) Climate and energy implications of crypto-assets in the United States. White House Office of Science and Technology Policy, Washington, D.C., 46 pp.

Ostrom, E. (2009) A general framework for analyzing sustainability of social-ecological systems. **Science** 325: 419-422. https://www.science.org/doi/abs/10.1126/science.1172133

Pennington, D. D., Simpson, G. L., McConnell, M. S., Fair, J. M., & Baker, R. J. (2013) Transdisciplinary research, transformative learning, and transformative science. **BioScience** 63: 564-573. http://dx.doi.org/10.1525/bio.2013.63.7.9

Pohl, C. (2008) From science to policy through transdisciplinary research. **Environmental Science & Policy** 11: 46-53. http://dx.doi.org/10.1016/j.envsci.2007.06.001

Pretty, J., Sutherland, W.J., Ashby, J., Auburn, J., Baulcombe, D., Bell, M., *et al*. (2010) The top 100 questions of importance to the future of global agriculture. **International Journal of Agricultural Sustainability** 8: 219-236. http://dx.doi.org/10.3763/ijas.2010.0534

Rigby, E. (2005) Linking research and policy on Capitol Hill: insights from research brokers. **Evidence & Policy** 1: 195-214. http://dx.doi.org/10.1332/1744264053730798

Rudd, M.A. (2014) Scientists' perspectives on global ocean research priorities. **Frontiers in Marine Science** 1: 36. https://doi.org/10.3389/fmars.2014.00036

Rudd, M.A. (2015) Scientists' framing of the ocean science–policy interface. **Global Environmental Change** 33: 44-60. http://dx.doi.org/10.1016/j.gloenvcha.2015.04.006

Rudd, M.A. (2023) 100 important questions about Bitcoin's energy use and ESG impacts. **Challenges** 14: 1. https://doi.org/10.3390/challe14010001

Rudd, M.A., Ankley, G.T., Boxall, A.B.A. & Brooks, B.W. (2014) International scientists' priorities for research on pharmaceutical and personal care products in the environment. **Integrated. Environmental Assessment and Management** 10: 576-587. http://dx.doi.org/10.1002/ieam.1551

Rudd, M. A., Beazley, K. F., Cooke, S. J., Fleishman, E., Lane, D. E., Mascia, M. B., *et al*. (2011) Generation of priority research questions to inform conservation policy and management at a national level. **Conservation Biology** 25: 476-484. http://dx.doi.org/10.1111/j.1523-1739.2010.01625.x

Rudd, M.A. & Fleishman, E. (2014) Policymakers' and scientists' ranks of research priorities for resource-management policy. **BioScience** 64: 219-228. https://doi.org/10.1093/biosci/bit035

References

Rudd, M.A., Moore, A.F.P., Rochberg, D., Bianchi-Fossati, L., Brown, M.A., D'Onofrio, D., *et al.* (2018) Climate research priorities for policy-makers, practitioners, and scientists in Georgia, USA. **Environmental Management** 62: 190-209. https://doi.org/10.1007/s00267-018-1051-4

Sutherland, W. J., Adam, W. M., Aronson, R. B., Aveling, R., Blackburn, T. M., Broad, S., et al. (2009) One hundred questions of importance to the conservation of global biological diversity. **Conservation Biology** 23: 557 – 567. http://dx.doi.org/10.1111/j.1523-1739.2009.01212.x

Sutherland, W.J., Bardsley, S., Clout, M., Depledge, M.H., Dicks, L.V., Fellman, L., *et al.* (2013a) A horizon scan of global conservation issues for 2013. **Trends in Ecology & Evolution** 28: 16–22. http://dx.doi.org/10.1016/j.tree.2012.10.022

Sutherland, W.J., Bennett, C., Brotherton, P.N.M., Butterworth, H.M., Clout, M.N., Côté, I.M., *et al.* (2023) A global biological conservation horizon scan of issues for 2023. **Trends in Ecology & Evolution** 38: 96-107. https://doi.org/10.1016/j.tree.2022.10.005

Sutherland, W.J., Fleishman, E., Mascia, M.B., Pretty, J. & Rudd, M.A. (2011) Methods for collaboratively identifying research priorities and emerging issues in science and policy. **Methods in Ecology and Evolution** 2: 238–247. http://dx.doi.org/10.1111/j.2041-210X.2010.00083.x

Sutherland, W.J., Freckleton, R.P., Godfray, H.C.J., Beissinger, S.R., Benton, T., Cameron, D.D., *et al.* (2013b) Identification of 100 fundamental ecological questions. **Journal of Ecology** 101: 58-67. http://dx.doi.org/10.1111/1365-2745.12025

Sutherland, W.J. & Woodroof, H.J. (2009) The need for environmental horizon scanning. **Trends in Ecology & Evolution** 24: 523-527. https://doi.org/10.1016/j.tree.2009.04.008

Sutton, A.M. & Rudd, M.A. (2016) Crossing science–policy–societal boundaries to reduce scientific and institutional uncertainty in small-scale fisheries. **Environmental Management** 58: 565-584. https://doi.org/10.1007/s00267-016-0737-8

Van den Brink, P.J., Boxall, A.B.A., Maltby, L., Brooks, B.W., Rudd, M.A., Backhaus, T., *et al.* (2018) Toward sustainable environmental quality: priority research questions for Europe. **Environmental Toxicology and Chemistry** 37: 2281-2295. https://doi.org/10.1002/etc.4205

Wisz, M.S., Satterthwaite, E.V., Fudge, M., Fischer, M., Polejack, A., St John, M., *et al.* (2020) 100 opportunities for more inclusive ocean research: cross-disciplinary research questions for sustainable ocean governance and management. **Frontiers in Marine Science** 7: 576. https://doi.org/10.3389/fmars.2020.00576

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Sino Global Capital

SINO

GLOBAL CAPITAL

RESPONSE TO

RFI 88 FR 5043

Request for Information; Digital Assets Research and Development.

SUBMITTED
MARCH 3, 2023

EXECUTIVE SUMMARY

To maintain its status as a global leader and to augment existing regulations and laws, Executive Order 14097 asserts that the United States has a vested "interest in responsible financial innovation, expanding access to safe and affordable financial services, and reducing the cost of domestic and cross-border funds transfers and payments, including through the continued modernization of public payment systems."

The government of the United States could create an era of safe, efficient, favorable and beneficial participation of American citizens by developing legislation on three strategic areas of domestic digital asset policy focused on: i. resolving inefficiencies in cross-border transfers, ii. developing a regulatory regime for tokenized financial markets, and iii. establishing industry safeguards for and proactively supporting a system of digital IDs.

INTRODUCTION

"If danger ever reach us, it must spring up amongst us. It cannot come from abroad. If destruction be our lot, we must ourselves be its author and finisher. As a nation of freemen, we must live through all time, or die by suicide."
- President Abraham Lincoln

On January 27, 1838, President Lincoln delivered a speech titled "The Perpetuation of Our Political Institutions", wherein the sixteenth President warned that domestic interests seeking to disrespect the laws of the United States could in fact destroy the very fabric of our Union. One hundred eighty five years later these remarks could not be more relevant. The United States' seemingly haphazard, patchwork approach to regulation of the digital asset industry threatens to destroy any lingering hopes of American relevance in the global digital assets industry.

Described by some in the blockchain industry as a 'carpet bombing' of the American private sector's involvement in the coming digital asset age, ill-conceived "regulation by enforcement" and a lack of government coordination simultaneously ensured two things: first, a chilling effect on desire or appetite of compliant American interests in the space to continue domestically or otherwise, and perhaps more importantly, justification for a shift away from America as the natural center of gravity in digital asset innovation to more hospitable, safe, regulated, legislated, and transparent markets. Market participants have left the US and more are leaving every day.

Absent a whole-of-government approach endorsed by Executive Order 14097, led by a nimble legislative branch of Government that recognizes the opportunity and need to augment established laws and precedent with the creation of smart, new laws to deal with new technologies and foster innovation and leadership designed to keep America and American interests at the global forefront of this burgeoning new industry, current practice by overreaching regulatory bodies might make true President Lincoln's ominous admonition and challenge. Without just, reasonable and modern laws creating a practical framework and strategy for future American innovation in the digital assets sector, outdated inflexible bodies will all but surely stifle any progress made by American innovators in this sector and kill American advantage from within.

METHODOLOGY

Focus

The SGC response follows a thematic approach, focusing on three distinct areas that relate to SGC's activity as a globally-focused digital assets venture capital firm, namely those pertaining to cross-border transfer of funds, financial market infrastructure (FMI), and salient aspects of digital identity and wallets.

Structure

Each section begins with an exploration within each area of the pertinent or relevant challenges and opportunities. This is followed by a section titled 'Suggested Research', which highlights areas where digital assets and blockchain might be helpful in the resolution of the named problems, with recommendations to explore and develop legislation in a manner defined by the Executive Order as being seen to be in the best interest of the United States.

Relevance

Each section of the response is correlated to one or more of the six topics of the RFI defined as the following key terms of relevance as disclosed in Document 88 FR 5043 titled Request for Information; Digital Assets Research and Development. These are defined and referenced by the following key terms:

- *Topic 1: Goals, sectors, or applications that could be improved with digital assets and related technologies.*
- *Topic 2: Goals, sectors, or applications where digital assets introduce risks or harms.*
- *Topic 3: Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.*
- *Topic 4: R&D that should be prioritized for digital assets (especially in relation to a potential U.S. CBDC system).*
- *Topic 5: Opportunities to advance responsible innovation in the broader digital assets ecosystem.*
- *Topic 6: Other information that should inform the R&D Agenda.*

THREE STRATEGIC AREAS OF DIGITAL ASSETS RESEARCH AND DEVELOPMENT

1. SWIFT VS. BLOCKCHAIN

“Banking organizations should ensure that crypto-asset-related activities can be performed in a safe and sound manner, are legally permissible, and comply with applicable laws and regulations, including those designed to protect consumers.” [1]

When paired with smart policy and legislation, blockchain can help banks do that much more efficiently.

PROBLEM

SWIFT is a messaging network which handles around 5 trillion USD a day through approximately 35 million transactions enacted between 11 thousand member financial institutions. When a member bank initiates a payment through SWIFT, it sends a payment instruction message to the recipient bank. This message contains information about the payment, including the amount, currency, and account details of the sender and receiver. The recipient bank then uses this information to process the payment, which typically involves moving funds between accounts or using a correspondent banking relationship to facilitate the transfer. Although massive, several major problems plague SWIFT:

01
Low Speed

SWIFT separates messaging from payment. The SWIFT system provides a secure and standardized platform for banks to exchange messages and other information related to financial transactions. These messages can include instructions for payment, but the actual movement of funds is handled separately through other mechanisms, such as correspondent banking relationships or settlement systems. Another, but related, problem is different time zones. SWIFT transfers are processed during business hours, which can vary by country and time zone. If money would be transferred outside of these hours, there may be a delay in processing the transaction.
As a result, SWIFT transfers are not instant. It usually takes 1-4 business days for the funds to be available to the recipient. The duration depends on whether the two involved banks have a direct relationship or not.

1. https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf
2. https://www.swift.com/about-us/discover-swift/fin-traffic-figures
3. https://www.csis.org/analysis/sanctions-swift-and-chinas-cross-border-interbank-payments-system

02
High Cost

Each intermediary bank involved in the transfer can charge a fee for processing the transaction, which can add up quickly. This results in significantly higher costs of intermediation.

03
Likelihood Of Errors

The multiplicity of intermediaries that usually get involved in any given transfer significantly increases the likelihood of errors, especially for banks that have not adopted yet the standardized messaging system ISO 20022. This can be particularly problematic if there are discrepancies in the information provided by the sender or if there are regulatory requirements that need to be met. Furthermore, human intervention to correct errors can result in additional costs and error vectors.

04
Scalability

SWIFT's scalability is limited by the separation between messaging, on the one hand, and transfer and settlement, on the other. For large transfers, the messaging system can work, but transfer and settlement are bound by the limited capacity of the transfer and settlement system.

The cross-border transfer system of the future should be faster, cheaper, and less prone to errors. It should also facilitate scalability by not separating the transfer of value from the messaging protocols. Blockchain technology enables assets to be transferred and settled in real time given the unified ledger all market participants record their assets and liabilities on. This reduces errors as blockchains can enable preclearance which creates efficiencies in regulatory compliance, thereby reducing costs for compliance and errors from manual processing.
Blockchain can also help improve the resilience of cross-border transfer networks and remove the risks arising from centralized points of failure.

SUGGESTED RESEARCH

Despite the aforementioned benefits, the use of blockchain in cross-border transfers raises a number of challenges, which requires further research that aims to:

- Determine which cryptocurrency among the 9,000-22,000 cryptocurrencies present today or existing blockchain technology stack could provide a reliable solution for cross-border transfers, especially given the great variation among cryptocurrency in their technical specifications, market cap, and user base.
- Determine if cross-border transfers are made at a wholesale or retail level. Each option offers various degrees of speed, low cost and control, and any choice in this regard would necessarily involve a tradeoff between these competing goals.
- Clarify how identities of transactors are to be ascertained on-chain and which regulation should be applicable. Specifying the applicable regulation would be especially relevant in cases where senders and recipients are subject to different digital identity standards.
- Ensure that anti-money laundering, counter financing of terrorism, and other screenings required under applicable regulations are performed on any transfer and explore if a certain degree of transaction centralization is necessary.
- Ensure a high degree of competition between public (i.e., CBDC-based) and private (i.e., cryptocurrency-based) solutions.
- Facilitate the adoption of innovative solutions with respect to screenings, including automation, entrusting them with accredited parties or government agencies, or, alternatively, relying on a decentralized system of digital identity or whitelisting.

RELEVANCE:
Topic 4, Topic 1

4.https://blogs.lse.ac.uk/businessreview/2019/11/04/do-six-per-cent-of-financial-transactions-sent-via-the-swift-system-really-fail/
5. https://www.ft.com/content/91342189-978f-4d44-9dcf-b993983f08f9
6. https://coinmarketcap.com/.

2. AUTOMATING SECURITIES TRADING

While tokenized markets have the potential to revolutionize traditional finance and create new opportunities for both issuers and investors, it is crucial that these markets are designed and regulated in a way that protects investors, promotes fair competition among issuers, and ensures the stability of the financial system as a whole.

PROBLEM

Due to the global accessibility and openness of the chain as well as the lack of a centralized point of accountability, implementing regulatory action may be challenging. Current regulatory regimes may not be suitable for tokenization and, thus, may not be capable of fostering confidence and reducing uncertainty. Differences in national standards applicable to tokenization may give rise to regulatory arbitrage opportunities, leading to a race to the bottom.

The use of blockchain and smart contracts can revolutionize securitization throughout the various stages of a security's life cycle:

- **01 Origination** — Issuers of securities can have unique identities on the blockchain that facilitate the verification of their identity and creditworthiness by potential lenders, not only in issuers' home country, but from all over the world.

- **02 Structuring And Review** — All parties can access and review the data of issuers of securities, with the possibility of automating this part of the process using smart contracts.

- **03 Initials Offerings** — Blockchain makes it possible for issuers to directly sell securities to investors, without the need for an intermediary, creating efficiency gains for both issuers and investors. This part of the process can also be automated, at least with respect to post-purchase settlement, using smart contracts.

- **04 Servicing** — Functions such as dividend or interest distributions can be automated using smart contracts, which can also be used to enforce the security terms and conditions in case of default on those payments.

- **05 Secondary Trading** — Blockchain technology can make secondary markets more globalized and standardized and, thus, more liquid. Securities could be easily traded in different countries on a 24-7-365 basis and can be bought and sold on a P2P basis, which creates efficiency gains for investors and liquidity gains for issuers. Smart contracts can facilitate secondary trading of securities by automating post-sale settlement and lowering liquidity, credit, and default risks, thereby reducing needed margins.

SUGGESTED RESEARCH

Further research is needed to:

- Ensure effective consumer protection, especially in light of the global nature of markets. Future regulations may need to create roles that do not currently exist or exist in a different form in today's financial markets. For example, licensed third parties may be needed to evaluate the accuracy of the information provided by issuers, scrutinize the identity of investors, onboard investors, and conduct regulatory screenings such as anti-money laundering, counter financing of terrorism, and the like. Regulation should also ensure that consumers have adequate avenues for recourse and redress in case they suffer any damages.

- Consider how to implement a 24/7 blockchain trading solution and market structure designs that do not fragment liquidity given that in current traditional finance markets, the vast majority of liquidity in the market centers around end of day cash settlements and asset valuation calculations.

- Develop the financial blockchain infrastructure and token architecture to facilitate real time CBDC cash settlement necessary to simultaneously clear and settle securities in real time.

- Devise new consumer protection rules aimed to protect investors from novel risks posed by blockchain technology, such as operational failure, cyber attacks, and identity theft.

- Ensure the smooth functioning of the new marketplace on-chain, interoperability among different chains, the absence of artificial barriers to entry, and the safety and soundness of market networks.

- Level the playing field between on-chain and off-chain financial markets and create virtuous interactions or gateways between the two.

- Protect market integrity, especially in novel, immature markets and mitigate the risk of contagion.

- Provide effective legal protections for American investors investing in securities issued by foreign entities.

RELEVANCE:

Topic 1, Topic 2, Topic 4

3. DIGITAL IDENTITIES

On the internet, individuals need to use different components of their identities to gain or maintain access to online services. Individuals, however, do not fully control these identity components, and the value created using them is usually not shared with individuals. Furthermore, individuals' activities online give rise to a new form of identity, which is digital identity, that incorporates distinct digital identifiers of an individual, such as IP addresses, passwords, biometrics, and behavioral and biographic information. Blockchain can help safe sharing and storing of such sensitive information.

PROBLEM

Identity consists of basic information or claims about a person, such as their name, date and place of birth, address, nationality, physical features, and even health condition. In most countries, including the U.S., individuals get their identities documented in identifiers, such as ID cards, passports, social security numbers, or driving licenses, all of which are granted by government entities and stored on these entities' databases.

Currently, Personal Identifiable Information (PII), whether related to physical or digital identity, is stored on centralized databases controlled by public and private actors. The centralization of PII storage, coupled with weak cybersecurity measures and the rising value of PII, has led to a sharp increase in cyber attacks targeting PII. In 2018, these attacks amounted to 97% of all targeted cyber attacks in the U.S. Management of digital identities is no less problematic. The platforms that use digital identities to provide services manage them in an extremely fragmented way, requiring users to create and safely store numerous usernames and passwords, and increasing the likelihood of loss of access to services and/or funds. Lastly, the relationship between physical and digital identity is very weak, which makes individuals more exposed to the risks of digital identity theft, fraud, blackmailing, and financial loss.

In recent years, the use of blockchain technology has been proposed as a solution to many of these problems through what is known as self-sovereign identity (SSI) viewed as a means to better protect PII and enable individuals to have more control over their identities. With SSI, individuals can store their identifiers on a local device and share them with peers or service providers, without any reliance on a centralized database.

SSI is enabled through a multi-source identity system that relies on three parties: (1) a credential issuer who determines the credentials to issue, what they signify, and how they can be validated, (2) a credential holder who determines the credentials to obtain and use, and (3) a credential verifier who attests to the veracity of the credentials. In an SSI system, credentials are encrypted, pseudonymized, and stored on a chain, making it very hard to tamper with. Individuals determine when and under what conditions their credentials can be shared, which overall considerably limits the disclosure of this data and puts individuals in a better position to reap the economic benefits of their physical and digital identities.

7. https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf.

SUGGESTED RESEARCH

Despite the promising prospects of SSI in terms of protecting individuals' physical and digital identities and improving individuals' bargaining position vis-a-vis online platforms, further research is needed to effectively implement this system, particularly to:

- Ensure that digital identity systems can operate across different platforms so as to defragment user experience, minimize the risk of losing access, and put individuals in full control of their data sharing.
- Enable the creation of resilient digital identity systems that can protect users' data at all times, mitigate operational risks, and minimize the risk of system failure.
- Develop scalable digital identity systems that can support millions of users and transactions while preserving security and privacy, without creating barriers to entry that may limit competition and innovation.
- Set standards for the issuance and use of digital IDs, determine the legal character of issuers (e.g., private entities, public utilities, government entities), and clarify the relationship between issuers, holders, and verifiers.
- Negotiate global rules for the issuance of digital IDs to minimize fragmentation, combat criminal activity, both domestic and cross-border, and facilitate cross-border transactions.
- Guarantee usability and accessibility for everyone, particularly marginalized and underserved communities, foster trust in digital identity systems, and educate the general public about the benefits and risks of digital identities.
- Establish clear guidelines for the relationship between issuers of legacy identifiers and issuers of digital identities, with a view to improving user experience and creating synergies on and off chains.

RELEVANCE:

Topic 1, Topic 2, Topic 3, Topic 5

CONCLUSION

The United States government could create a favorable domestic environment for private sector development of innovation and industry in the digital asset space, by clearly defining taxonomies, and establishing streamlined, compliant procedures that are supported by law and interdepartmental coordination.

Most importantly, however, is a simple recognition of a plain truth– like it or not, by just its very presence, blockchain has changed the world, and there is no going back to how things were before. Should the United States government develop such policies, Americans could actively and safely participate in global digital economies, and the government would help maintain American leadership as the global standard bearer of best practice and innovation in critical emerging technologies.

As an American-founded and globally-focused venture capital firm specializing in digital assets, Sino Global Capital wholeheartedly supports the desire of the legislative and executive branches of government to fill the current vacuum of domestic modern laws and regulations surrounding this new technology. It is our hope that responses to this request for information helps ensure American relevance as a thriving and globally competitive digital assets market, and secures American strategic national interest at the digital forefront of the rest of human history.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Securities Industry and Financial Markets Association ("SIFMA")

By Electronic Mail

March 3, 2023

The White House Office of Science and Technology Policy (OSTP)
Eisenhower Executive Office Building
[redacted]

Re: Request for Information: Digital Assets Research and Development Agenda

To Whom It May Concern:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the request for information ("RFI") issued by the White House Office of Science and Technology Policy ("OSTP") to help identify priorities for research and development related to digital assets, including various underlying technologies such as blockchain, distributed ledgers, decentralized finance, and smart contracts. The RFI also solicits comment on several related issues such as cybersecurity and privacy, programmability, and sustainability as they relate to digital assets.[2]

SIFMA welcomes the OSTP's interest in seeking additional information on the research and development ("R&D") opportunities that could arise from digital assets. In particular, the OSTP's interest in understanding the "goals, sectors, or applications that could be improved with digital assets and related technologies," as well as the "goals, sectors, or applications where digital assets introduce risks or harms."[3] SIFMA's response to the RFI focuses on the opportunities and possible risks associated with digital assets and distributed ledger technology ("DLT") in the context of capital markets products and applications.

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] *See* Office of Science and Technology Policy, 88 Fed. Reg. 5,043 (Jan. 26, 2023).

[3] *Ibid.* 5045.

[redacted]
www.sifma.org

SIFMA believes that these new technologies can drive substantial efficiency, security, transparency, and financial inclusion benefits to U.S. capital markets, providing that their associated risks are appropriately managed. The best way to ensure that these potential risks are appropriately managed, and that experimentation and innovation more generally occurs in a responsible manner that protects investors, is to have such activities occur within the existing regulatory frameworks that govern U.S. capital markets. As such, this response is focused on the opportunities, risk management issues, and regulatory considerations associated with the application of DLT to existing financial instruments, payment instruments and payments infrastructures (in contrast to its use in other types of native digital assets, such as cryptocurrencies).

Executive Summary

SIFMA is submitting this response to highlight the following issues:

- ***Potential Capital Markets Use Cases***: There are a variety of capital markets focused DLT use cases that SIFMA members are exploring and discuss their potential benefits. These include:
    - Blockchain infrastructure applications that could improve the speed, security, and/or efficiency of existing processes;
    - The tokenization of "traditional" securities and the issuance of "natively" digital securities, which could offer significant benefits to a wide range of market participants;
    - The tokenization of non-security assets (*e.g.,* tokenized deposits or fiat currency); and
    - Ways in which DLT can be used to make cross-border payments faster, less costly, less risky and more broadly accessible.

- ***Understanding Technology Differences:*** Policymakers and market participants need to understand the distinct risks and benefits that arise from differences in the underlying technology infrastructure that enables digital asset products and services. Specifically, it is important to understand:
    - The differences between technology infrastructures that are accessible only to a private or restricted network versus those that are publicly available.
    - The differences between the control privileges for users of the network, whether those networks are "permissioned" or "permissionless". Regulated financial institutions are looking at both "private-permissioned" and "public-permissioned" networks. Each type of network has its own valuable features that offer substantially more embedded controls and risk management functionality than "public-permissionless" networks, such as those that drive the Bitcoin network.
    - The risk of a DLT application needs to take into context the features of the technology itself, the product or operational process it drives, and the broader risk management frameworks provided by the institution(s) operating it.

- ***Building on Existing Risk Management Programs at Regulated Institutions*****-- Capital Markets:** DLT applications can benefit by leveraging existing risk management control functions at regulated financial institutions. Mature risk management frameworks capturing a range of technology and operational risks already exist at these institutions. This framework provides financial institutions the ability to assess and identify which technology configurations present the least risk, and layer additional controls on top of those offered by the DLT platform itself. This process of managing risks when deploying new DLT infrastructure is similar to the processes that financial institutions have used to manage decades of technology innovation and address risks associated with legacy systems.

- ***Regulatory Modernization:*** It is crucial that the regulatory framework be modernized to support, or clarify that current regulations allow for, innovation in the digital assets space and maintain the inherent competitive advantage of U.S. markets in regulated digital products. This is best accomplished by applying existing, well-developed, and broadly understood regulatory frameworks at both the federal and state level to digital asset-oriented entities and products, with appropriate updates, including through interpretive guidance or commentary, that reflect the unique features of blockchain technology. As policymakers update existing rulebooks, they should also prioritize investor protection, adopt a "technology neutral" approach, and follow the principle of "same risk, same activity, same regulatory outcome."

- ***Updating Standards:*** It is vital that existing technology and operational standards supported by the Federal government be updated to accommodate DLT, *e.g.,* through continued investment in research and projects being conducted by the National Institute of Science and Technology ("NIST").

- ***Development of a U.S. Central Bank Digital Currency ("CBDC"):*** We highlight existing work that SIFMA has conducted in this area, with a focus on the possible benefits of a wholesale CBDC for certain capital markets applications. SIFMA underscores the importance, however, of conducting additional research and study before moving forward with the adoption of any form of U.S. CBDC.

- ***Public-Private Partnerships:*** SIFMA recommends that policymakers establish public-private task forces and working groups to drive research and support responsible development in the digital assets space.

* * *

SIFMA appreciates the OSTP's consideration of these comments and would be pleased to discuss any of these views in greater detail if it would assist with their deliberations. Please contact Charles DeSimone at [redacted] and Peter Ryan at [redacted] if you wish to discuss the points raised in this letter further.

Sincerely,

[redacted]

Kenneth E. Bentsen, Jr.
CEO and President
Securities Industry and Financial Markets Association

1. Benefits of Digital Assets and Frameworks for Understanding Risk Management

SIFMA and its members believe that the application of digital asset technology has the potential to drive substantial improvements in the U.S. capital markets. Digital assets innovation by regulated entities in regulated products arguably offers the best venue for digital assets experimentation and innovation; building on existing regulatory frameworks and protections. In this letter, SIMFA discusses the opportunities and regulatory and risk management issues associated with the application of DLT to regulated financial products, such as equity and debt securities.

Notably, these products and applications are distinct from other types of digital assets, such as those commonly referred to as "cryptocurrencies." While a range of taxonomies and terminology are used to categorize DLT-based assets, the framework adopted by the Basel Committee on Bank Supervision ("BCBS") differentiates between three broad categories: tokenized traditional assets, which often create efficiencies within the well-established banking framework; cryptoassets with effective stabilization mechanisms (*i.e.,* stablecoins); and unbacked cryptoassets, such as Bitcoin.[1] The Global Financial Markets Associations ("GFMA"), of which SIFMA is a member, has developed a taxonomy that further differentiates digital assets into six categories: 1) value-stable digital-assets, including CBDCs, financial market infrastructure ("FMI") tokens, tokenized commercial bank money, and stablecoins; 2) security tokens; 3) cryptocurrencies; 4) settlement tokens; 5) utility tokens; and 6) other crypto-assets (*i.e.,* those not structured as value-stable crypto-assets).[2]

The absence of consistent definitions or a nuanced taxonomy of different digital asset types used by regulators creates major challenges and stifles innovation. Unclear or inconsistent definitions create obstacles for firms who are looking to apply DLT infrastructure to create efficiencies and carry out well established and already permissible activities. For example, many digital asset activities being explored by capital markets participants are simply using new infrastructure to record ownership of existing registered products, yet regulatory definitions often fail to distinguish between this type of activity and non-traditional applications of digital asset technology. The lack of consistency in taxonomies internationally also creates challenges for market participants, leading to differential treatment for certain classes of assets and activities depending on jurisdiction. Continued U.S. leadership in digital assets innovation and in the capital markets more broadly will be contingent on ensuring greater harmonization of taxonomies across major jurisdictions and on U.S. policymakers taking a more nuanced approach to definitional issues than has been shown to date.

In addition to being mindful of the distinctions between different types of digital assets, policymakers also need to understand the important differences in configurations of the underlying digital ledger technology and the impacts of those differences (see section 3 below). These distinctions between digital assets and between blockchain infrastructures should shape the type of oversight and investor protections that an activity, asset, or entity should be subject to. Research into the broad category of "digital assets" needs to be cognizant of these

---

[1] Basel Committee on Banking Supervision, "Prudential treatment of cryptoasset exposures" December 2022, available at: https://www.bis.org/bcbs/publ/d545.pdf

[2] The full taxonomy is provided in Annex 1 to the GFMA response to the Financial Stability Board's (FSB) questions for consultation on "International Regulation of Crypto-Asset Activities – A Proposed Framework," December 2022, available at: https://www.gfma.org/wp-content/uploads/2022/12/gfma-response-to-fsb-crypto-asset-consult-15-december-2022.pdf

foundational differences in features and applications and produce policy recommendations that appropriately reflect these distinctions.

As policymakers conduct further research, SIFMA furthermore encourages them to focus on discrete digital asset types that are designed and issued in compliance with existing capital markets regulatory frameworks, and on specific infrastructure configurations that best enable regulated financial entities to manage risk, maintain fair and orderly markets, and protect the interests of clients and investors.

2. Potential Use Cases and their Benefits for Regulated Entities

Below, SIFMA highlights several applications of digital asset products and services and discuss the potential benefits they could offer capital markets participants and the broader economy. These include blockchain based infrastructure; native digital security issuance; tokenization of existing financial instruments; tokenized non-security assets such as commercial bank deposits; and cross-border transfers.

A) Blockchain Infrastructure Applications

Market participants continue to explore and implement a range of projects using underlying blockchain technology to improve upon existing industry functions and processes. The focus is not to create new blockchain based assets, but to make processes around existing assets faster, more secure, and more efficient, or to take advantage of the way blockchain records provide immutability and greater transparency in data.

These applications include using blockchain based settlement models to allow for faster, more efficient, or more customized settlement of existing "traditional" securities on an optional basis.[3] Similarly, firms are exploring how smart contracts could automate existing industry processes, such as payment or delivery of securities or funds, allowing for faster transactions, increased confidence, and greater customization. Other projects explore the potential for blockchain based records to provide an authoritative record of information, showing not just current prices or ownership structures, but also historical developments. Blockchain based "oracles" can be designed to provide common understanding of critical information within a single firm or across a range of participants in a market, or investors in a common asset or investment vehicle. For example, certain forms of privately held companies feature evolving ownership structures and corresponding valuation levels, which could be tracked using blockchain systems.

B) Issuance of Natively Digital Securities

Another area of interest for SIFMA members is the issuance of natively digital securities, which are issued and tracked on blockchain infrastructure. These have been referred to using a range of different terms, including "security tokens" and "digital asset securities," and, as discussed below, share some similarities with "tokenized securities" (that is securities that are issued traditionally but represented on a blockchain for books and recordkeeping purposes).

[3] While market participants are exploring the potential for blockchain based settlement models to allow for faster settlement options, the industry is preparing to shorten the settlement cycle for equities and certain other securities to one business day after the trade is executed (T+1), which is expected to be complete in 2024. Moving the settlement cycle broadly to something faster than T+0 (whether same day settlement on an end of day basis (T+) settlement) or "atomic settlement" is challenging.

Natively digital securities offer potential advantages to market participants and can enable a range of innovations in how securities are issued, traded, settled, and serviced. Natively digital securities can be more easily marketed and can also be easier to structure and issue. This can allow for greater customization, potentially allowing asset types which were previously cost inefficient to be offered to investors with the protections provided by securities laws and regulations.

Blockchain based trading and settlement can also offer greater speed and efficiency, although it would need to be supported by a robust set of settlement tools on the blockchain network and an on-blockchain network payment option, whether that be tokenized cash, a settlement token or equivalent, or a CBDC. These considerations also apply to already existing assets that are tokenized, as discussed below.

Natively digital securities can also embed the calculations for the security (such as coupon payments) in the asset itself, providing greater efficiency in asset servicing and greater customization to fit either investor demands or the unique features of the economic asset underlying the security. For example, green bond payments could have functionality that embeds the ability to track climate developments within the security when it is issued, providing greater transparency to investors.

C) Tokenization of Previously Issued Securities

In addition to issuing securities natively on a blockchain, firms are also exploring the opportunities offered by tokenizing securities which were already issued "traditionally" using existing industry infrastructure. Under this process, a security holder can create a representation of the security on a blockchain network through the process of tokenization, so that the representation of the rights to the security can be tracked, traded, and cleared and settled using DLT infrastructure. This process can be managed by a custodian, who ensures that the underlying security is secure and immobilized, using existing industry operations and in compliance with well-established regulations.

Tokenization of existing securities can offer a range of benefits, some of which overlap with natively digital securities. Tokenization in traditionally opaque markets can improve efficiency and market quality, such as by providing additional liquidity, exposure to broader groups of investors, or more efficient settlement and asset servicing. Tokenization can also offer flexibility in its functionality in areas where existing industry infrastructure cannot, such as highly customized settlement instructions or securities lending or repo transactions on shorter time periods than are currently available. Additionally, tokenized securities can address challenges around cross-border asset transfers.

D) Tokenization of Non-Security Assets

Non-security assets can also be represented on a DLT network via tokenization, offering a range of benefits to market participants, infrastructure operators, and end investors.

One key example is commercialized bank deposits, which can function as tokenized fiat currency that can serve as a vehicle for handling the payment leg of securities settlement on-chain, allowing for the entirety of a transaction or trade (*i.e.,* through settlement and payment) to be carried out on a DLT network, facilitating greater efficiency and potentially faster settlement models. Alternatively, they can be used to support settlement tokens which can be used within a given infrastructure venue. The Bank for International Settlements has recently highlighted to potential for such tokenized deposits to become interoperable with central bank money in commercial payment systems.[4] Examples of such tokenized deposits include products already in operation, such as Onyx, and the Regulated Liability Network, which is in proof of concept.[5] This function has some overlap with the potential role for a CBDC, which may be, at best, duplicative, as discussed below.

E) Cross Border Transfers

Firms are also using blockchain to support innovation in cross border payments. Beyond discussions of how digital assets might potentially facilitate cross-border payments, there are a range of use cases and potential benefits for handling fiat currencies in cross border transactions via DLT infrastructure. These include faster payments and greater security and auditability of transaction histories, as well as potentially lower costs, broader access, and more robust controls for anti-money laundering ("AML") / know-your-customer ("KYC") programs.[6]

3. Understanding Technology Differences and their Risk Implications

Just as it is critical for policymakers to understand and define the differences between digital asset types and to ensure that policy and regulatory frameworks reflect those differences, it is equally important to differentiate among different configurations of the underlying technology infrastructure that enables digital asset products and services. Discussions of DLT or blockchain infrastructure often conflate all types of network configurations and obscure the very real differences between them – differences that have major impacts on risk, users, and how technology innovation can be integrated within existing regulatory frameworks.

The type of digital ledger architecture employed has important implications across a range of issues of concern to policymakers, including anonymity, efficiency of transaction processing, and asset security. Focusing on the risks associated with certain types of common ledger configurations may obscure the fact that other technology arrangements can be designed to align with the goals and requirements of existing regulatory frameworks. For example, policymakers should not conflate the experiences of markets and infrastructure developed for pseudonymous bearer assets (such as Bitcoin) with regulated entities engaging in traditional capital markets activities, and DLT infrastructure more broadly.

At a high level, the key features of DLT networks can be differentiated along two axes – the accessibility of the network (whether it is restricted only to certain users or is publicly available)

---

[4] "Innovation and the future of the monetary system," Keynote speech by Agustín Carstens, General Manager of the BIS, at the Monetary Authority of Singapore (MAS), Singapore, 22 February 2023.https://www.bis.org/speeches/sp230222.htm

[5] As proposed, the tokenized commercial bank deposits under the Regulated Liability Network (RLN) proposal could be readily exchanged with existing account-based forms. A description of the RLN proposal can be found at Regulated Liability Network. Policymakers should explore if and how these alternative technology configurations could meet the objectives of a CBDC, such as the instant movement of value 24/7 either domestically or internationally, integrated into other digitized processes, and serve as "programmable money" insofar as payments can be automated or made conditional on events.

[6] For example, in 2021, Wells Fargo and HSBC entered into a bilateral agreement to settle FX transactions through a blockchain-based solution designed to, among other things, reduce settlement risk in certain foreign exchange transactions, further details available at: *"*Wells Fargo and HSBC establish Bilateral Agreement to Settle FX Transactions Through a Blockchain-based Solution*".*

and the control of privileges for users of the network (*i.e.*, authentication of who can carry out specific actions, such as writing changes to the ledger). This schema results in three main types of distributed ledgers:

- ***Private Permissioned:*** Closed-loop, private networks, which restrict access to predetermined users only.
- ***Public Permissioned*:** These applications are built on a public network foundation but with the addition of use controls on top of the underlying network to create what are effectively closed networks (which vary by design), given selective restriction of access through authentication for governance, administration, or other privileges.
- ***Public Permissionless*:** Open, public networks that do not restrict access for privileges. While they present several risk issues, these networks are among the largest operating today and present a track record of resilience, supported by a large community of users.

The chart below summaries some of the key distinguishing features of these network types[7]:

	Private Permissioned	**Public Permissioned**	**Public Permissionless**
Governance	Centralized	Centralized protocol for the application (as opposed to the broader network)	Decentralized
Accessibility to Users	Closed	Closed (for the relevant application)	Open
Control over Privileges	Can be defined as required	Users authenticated for specific roles	All users can perform all roles
Identification	All users known	All users known (for the relevant app.)	Pseudonymous
User Base	Very limited (by design)	Limited (for the relevant application)	Broad

Understanding and clearly defining these differences is critical, so that oversight and regulation can focus on best managing the risks associated with each activity. Without understanding these structural differences in how DLT networks manage risk, policymakers may assume incorrectly that anything touching DLT introduces novel risk and so requires novel regulatory treatment, such as that articulated in SEC Staff Accounting Bulletin 121[8] or in the imposition of capital surcharges for banks engaging in any form of DLT activity.

In general, regulated financial institutions are working with DLT configurations that are built on embedded control frameworks – whether those controls involve access to the network, permission structures, or both. These frameworks need to be distinguished from the technology configurations adopted by certain other crypto assets, which have emphasized pseudonymity and distributed networks, creating additional risks not present in certain types of distributed

[7] The summary above introduces at a high level the risk management controls associated with each type of technology configuration. SIFMA would be happy to discuss in greater depth the risk management controls associated with each network type and how they are consistent with the oversight and risk management requirements of regulated financial institutions.

[8] Securities and Exchange Commission Staff Accounting Bulletin No. 121, March 31, 2022, available at: https://www.sec.gov/oca/staff-accounting-bulletin-121

ledger configurations. For example, policymakers have raised concerns about certain features of the Bitcoin network – that system looks the way it does because of specific design choices made by its users. In contrast, regulated financial institutions are making choices based on their own requirements, including safety and soundness concerns as well as consumer protection, which result in a very different set of controls and operating models.

It is critical not to assume that any one type of network is necessarily more risky than other types. The key is understanding applicable risk management features and how they align with the goals of the product they are supporting, other organizational controls that may be in place, and any regulatory requirements. For example, if a permissionless network has certain attributes (*e.g.,* significant volume and dispersion of nodes), its immutability and threat resistance can be significantly lower than a permissioned network with a single party controlling the network. As a result, the Bitcoin network itself – while it has many features that are concerning for financial regulators – has proved to be very resistant to direct hacks.

4. Regulated Financial Institutions Working with DLT Can Build on Existing Risk Management Programs

Beyond the controls inherent in the blockchain network itself, DLT applications in the capital markets leverage controls from regulated financial institutions' existing technology and operational risk management programs. These well-developed and mature programs provide a framework for financial institutions to assess and identify which technology configurations present the least risk for potential applications and then layer additional controls on top of those offered by the DLT platform itself. This process of managing risks when deploying new DLT infrastructure is like the processes that financial institutions have historically used to manage prior waves of technology innovation and address risks.

As discussed above, the rubric of "digital assets" covers a broad range of diverse products, supported by technology configurations with fundamental differences in the tools they offer to manage multiple types of risk. Analysis of risk in DLT applications and products must not be generalized but focus on specific applications and shaped by risk through a combination of 1) the digital asset type, 2) its implementation model and underlying technology, and 3) its place in the securities lifecycle.

When SIFMA focuses on the regulated products and use cases described above (such as infrastructure applications, digital securities issuance and asset tokenization), we believe that they represent traditional financial products and activities and can therefore be governed effectively under existing risk frameworks. The existing, well-developed and broadly understood regulatory frameworks at both the federal and state level that apply to regulated entities provides a robust foundation for the risk management and customer protection in digital asset markets. These frameworks should be supported by appropriate modifications that reflect the unique features of blockchain technology to ensure that activities with similar risk profiles are regulated similarly.

As regulated firms look to apply DLT to regulated products and activities, they are guided by these regulatory frameworks, covering everything from entity disclosures and reporting requirements, compliance and risk management rules, requirements for the separation of different functions and activities, trading and market rules, and protection and segregation of client assets. These regulatory frameworks place investor protection at the forefront, alongside other key regulatory objectives such as market integrity and risk management. While some regulatory modernization might be necessary to account for the unique features of DLT, these frameworks provide a robust baseline of customer protection and risk management.[9]

For example, many have pointed to illicit finance concerns as a key risk associated with expansion of digital asset markets. Regulated financial institutions, however, have a long history of developing and honing Bank Secrecy Act ("BSA") and Combating the Financing of Terrorism ("CFT") compliance programs, including AML and KYC procedures, and illicit financing controls. They have a well-established track record of managing a wide variety of existing and emerging illicit financing risks and they are uniquely positioned to apply that deep expertise to digital assets. Similarly, mature regulatory frameworks governing illicit financing risks can be applied to digital asset technologies, albeit with possible modifications that reflect the underlying technology's unique characteristics.[10]

As policymakers assess the risk impact of DLT, it is important to remember that existing systems also pose risks. Over time, those risks have been understood and managed, and financial institutions have continued to evolve controls to address them. For example, over the past decade, the financial services industry has recognized the threat from cyberattacks and evolved its controls to meet the cyber threat and secure its expanding digital operations.

Given this experience and the focus of regulated institutions on deploying risk mitigants from the outset of any new technology development, SIFMA members and the financial infrastructure providers they work with are well equipped to apply existing risk management structures to manage DLT as they have withc other new technologies. SIFMA appreciates the concern of policymakers to ensure that future financial innovation based on DLT meets the same standards of security, reliability and client protection as existing technology. The securities industry agrees that addressing these concerns is foundational to our work with blockchain applications.

Given the existing technology and operational risk frameworks that regulated firms already have in place, combined with the protections inherent in appropriate technology configurations and the protections provided by existing product and entity level regulations, there is no reason to impose additional restrictions on the application of DLT by such firms. In particular, imposition on banks of any form of infrastructure risk capital surcharge for simply using DLT is both unnecessary and a major impediment to responsible blockchain innovation.[11] Allowing regulated financial institutions to apply DLT to regulated products and activities policymakers provides low-risk opportunities for regulators understand the benefits of digital assets

---

[9] For a further discussion of the role of existing regulations in providing oversight to emerging digital asset markets and activities, please refer to SIFMA's January 2023 blog post "Addressing Regulatory Gaps in the Digital Asset Ecosystem," available at: https://www.sifma.org/resources/news/addressing-regulatory-gaps-in-the-digital-asset-ecosystem/

[10] For a further discussion of the application of illicit financing regulations to digital assets and opportunities for regulatory modernization, please see SIFMA's response to the Treasury Department's September 20, 2022 Request for Comment ("RFC") on "Ensuring Responsible Development of Digital Assets" as it pertains to illicit finance and national security risks, November 2022, available at https://www.sifma.org/wp-content/uploads/2022/11/SIFMA-Treasury-Illict-Finance-RFC-11-03-2022.pdf

[11] SIFMA discussed these issues in greater depth in our joint trades' response to the second consultation issued by the BCBS on the prudential treatment of crypto assets Global Financial Markets Association ("GFMA"), Institute of International Finance ("IIF"), International Swaps and Derivatives Association ("ISDA"), Financial Services Forum, Futures Industry Association ("FIA"), Bank Policy Institute, International Capital Market Association ("ICMA"), and International Securities Lending Association ("ISLA"), "Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures." Available at: Joint Trades Comment Letter - Second Consultation on Prudential Treatment of Cryptoasset Exposures (sifma.org).

innovation, with innovation occurring in a controlled environment with well-established regulatory and risk management guardrails in place.

As discussed above, different technology configurations and infrastructure types have their own inherent strengths. This difference needs to be considered as policymakers assess how the broader risk management frameworks in place at regulated financial institutions integrate with new DLT platforms. For example, applications that use public blockchains which are open source, and are supported by many users who are working on the technology itself and vetting its code, while private ledgers offer control over choosing who participants are and how they interact, and rely on the individual users to vet all coding and functionality.

Policymakers should also consider broader technology and governance developments that can support risk management for DLT infrastructure. As discussed later, standards development and modernization, an area where the support of the Federal government is particularly valuable, is vital. The development of systems for verifiable credentials can address the risks of certain network types. Similarly, frameworks for the governance and management of public vs private information *(i.e.,* zero knowledge proofs) and how and what is disclosed on chain can draw from existing reporting and SEC disclosure frameworks, which provide models for appropriate sharing of information.

5. Regulatory Modernization

As noted above, SIFMA believes that existing and well understood regulatory frameworks can be applied, with appropriate modifications to reflect the distinct features of blockchain technology, to the types of digital assets and activities discussed in this letter. SIFMA welcomes the efforts of the Administration, (including the President's Executive Order on Digital Assets[12] and subsequent reports[13]) as well as Members of Congress and regulatory agencies to address gaps in the regulatory framework governing digital asset products and activities. It is crucial that policymakers act in a thoughtful but expeditious manner to clarify which existing rules or guidance apply to various types of digital assets and activities, define asset classes clearly, and identify rules that should be updated in order to foster responsible innovation by regulated financial institutions.

It is vital that robust investor protections should be at the forefront of all regulatory modernization efforts in order to build confidence in these new products and technologies. Any framework should also adopt a technology neutral approached based on "same risk, same

[12] Exec. Order No. 14067, 87 Fed. Reg. 40881 (July 8, 2022); White House, Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (2022).

[13] U.S. Department of Treasury, Report on The Future of Money and Payments (2022); U.S. Department of Treasury, Report Crypto-Assets: Implications for Consumers, Investors, and Businesses (2022); U.S. Department of Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets (2022); Press Release, Janet Yellen, Sec'y, U.S. Department of Treasury, on the Release of Reports on Digital Assets (Sept. 16, 2022); U.S. Department of Justice, Office of the Attorney General, The Role Of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets (2022); Press Release, U.S. Department of Justice, Justice Department Announces Report on Digital Assets and Launches Nationwide Network (Sept. 16, 2022); U.S. Department of Commerce, Responsible Advancement of U.S. Competitiveness in Digital Assets (2022); Press Release, Statement from Gina M. Raimondo, Sec'y, U.S. Department of Commerce, Responsible Advancement of U.S. Competitiveness in Digital Assets Report Release (Sept. 16, 2022); Financial Stability Oversight Council (FSOC), Report on Digital Asset Financial Stability Risks and Regulation (Oct. 3, 2022).

activity, same regulatory outcome" principle, acknowledging that there are important differences between types of digital asset products, applications and activities that do not allow for a "one-size-fits-all" approach to regulation. It is also important that in any regulatory modernization effort that regulators recognize the differences between blockchain-native assets and the use of blockchain technology to facilitate traditional asset transactions given the significantly different risk profiles inherent of each activity.[14] Finally, to the extent possible, U.S. policymakers should also work towards regulatory interoperability between jurisdictions, to support the cross-border role of many digital asset market participants and support the competitiveness of U.S. capital markets and firms.

6. Updating Standards

SIFMA welcomes the OSTP's interest in supporting development of industry standards. The Federal government can play a critical role in responsible digital asset innovation by supporting the modernization of existing technology and operational standards to accommodate DLT. Standards provide common practices that firms can apply to demonstrate that they are understanding and managing risk appropriately. Updated standards are particularly valuable in providing common industry approaches to understanding and managing risk that can allow users of DLT to demonstrate that they are using this technology in ways that meet the expectations of their clients, counterparties, and regulators.

SIFMA encourages NIST to continue its investment in open-source research and initiatives focused on producing technical standards and guidance. In particular, SIFMA members look forward to building on standards under development such as:

- The use of blockchain technology (Blockchain | NIST);
- Cryptographic techniques particularly around threshold schemes that firms may use in the future such as multiparty computation (Multi-Party Threshold Cryptography | CSRC (nist.gov)); and
- Updating standards and certifications (such as FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov) – FIPs) to include considerations for blockchain technology. [15]

SIFMA also encourages NIST and other standard setters to explore how specific cybersecurity standards or approaches could guide interactions with public permissionless blockchains (such as more guidance for the application of these technology configurations under NIST's

[14] These points were discussed in more detail in SIFMA, Prioritizing Investor Protection and Existing Regulatory Frameworks in Digital Asset Legislation, Letter to Senate Banking Committee, Senate Agriculture Committee, House Financial Services Committee, and House Agriculture Committee (Oct. 11, 2022). See also Peter Ryan, "U.S. Digital Assets Policy Should Prioritize Investor Protection and Build Upon Our Robust Regulatory Frameworks," SIFMA Blog, November 16, 2022, available at: US Digital Assets Policy Should Prioritize Investor Protection and Build Upon Our Robust Regulatory Frameworks - SIFMA - US Digital Assets Policy Should Prioritize Investor Protection and Build Upon Our Robust Regulatory Frameworks - SIFMA.

[15] National Institute for Standards and Technology (NIST) Blockchain Projects, available at: https://www.nist.gov/blockchain; NIST Multi-Party Threshold Cryptography Project, available at: https://csrc.nist.gov/Projects/threshold-cryptography; NIST Security Requirements for Cryptographic Modules Project, available at: https://csrc.nist.gov/publications/detail/fips/140/2/final

cybersecurity framework, which is used by most financial institutions).[16] Additionally, research and development into interoperability of blockchain standards for banks as well as smart contract standards are valuable.

Beyond technical standards, accounting and valuation standards will likely need to be updated to account for unique features of new digital asset types and operating models. Finally, work on all standards development will be most effective if those efforts are coordinated internationally, both through engagement with international processes such as the International Organization for Standardization ("ISO") as well through bilateral and multilateral cooperation with other major jurisdictions.

7. CBDCs

SIFMA appreciates the RFI's questions on mechanics and design considerations for a potential U.S. CBDC. Before undertaking what would be "a highly significant innovation in American money," policymakers should be clear on why a U.S. CBDC is needed and what problems it would address. Once that is established, it is important to agree on a clear understanding of the many design considerations that would shape its impact and operations. These analyses should include, but would not be limited to, an evaluation of the effects of different types of CBDC systems on financial stability and the implementation of monetary policy; key short-term funding markets; existing payments systems, with which any CBDC would need to be interoperable; consumer privacy; as well as AML and sanctions regimes.

Given that much more study needs to be undertaken to properly understand these benefits and costs, SIFMA does not take a position in this letter on the desirability of adopting a U.S. CBDC, although SIFMA does believe that *if* policymakers were to move forward with adoption at some future point, after the appropriate steps above were completed, the primary focus should be on wCBDC. SIFMA encourages the OSTP to review the SIFMA comment letter in response to the Federal Reserve Board discussion paper "Money and Payments: The U.S. Dollar in the Age of Digital Transformation."[17]

SIFMA also encourages policymakers to explore a careful review of whether the goals of a wCBDC might best be accomplished through regulated commercial models which are already available or under development and proving effective. Analysis should cover a broad range of models which could meet the objectives that policymakers seek to achieve through a potential digital dollar. For example, these could include various systems of private tokens, tokenized cash, bank-minted tokenized deposits referencing fiat currency on blockchain, or the Regulated Liability Network (RLN) proposal to tokenize central bank, commercial bank, and electronic money on the same chain to deliver a next generation digital money format based on national currency units.[18] . SIFMA's response to the Treasury Department's Request for Comment on

[16] National Institute for Standards and Technology (NIST) Cybersecurity Framework, available at: https://www.nist.gov/cyberframework

[17] SIFMA response to the Federal Reserve Board of Governors discussion paper entitled "The U.S. Dollar in the Age of Digital Transformation," May 2022, available at: https://www.sifma.org/resources/submissions/cbdc-discussion-paper-response/

[18] For example, as proposed, these "RLN tokens" could be readily exchanged with existing account-based forms. Policymakers should explore if and how these alternative technology configurations could meet the objectives of a CBDC, such as the instant movement of value 24/7 either domestically or internationally, integrated into other

"Ensuring Responsible Development of Digital Assets provides a more extended discussion of the potential role of private sector alternatives to a CBDC.[19]

8. Public-Private Partnerships

As the OSTP looks to move forward with its research agenda for the responsible development of digital assets, SIFMA strongly recommends the formation of a public-private working group/task force to help drive analysis and accelerate the policy changes that are needed for broader adoption and responsible innovation. We believe there is great value in the public sector working with the private sector users of blockchain technology, to understand the use cases and technology configurations which are most relevant and the design considerations and regulatory challenges that shape financial institutions' work. Including representatives of regulated financial institutions in any public-private working group would be particularly valuable given SIFMA's members' perspective as responsible users of the technology who are trying to innovate within a controlled and regulated environment.

digitized processes, and serve as "programmable money" insofar as payments can be automated or made conditional on events.[18]

[19] SIFMA response to Treasury Department's Request for Comment ("RFC") on "Ensuring Responsible Development of Digital Assets," August 2022, available at: https://www.sifma.org/wp-content/uploads/2022/08/Ensuring-Responsible-Development-of-Digital-Assets.pdf

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Stardust Labs

To Whom It May Concern:

My name is Adit Patel, CEO and Founder of Stardust Labs. Stardust Labs is a distributed ledger research organization funded by the United States' National Science Foundation. (Award ID: 2213017 [https://www.nsf.gov/awardsearch/showAward?AWD_ID=2213017]).

We are responding to "Request for Information; Digital Assets Research and Development" as we believe the U.S. is overlooking the impact this technology could have with military applications. DLT could quickly remedy the existing weaknesses of America's geopolitical enemies to the detriment of US National Security.

Attached below is a quick summary:

"Amateurs talk about tactics, but professionals study logistics."
– Gen. Robert H. Barrow, USMC (Commandant of the Marine Corps) noted in 1980

Since the advent of organized warfare, the effectiveness of a military force has always been in lockstep with the efficiency of its logistics and procurement. The world class logistics of the US military are an asymmetric advantage that has on multiple occasions led to US victory in spite of sub-optimal operational decisions and poor tactics. (https://thestrategybridge.org/the-bridge/2022/6/14/asymmetric-advantage-or-achilles-heel-logistics-in-the-us-military)

In the most recent kinetic action on the Ukraine boarder, the Russian army failed to achieve its strategic objectives almost entirely due to endemic corruption that crippled their logistic chains. Russia began this invasion with a military an order of magnitude larger than Ukraine's, however even that overwhelming advantage was completely overcome by the disadvantages of corruption and poor logistics.

China is closely watching the invasion to learn lessons from Russia's logistical failure. However, Xi Jinping is already well aware of the impact of inefficient logistics in military structures and has heavily focused on eliminating corruption in the military over the past decade. (https://www.scmp.com/news/china/military/article/3196292/xi-says-chinas-military-must-push-political-education-anti-corruption-efforts) However, this is a task much easier said than done, corruption in military organizations is notoriously difficult to manage. (https://www.imf.org/external/pubs/ft/wp/2000/wp0023.pdf). It is particularly difficult in authoritarian regimes, as their leaders cannot adopt western doctrines of independent oversight in the military as it would serve as a potential challenge to their power.

In brief, corruption in Russia's and China's military is endemic (https://www.politico.eu/article/russia-military-corruption-quagmire) and difficult to eliminate given their rigid command structure, centralized authority and the absence of independent oversight. Most efforts to reduce corruption have failed as centralized measures are simple to circumvent through further bribes or threats, which ironically have further exacerbated the issue. (https://www.youtube.com/watch?v=i9i47sgi-V4)

Solving these systemic issues is at the forefront of Chinese strategy over the next decade and why Xi Jinping stressed China would "continue its unprecedented anti-corruption campaign within the People's Liberation Army" at China's 20th party congress.

DLT, or a Central Banking Digital Currency (CBDC), could rapidly solve the problems of corruption in Russia's and China's military without requiring liberalization. Powering military logistics, procurement, and sustainment with this technology could let our geopolitical rivals quickly identify corruption and dramatically increase the effectiveness of their military logistics, heightening their threat to U.S. national security in any future conflicts.

DLTs are perfect for eliminating corruption in military logistics as corrupt individuals can't bribe or threaten a distributed ledger node, nor can they falsify the data. Every action results in a fingerprint on the decentralized ledger that would allow an authoritarian regime to oversee every transaction without creating a power center or a centralized oversight committee that could potentially rival them. By employing even a single node, the central office can completely eliminate the ability to falsify audits and reports and track every every quantum of currency through every transaction.

As an illustrative example, with DLT powered military logistics and sustainment, Xi Jinping can track the capital central command issued for a PLA's tank division's IR upgrade packages from authorization, through the division, the tank manufacturer, all the way down to the individual suppliers and component manufacturers. With a CBDC that would extend all the way down to the individual RMB in the workers digital wallet. If the capital ever exits that chain at any point, becomes involved in suspicious transactions, or quality gaps are found during inspections, DLT gives indisputable proof of corruption and allows you to quickly trace it back to the offending party. Over time this will allow the PLA to quickly root out systemic corruption and dramatically improve military effectiveness and readiness.

The United States excels at military logistics and has a military largely free of corruption. Many of the above benefits are negligible for the U.S. military. Recent DoD research into blockchains has been focused on marginal improvements for supply chain tracking and has completely overlooked its disruptive effects on corruption and the advantages it has for our geopolitical adversaries from their perspectives. (https://apps.dtic.mil/sti/pdfs/AD1107534.pdf & https://www.army.mil/article/227943/blockchain_for_military_logistics). We believe DLT and a CBDC would have incredible benefits for Russia's and more specifically China's military given the challenges they face today.

That being said, there may be some advantages for the U.S. to explore this technology for its own efforts training allies. Corruption in foreign militaries has deeply affected how effective the US has been at training units in countries such as in Afghanistan that are plagued by corruption. (https://www.theatlantic.com/ideas/archive/2021/08/us-afghanistan-taliban-training/619774/) This is a problem that has the potential to extend even to the Ukrainian military in the long-term. DLTs designed for military logistics, might serve as an efficient way for the U.S. to maintain oversight without creating friction in every transaction.

In summary, this formal comment urges the Office of Science and Technology Policy (OSTP) to pay closer attention to the military applications of this technology with a particular focus on the impacts it could have in modernizing and enhancing the capabilities of the militaries of the United States' chief geopolitical rivals, Russia and China.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Stellar Development Foundation ("SDF")

Stellar Development Foundation

[redacted]

Nik Marda
Anna Brady-Estevez
James Joshi
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
[redacted]

Submitted via: DARD-FTAC-RFI@nitrd.gov

March 3, 2023

Subject: **RFI Response: Digital Assets R&D Agenda (88 FR 5043; Document Number 2023-01534)**

To Whom It May Concern:

The Stellar Development Foundation ("SDF") submits this letter in response to a Request for Information (RFI) on "Digital Assets Research and Development," which was made by the Office of Science and Technology Policy (OSTP) on January 26, 2023.[1] Like the RFI itself, this letter builds upon terms and subject matter defined in Executive Order 14067 (issued on March 9, 2022, and entitled "Ensuring Responsible Development of Digital Assets").[2] The RFI covers six specific topics and invites general input on research and development related to digital assets.

SDF appreciates that OSTP is carefully studying this emerging and complex field, as part of an interagency process. Digital assets have the potential to fundamentally transform how people across the world think about and use money, and to expand access to fast, affordable, and transparent financial services for all. The term "digital assets" is broadly defined by Executive Order 14067 and captures a wide range of tokens, technologies, services, and projects – including stablecoins and central bank digital currencies.[3] Those digital assets may serve different purposes and use cases, have different pros and cons from a policy perspective, and are all likely to co-exist, overlap, and in some cases inter-operate in the years ahead. As a whole, the U.S. government has a critical role to play in shaping the evolution of the digital assets sector and promoting financial stability, consumer protection, and responsible innovation -- while also reinforcing U.S. global leadership and preserving national security.

---

[1] Office of Science and Technology Policy, *Digital Assets Research and Development: Request for Information*, 88 FR 5043 (Jan. 26, 2023), https://www federalregister.gov/documents/2023/01/26/2023-01534/ Request-for-information-digital-assets-research-and-development.

[2] Executive Office of the President, *Ensuring Responsible Development of Digital Assets*, 87 FR 14143 (Mar. 14, 2022), https://www.federalregister.gov/documents/2022/03/14/2022-05471/ ensuring-responsible-development-of-digital-assets (hereinafter, the "Order" or "Executive Order").

[3] Executive Order at Sec. 9(c)-(d).

OSTP, in particular, is uniquely positioned to examine the technical dimensions of digital assets and the engineering implications of developing digital asset systems for particular contexts. Specifically, this letter addresses two key points for OSTP's consideration:

(1) Software interoperability and the ways in which OSTP and the broader federal government could explore and develop the benefits of enabling digital assets and digital asset systems to freely interoperate; and

(2) Novel forms of programmability of digital assets, which OSTP should research, particularly as it pertains to future government programs and services.

We hope this material is useful for OSTP's ongoing efforts.

Stellar Development Foundation

By way of background, SDF is a US-based nonstock, nonprofit organization that contributes to the development and growth of the Stellar network ("Stellar") and the "Stellar ecosystem" – the individuals, developers, and businesses who build on or interact with Stellar. Stellar is an open-source network that connects the world's financial infrastructure. Founded in 2014, SDF helps maintain Stellar's codebase, supports the technical and business communities building on the network, and serves as a speaking partner with policymakers, regulators, and institutions. Our mission is to create equitable access to the global financial system, using the Stellar network to unlock the world's economic potential through blockchain technology.

From a technology standpoint, Stellar offers a decentralized, fast, scalable, and sustainable network for financial products and services. It is both a cross-currency transaction system and a platform for digital asset issuance that offers unique, robust asset issuer controls. Financial institutions and fintechs worldwide issue assets and settle payments on the Stellar network, which has grown to more than 7 million accounts. As of February 2023, over 10 billion operations have been processed on the Stellar network.

In Washington, D.C., SDF has engaged in public commentary, Congressional testimony,[4] committee briefings,[5] and proactive consultations with U.S. lawmakers, administration officials, and regulators, both one-on-one and through industry associations.

(1) The federal government should promote interoperability among digital assets, including through the development of standards and in consultative public forums.

Interoperability among technology products and platforms – including in the digital assets space – benefits the public interest. The government should explore technical and standard-setting measures to

[4] *See, e.g.*, Stellar Development Foundation, *Digital Assets and the Future of Finance: Testifying Before the US House Committee on Financial Services*, SDF Blog (Dec. 8, 2021), https://www.stellar.org/blog/digital-assets-and-the-future-of-finance-testifying-before-the-us-house-committee-on-financial-services?locale=en.
[5] *See, e.g.*, Stellar Development Foundation, *House Financial Services Committee Briefing Takeaways*, SDF Blog (Sept. 28, 2020), https://www.stellar.org/blog/sdf-on-capitol-hill?locale=en.

promote interoperability among digital assets, as well as between digital asset systems and traditional financial systems.

In other technological contexts, both OSTP[6] and other federal entities[7] have repeatedly recognized the value and importance of interoperability, within the government, as part of particular government-supported programs, and across organizations and industries. For good reason: interoperability can promote competition, innovation, efficiency, and consumer rights. A prime example is the set of protocols and specifications that undergird the World Wide Web, known as the "Internet layer." At a practical level, interoperability at the Internet layer means that any person can open up nearly any web page from any device -- and that one email service readily can communicate with another.[8] At a higher level, that interoperability is central to the extraordinary growth of the Internet over the last thirty years and its revolutionary potential. SDF adheres to that same principle of interoperability today.

The affirmative benefits of interoperability extend to the digital assets space. Namely, being able to quickly, easily, and safely exchange digital assets or move them from one platform, financial institution, or wallet to another is generally good for consumers and markets alike. These forms of interoperability –

---

[6] *See, e.g.*, OSTP, "Request for Information on Advancing Privacy-Enhancing Technologies," 87 Fed. Reg. 35250, 35252 (June 9, 2022) (seeking information where Privacy-Enhancing Technologies might assist in data portability and interoperability); OSTP, "Request for Information on Data Collection for Emergency Clinical Trials and Interoperability Pilot," 87 Fed. Reg. 65259, 65260 (Oct. 28, 2022) (seeking input on "Fast Healthcare Interoperability Resources . . . in the pre-emergency phase as well as in an emergency setting."); Director John P. Holdren, OSTP, "Memorandum for the Heads of Executive Departments and Agencies" (Feb. 22, 2013) https://www.osti.gov/ostp-public-access-memo-2013 (discussing why scientific publications and data must contain features that encourage innovation in interoperability and accessibility).

[7] *See, e.g.*, "Federal Cybersecurity Research And Development Strategic Plan," National Science & Technology Council, Cyber Security And Information Assurance Interagency Working Group Subcommittee On Networking & Information Technology Research & Development Committee On Science & Technology Enterprise (Dec. 2019), https://www nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf (outlining how the government can, *inter alia*, "expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.") (citations omitted); U.S. National Artificial Intelligence Office, "Advancing Trustworthy AI," 2022, https://www.ai.gov/strategic-pillars/advancing-trustworthy-ai/ (discussing "[m]etrics, assessment tools, and technical standards are essential for ensuring that AI technologies meet critical objectives for functionality and interoperability"); NIST, "Smart Grid National Coordination" (Jan. 6, 2021), https://www.nist.gov/programs-projects/smart-grid-national-coordination (discussing a "national public-private stakeholder partnership effort to accelerate development of interoperability standards for the smart grid, fulfilling NIST's statutory responsibility under the Energy Independence and Security Act of 2007"); U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review* at S-7 (Jan. 2017), https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review%20Summary%20for%20Policymakers.pdf ("Interconnection standards and interoperability are critical requirements for seamless integration of grid-connected devices, appliances, and building energy-management systems, without which grid modernization and further energy efficiency gains may be hindered"); U.S. Department of Commerce, "Spectrum Policy For The 21st Century: The President's Spectrum Policy Initiative: Report" (June 2004), https://www ntia.doc.gov/legacy/reports/specpolini/presspecpolini_report1_06242004.htm (recommending that "[t]he Department of Homeland Security (DHS) and NTIA as well as the Office of Science and Technology Policy (OSTP) … coordinate with the Departments of Defense, Justice, Agriculture, and the Interior and other appropriate federal agencies and entities, including the FCC, to develop and implement a plan to address the spectrum needs of federal, state, and local communication interoperability and the continuity of government operations in light of continuing terrorist threats, emergencies, and day-to-day operations.").

[8] *See e.g.,* Sukhi Gulati-Gilbert et al., *Preserving the Open Internet Through Interoperability*, Center for Democracy & Technology (July 21, 2022), https://cdt.org/insights/preserving-the-open-internet-through-interoperability/.

both across blockchains and between blockchain networks and traditional financial systems – fosters consumer choice, competition and innovation among private companies, asset liquidity, and convenience in payment mechanisms.

The principle of interoperability is particularly important because we expect there will continue to be multiple digital asset types and providers, both private and public alike. In the years ahead, we assume that several types of digital currencies will co-exist and be exchanged for one another, and will also interact with fiat currencies, including: (1) privately issued digital currencies, both centralized and decentralized (such as Bitcoin and Ethereum); (2) fiat-backed stablecoins (such as USD Coin); and (3) central bank digital currencies (CBDCs). We detailed these forms of co-existence in our August 8, 2022, letter to the U.S. Treasury Department.[9]

While we understand that the U.S. government has not yet made a decision about whether to pursue its own CBDC,[10] we know that several other U.S. allies are moving forward with CBDC development,[11] and that other stablecoins remain in wide circulation.[12] There too, interoperability remains functionally important for consumers and potentially strategically important for the U.S. Moreover, Washington should take on a leadership role in setting global standards on interoperability and encourage the development of CBDC standards that allow for these currencies to interact with one another, regardless of underlying system or protocol. Likewise, the Board of Governors of the Federal Reserve System has also noted the value of interoperability in some of its recent reports.[13]

The Stellar network itself is designed with interoperability in mind. As an open, interoperable payments platform, Stellar has robust documentation, software tools, and a developer community that support quick integration with and connection to the network. The core protocol is complemented by ecosystem proposals (SEPs) that facilitate interoperability between financial entities connected to blockchain infrastructure and the traditional banking system. Through these SEPs, the Stellar ecosystem is unique in focusing on connections between traditional financial markets and decentralized finance. For

---

[9] *See* SDF, *Ensuring Responsible Development of Digital Assets; Request for Comment (87 FR 40881; Document Number 2022-14588)*, Letter to the U.S. Treasury Department (Aug. 8, 2022), https://resources.stellar.org/hubfs/SDF%20Treasury%20Comment%20Letter%20-%208-8-22.pdf; SDF, *"We Must Prioritize Interoperability Going Forward:" SDF's Response to Treasury's Request for Comment* (Aug. 8, 2022), https://stellar.org/blog/response-to-the-treasury-on-digital-assets.

[10] *See e.g.*, Inbar Preiss, *The Fed has 'not decided to proceed' with a digital dollar, says Powell*, The Block (Sept. 27, 2022) https://www.theblock.co/post/173111/the-fed-has-not-decided-to-proceed-with-a-digital-dollar-says-powell; *cf.* Governor Christopher J. Waller, *The U.S. Dollar and Central Bank Digital Currencies*, Symposium of the Harvard National Security Journal (Oct. 14, 2022), https://www federalreserve.gov/newsevents/speech/waller20221014a.htm.

[11] *See generally* Atlantic Council, *Central Bank Digital Currency Tracker* (2022), https://www.atlanticcouncil.org/cbdctracker/ (last visited Feb. 27, 2022).

[12] *See generally* CoinMarketCap, *Top Stablecoin Tokens by Market Capitalization* (last visited Feb. 27, 2022), https://coinmarketcap.com/view/stablecoin/.

[13] *See* Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation* at 15 (Jan. 2022) ("CBDC has the potential to streamline cross-border payments by using new technologies . . . and creating additional opportunities for cross-jurisdictional collaboration and interoperability."). *See also* U.S. Department of Treasury, *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067* at 22 (Sept. 2022) ("Interoperability between central-bank operated payment systems is relatively uncommon today due to the risks and technical complexity, as well as considerations related to jurisdictions' economic governance, rule of law, national security, and the need to align regulations").

example, SDF and its partner MoneyGram International in 2022 announced MoneyGram Access, a first-of-its-kind global on/off-ramp service for digital wallets utilizing the Stellar network. With the launch of this program, digital wallet users can now move seamlessly from cash to digital assets to cash again–all without requiring a bank account or credit card yet still subject to local compliance standards. MoneyGram International agents, as the designated on- and off-ramps, perform required compliance screening, ensuring that strong know-your-customer mechanisms remain in place. MoneyGram Access creates an important bridge between digital assets and cash, demonstrating that blockchain can – and should be – interoperable with traditional financial infrastructure.

Conversely, the *lack* of interoperability can cause serious problems both within and outside of the digital asset context. Outside the context of digital assets, systems and software that cannot interoperate often cause costly outages and malfunctions and serious emergencies.[14] Within the universe of digital assets too, when large-scale digital assets systems are not interoperable, it can cause considerable inefficiency for consumers, market fragmentation, or liquidity issues (in the case of tokens that are traded).[15] For open source digital asset projects, interoperability can be exacerbated by the problem of orphaned code, which arises when a piece of software continues to be used, but the engineers who originated or maintained it are no longer involved or around.[16] Indeed, promoting the continued interoperability and vitality of open source projects also aligns with this Administration's examination of how to "prioritize the most important open source projects and put in place sustainable mechanisms to maintain them."[17]

Furthermore, the history of the Internet also underscores the broader significance of interoperability for frontier technologies. I have direct experience with the critical role interoperability plays in fostering innovation and accessibility. Prior to becoming CEO and Executive Director of SDF, I served as the Chief Operating Officer of Mozilla, the maker of the free and open-source Firefox web browser. At Mozilla, I advocated for the need for openness and interoperability in technology. My experience there shaped my understanding of the importance of common standards that allow systems to freely interact with one another. Today, at SDF, I continue to push for these same values of openness and interoperability in the blockchain industry, so that we can encourage competition and innovation – just as we did in the early days of the Web. Interoperability at the Internet layer has made the world a different and better place. This same

[14] *See, e.g.*, Ajay Harish, *When NASA Lost a Spacecraft Due to a Metric Math Mistake*, SimScale Blog (Oct. 17th, 2022), https://www.simscale.com/blog/nasa-mars-climate-orbiter-metric/; Bipartisan Policy Center, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* at 14 (Sept. 2011) (examining the 9/11 Commission's recommendation on radio interoperability for first responders' communications systems), https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/CommissionRecommendations.pdf; Michael P. Gallaher et al., *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry*, NIST (Aug. 2014), https://nvlpubs nist.gov/nistpubs/gcr/2004/nist.gcr.04-867.pdf ("Inadequate interoperability increases the cost burden of construction industry stakeholders and results in missed opportunities").
[15] Currently, the digital asset ecosystem includes thousands of tokens in various shapes and sizes, some of which may decrease in popularity, become obsolete, or be subject to regulation. SDF does not mean to suggest that interoperability between and among *all* of these tokens and their corresponding projects or products is equally necessary or beneficial, for the federal government or otherwise.
[16] *See, e.g.*, Klint Finley, *Giving Open-Source Projects Life After a Developer's Death*, Wired (Nov. 6, 2017), https://www.wired.com/story/giving-open-source-projects-life-after-a-developers-death/.
[17] *See* White House, *Readout of White House Meeting on Software Security* (Jan. 13, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/; Andrew Martin, *White House Enlists Software Industry to Improve Open-Source Security*, Yahoo News (Dec. 23, 2021), https://finance.yahoo.com/news/white-house-enlists-software-industry-213026544 html.

commitment to interoperability must guide our approach to digital assets. Without it, we will end up with less innovation and more concentrated ownership in the industry – much like what we have seen develop in the content layer on the web. Blockchain technology has the potential to enhance the current financial infrastructure by eliminating fragmentation and reducing barriers to access. But to make this a reality, we need policies that intentionally promote and encourage interoperability. The Biden Administration therefore has an essential role to play in shaping the future of the blockchain industry and the digital assets space, and in laying the groundwork for blockchains and traditional payments and banking infrastructure to interoperate. The United States can be a leader in building a truly open and accessible financial system. I applaud the U.S. government's efforts so far to direct research and development on interoperability and look forward to seeing how that informs global standards.

More specifically, the role of World Wide Web Consortium (W3C) in the early days of the Internet is a useful analogy for the digital asset realm, since W3C was pivotal in developing critical Internet technologies and ultimately ensuring the success of the Web. Over the years, W3C has fostered the development of hundreds of open standards in fair, free, and consensus-driven processes and has long valued interoperability as a critical design principle.[18] The U.S. government has supported W3C in various ways, including in 1994 through seed funding from DARPA (alongside the European Commission), and today through continued membership in W3C (e.g., by NIST and the Defense Information Systems Agency).[19] Nonetheless, the U.S. government has rightly been careful in balancing its support and leadership with W3C's independence and the benefits of an open, predominantly non-governmental community, and has shown important restraint in avoiding the creation of policies or regulations prematurely. Key to the development of common standards through W3C is that no one company (or entity) owns or controls the process or product.

Specifically, OSTP and the U.S. government should:

- Promote interoperability as a significant federal prerogative, including identifying areas that could benefit from greater interoperability and common technical standards, such as data portability, message forms, and digital identity.

- Conduct a review of core government processes to determine where digital assets projects may improve operational efficiencies and service provision (e.g., procurement, digital identification, CBDCs, etc.), and task relevant agencies and departments as well as industry groups to develop potential standards and interoperability solutions.

- Encourage U.S. federal agencies and departments that participate in the Small Business Innovation Research and the Small Business Technology Transfer programs–including but not limited to the Department of Commerce, the Department of Defense, the Department of Energy, the Department of Homeland Security, the Environmental Protection Agency, and the National Science

[18] *See generally* W3C, *W3C to become a public-interest non-profit organization* (June 28, 2022), https://www.w3.org/2022/06/pressrelease-w3c-le.html.en; Karl Dubost, *Open Standards Interoperability*, W3C Blog (May 20, 2008), https://www.w3.org/blog/2008/05/open-standards-interoperability/.
[19] *See, e.g.*, W3C, *Facts about W3C,* https://www.w3.org/Consortium/facts; W3C, *Current* Members, https://www.w3.org/Consortium/Member/List.

Foundation–to designate awards under these programs to support research on interoperability solutions for the digital assets industry.

- In collaboration with National Institute of Standards and Technology (NIST), elements of the Federal Reserve, and other relevant U.S. government entities, explore technical measures that would allow digital assets, including a potential wholesale or retail CBDC, to implement principles of interoperability. Consider setting up an interagency task force on interoperability, particularly as other pilot programs evolve.

- Assert U.S. leadership in open and transparent organizations that develop technical standards regarding payments and/or digital assets, such as the World Wide Web Consortium and other multilateral, public fora.

- Carefully examine the potential downsides of interoperability among digital assets in instances of market contagion or high-profile cyber-security breaches.[20] In many instances, OSTP may find pre-existing tools and techniques that can help limit contagion and detect security breaches.

(2) <u>The programmability of digital assets could serve various public purposes, which OSTP and other relevant federal agencies and departments should research through hands-on experimentation and applied demonstrations.</u>

Federal agencies have recognized the overarching significance of programmability in various technological settings.[21] In the digital asset context too, there is a growing appreciation among policymakers that programmability offers unique and tangible benefits -- for public and private infrastructure alike.

---

[20] *Accord* U.S. Department of Treasury, *The Future of Money and Payments*, *supra*, at 33 ("There are some countervailing considerations, however. As noted, high levels of interoperability between CBDCs could introduce counterparty, operational, and cyber risks.").

[21] *See, e.g.*, Department of Defense, "DoD Digital Modernization Strategy" (July 12, 2019), https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF (emphasizing "network technology aimed at making the network as agile and flexible [through] . . . . network virtualization, and automation through programmability."); NIST, "Guide to Operational Technology (OT) Security: Initial Public Draft," NIST Special Publication NIST SP 800-82r3, p. 202 (April 2022) (discussing networking technology that "acts as an abstraction layer for network programmability . . . ."); U.S. Department of Energy, "Transition 2020: Issue Papers," at 79-80 ("Over the past decade, DOE has become aware that future-generation systems will require significant changes in how high performance computers are designed, developed and programmed. . . . . To mitigate this complexity, a portion of the R&D investments will create tools that improve the programmability of exascale computers.").

Indeed, this has recently been the focus of reports and remarks at the Federal Reserve, Treasury Department,[22] and Bank for International Settlements.[23]

One of the unique benefits of digital assets, whether created by a private issuer or a public entity, is that they can offer novel forms of programmability that are not feasible with traditional physical assets or existing forms of fiat currency. For example, programmable digital assets can allow for scheduling, targeting, instant swapping, conditional transfers, and escrow-like functionality. Programmability could also introduce other innovations, like automatically initiating payments on the confirmed receipt of goods, routing tax payments directly to tax authorities at point of sale, and recording the ownership and transfer of stocks and other assets. Payment of interest on treasury securities could be automated using smart contracts–instead of the manual process used today–or payments for goods and services could be disbursed automatically following the completion of specified benchmarks or milestones. Many of these functionalities are simply not possible with paper money or physical coins.

Programmability can also enhance safety and certainty for issuers. For example, the Stellar network already offers asset issuers a selection of programmable features designed to improve consumer protections and limit fraud. These innovative solutions include clawbacks that allow issuers to reverse transactions in cases of fraud or error, and an "authorization required" feature that give issuers the ability to verify that an asset holder has fulfilled compliance requirements set by the issuer, such as local know-your-customer and anti-money laundering obligations before an asset is transferred. This model may be particularly relevant to the RFI's query about ensuring "fraud-resistant transaction programmability receive appropriate levels of R&D support."[24]

These forms of programmability may benefit U.S. interests and policy initiatives in various ways, particularly around cash assistance and other social benefits. Cash-based social programs -- like CalWORKS in the State of California and Temporary Assistance for Needy Families in Washington, DC, as well as the U.S. government's provision of COVID relief payments in 2020 and 2021 -- play an important role in helping individuals and families meet their basic needs. Programmability can allow local, state, and federal government agencies to precisely target support to those who need it most, and encourage increased efficiency, transparency, and convenience. Programmability also allows for the automation of microlending schemes, livelihood programs, and interventions for specific, vulnerable groups such as pregnant women

---

[22] *See, e.g.,* Board of Governors of the Federal Reserve System, Money and Payments: The U.S. Dollar in the Age of Digital Transformation 14 (Jan. 2022) ("a CBDC could potentially be programmed to, for example, deliver payments at certain times"); Alexander Lee, *What is programmable money?*, FEDS Notes 2021 (June 23, 2021); U.S. Department of Treasury, *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067* at 21 (Sept. 2022) (a CBDC "could also facilitate the use of transaction programmability, to allow for additional functionality of money. For example, payroll, government, or bill payments could be automated using CBDC, similar to how ACH works today, or new functions could be designed to facilitate micro and machine-to-machine payments.").

[23] *See also* Agustín Carstens, *Innovation and the future of the monetary system*, Bank for International Settlements (Feb. 22, 2023) ("there is great promise in developing the idea of a 'unified ledger' with a common programming environment . . . . Such a ledger allows for the use of smart contracts and composability. . . . With these new functionalities, any sequence of transactions in programmable money can be automated and seamlessly integrated. This reduces the need for manual interventions that delay transactions and reduces dependency on intermediaries, and also allows for simultaneous and near-instant payments and settlement.").

[24] RFI, *supra* at 5044.

and the formerly incarcerated. Federal agencies could use programmable assets to help with the allocation and administration of government benefits or the real-time, targeted distribution of economic stimulus funds. In certain scenarios, the government could also consider conditional or time-delimited asset transfers (e.g., benefits that must be used within nine months; or forms of "helicopter money").[25]

SDF has seen first-hand the ways in which programmability can add value in the context of international humanitarian aid and cash assistance programs. In collaboration with leading international aid organizations, SDF launched Stellar Aid Assist in December 2022, a first-of-its-kind disbursement system powered by the Stellar network to help aid organizations deliver urgently needed cash assistance to vulnerable populations quickly and transparently. Stellar Aid Assist enhances aid organizations' existing cash assistance efforts by leveraging digital wallets and a digital asset, such as the USDC. The use of a digital dollar provides a stable store of value and gives individuals the ability to exchange for local currency anywhere in the world through the MoneyGram network or other available offramps. Individuals remotely receive the digital dollars and hold them securely over time in a digital wallet, giving aid organizations an alternative to providing physical cash. It does not require a bank account, debit card, or credit card and provides recipients with a more secure place to hold and transport funds until cash is needed. With 1.4 billion people unbanked worldwide, and more than 103 million people forcibly displaced, this is a critical new option for individuals who have historically been dependent on receiving and carrying physical cash. Using Stellar Aid Assist, recipients can manage their funds entirely on their phone, wherever they go. Additionally, the use of the Stellar public blockchain provides greater transparency for aid organizations and their donors through the traceability of funds. The United Nations Refugee Agency, UNHCR, and the International Rescue Committee announced live pilots of Stellar Aid Assist for displaced individuals in Ukraine in December 2022 using the USDC asset, Vibrant digital wallet, and MoneyGram network. The tool is provided free of charge to organizations by SDF and can be used in additional geographies.

Cash-based transfers programs are a common form of development assistance even outside of emergency settings. For aid and development organizations, programmability gives the benefit of greater oversight (i.e., aid could be returned and repurposed if the recipient is deceased) while not violating the basic principles of cash-based assistance. In the future, programmable digital cash could be used to fulfill donor mandates on aid allocation and to set conditions, for instance, on where recipients can spend aid funds. Programs can be designed with smart contracts to automatically release funds once a certain set of conditions is met, which could automate and streamline efficiency within the aid sector.

---

[25] *See generally* Hon. J. Christopher Giancarlo, Testimony to the House Committee on Financial Services, *Inclusive Banking During a Pandemic: Using FedAccounts and Digital Tools to Improve Delivery of Stimulus Payments* (June 11, 2020), https://www.congress.gov/116/meeting/house/110778/witnesses/HHRG-116-BA00-Wstate-GiancarloJ-20200611.pdf;. Justice Clark Litle, *Programmable Digital Currencies Are Coming - Here's What That Means*, NASDAQ (Aug. 18, 2020), https://www.nasdaq.com/articles/programmable-digital-currencies-are-coming-heres-what-that-means-2020-08-18 ("In terms of distributing stimulus or emergency funds, the U.S. government and Federal Reserve would have a level of fine-tuned control like never before. Payments could be sorted out by income level, employment status, geographical location, or any number of other things. Digital dollars would likely also be programmable in and of themselves, allowing for instant tax payments at the point of sale. Tax refunds and rebates could be instant, too.").

Specifically, OSTP and the U.S. government should:

- Initiate pilot projects to explore various scenarios in which programmability may improve U.S. government services and benefit consumers. This sort of hands-on experience and experimentation can inform and illuminate policy discussions and also help the private sector better understand governmental programs and interests.

- Research the potential applications of programmability in the context of government aid and other federal programs and benefits.

- Convene policymakers at the Federal Reserve, the Treasury Department, and the U.S. Agency for International Development to study and how programmability might apply in the context of monetary policy and foreign policy and to consider ways to beta-test such applications in a discrete and safe environment.

- Also carefully examine some potential downsides of programmability, especially in the context of the automated execution of code based on inaccurate information. Moreover, OSTP could analyze how programmable digital assets might interact with malicious code or other cyber-security risks (e.g., an attacker who takes advantage of pre-programmed payment schedule to siphon off funds). Some of these security downsides may be amenable to technical improvements. Finally, as part of the broader focus on privacy in Executive Order 14067, OSTP should analyze the potential privacy implications of certain forms of programmability and the ability to preserve cash-like features.

Under all circumstances, the more hands-on experience and trial-and-error that OSTP and other relevant agencies can have with programmable assets, the quicker the U.S. government can determine whether and which of these features may be worth deploying in public infrastructure or promoting in the private sector.

*　　*　　*

SDF appreciates the opportunity to respond to the RFI and would be pleased to provide additional information that OSTP might find useful. In the years ahead, different types of technologies and digital assets will come and go, coincide, evolve, and in some instances interoperate – with varying effects on federal objectives, for example around financial inclusion, consumer protection, national security, and systemic risk. We urge OSTP and the U.S. government writ large to research and develop forms of interoperability and programmability, as part of an overarching policy and regulatory framework that reflects the co-existence and complexity of the digital asset ecosystem.

Sincerely,

[redacted]

Denelle Dixon
Chief Executive Officer & Executive Director
Stellar Development Foundation

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Stephen Diehl

RE: Request for Information; Digital Assets Research and Development - Office of Science and Technology Policy (OSTP).

Stephen Diehl
Software Engineer
Member of Public

Addressing:

- Goals, sectors, or applications where digital assets introduces risks or harms
- Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets

Response*:*

When analyzing the opportunities and risks involved with digital assets, we must initially start with a rigorous ontology of the technologies and financial instruments involved, the regulatory remit they fall under, and the potential public harms that arise from their existence.

The definition of *digital assets* defined in the RFI is too broad to analyze in its entirety. As stated, it would include traditional regulated instruments represented digitally, such as commercial bank deposits, equities, and money market funds, in addition to novel instruments, such as CBDCs and crypto assets. Instead, we should demarcate these types of assets based on the type and purpose of the financial instrument and the goals of the issuer in a *technology-neutral* manner. The use of cryptographic technology does not fundamentally change the economics or risks of a financial offering. A security offered on a distributed ledger is still a security; while technology may change and evolve, the technological substrate for markets does not fundamentally alter the nature of markets themselves. Responsible innovation must adapt technology to harmonize itself with our laws; we should not adapt our laws around technology—especially around unproven or untested technologies with negative externalities that impact the public.

Cryptoassets (colloquially known as *cryptocurrencies*), such as Bitcoin, Ethereum, Dogecoin, and some 20000+ other offerings, represent an umbrella category of financial instruments with varying aims that are built on various peer-to-peer internet platforms. The most common platform for building crypto assets is a *public blockchain:* a software system that networks computers together to create a ledger of transactions denominated in a financial asset issued on the network. This network has no single point of failure and is built to be *censorship resistant,* such that no one party can interdict transactions or seize assets issued on the network. The network is also constructed to allow assets to be custodied by individual participants as bearer instruments where holding specific cryptographic keys imparts "ownership" of the bearer instruments. This property is also combined with a system in which all financial transactions have complete finality after issuance and cannot be reversed.

Similarly, crypto assets have varying financial goals; some attempt to be a form of money issued by non-state entities (sometimes called *private money*), others attempt to be financial assets for speculation, and others, such as *stablecoins*, attempt to become payment mechanisms pegged to national currencies. These three categories form the core of our analysis of the crypto ecosystem.

For the first category, crypto assets that attempt to be private money[9] ultimately hit up against the same limitations as previous historical attempts—such as those in early 18th century America—that private money and microcurrencies have found. The classic economics textbook definition of money is a financial technology with three key properties: a *store of value*, a *unit of account*, and a *medium of exchange*. A store of value refers to the ability of money to maintain its purchasing power over time. This means that the same amount of money today will be able to buy the same amount of goods and services in the future. A unit of account refers to the function of money as a means of measuring the value of goods and services. Prices for goods and services are typically quoted in terms of the currency being used, and this allows for easy comparison of the relative value of different items. A medium of exchange refers to the function of money as a means of facilitating transactions between buyers and sellers. Money is widely accepted in exchange for goods and services, and this allows for the efficient transfer of goods and services.

Crypto assets attempting to be private money ultimately fail the two aspects of the money test since they are wildly suboptimal stores of value and both inefficient[1] and ineffective[2] mediums of exchanges as compared to normal currencies like the dollar and euro. Most crypto assets have fixed or algorithmic distribution mechanisms that expand the money supply according to a preset formula that does not incorporate macroeconomic information and thus can never achieve price stability relative to exogenous supply and demand information. Therefore crypto assets have no mechanism to achieve price stability relative to baskets of domestic goods and services and inevitably exhibit extreme price volatility. Since there is no formal system that gives rise to the price formation of crypto assets, there is no known mechanism for the volatility of these crypto assets to be abated, and crypto assets will thus always exhibit extreme volatility, making them unsuitable as a mechanism for commerce except for situations where counterparties are willing to endure extreme risk because the transaction is part of illicit activity or there is no other payment mechanism available. For instance, a standard mortgage contract could never be denominated in a hyper-volatile crypto asset since it would expose both the issuer and borrower to extreme price risk and make servicing the loan and denominating the underlying property in the crypto asset prohibitively expensive as compared to simply denoting the contract in dollars.

Crypto assets presented as money are a recreation of historical “hard money systems,” which contradicts modern understandings of monetary economics. The policy of institutions such as the Federal Reserve and European Central Bank is predicated on the belief that monetary policy, through adjustments in the money supply and interest rates, can effectively stabilize the economy and mitigate the adverse effects of aggregate demand shocks. Hard money systems, on the other hand, prioritize maintaining a stable price level and limiting inflation, often at the expense of economic growth and stability. According to the modern economics perspective, a rigid commitment to hard money policies can limit the ability of policymakers to respond to changes in economic conditions, as they are unable to adjust the money supply in response to shifts in aggregate demand. This can result in persistent unemployment and ineffective[4] stabilization of the business cycle.

Hard money systems can lead to excessively tight monetary conditions, which can further exacerbate economic downturns and limit the ability of the economy to recover. Deflationary cycles often historically occurred frequently under hard money systems, as a rigid commitment to maintaining a stable price level can lead to excessively tight monetary conditions. This occurs because the central bank may be limited in its ability to respond to changes in economic conditions, particularly during periods of economic downturns, as it is unable to increase the money supply to stimulate demand. In a deflationary cycle, declining aggregate demand leads to a decrease in prices, which in turn leads to a decrease in consumer spending, as individuals expect prices to continue to fall in the future. This further exacerbates the decline in aggregate demand, leading to a persistent deflationary spiral which are have been historically highly destructive to economies.

The unstable economics and intrinsic volatility of crypto assets, combined with the lack of a central issuer and a legal framework that recognizes these assets' status to denominate private debts and collect taxes, make crypto assets unsuitable as a medium of exchange. The design of the underlying networks of crypto assets to be both censorship-resistant and hard transaction finality is also at odds with the accepted norms of our financial system, which allow courts to interdict specific transactions to adjudicate fraud and rearrange estates according to our laws. Hard transaction finality is also antithetical to basic consumer protections and fraud prevention mechanisms. which always requires a human in the loop to correct errors and have the option to reverse transactions. The underlying design of censorship-resistant crypto assets is thus incompatible with the rule of law and national monetary sovereignty principles in its design.

The software architecture of crypto assets, with its key features of transaction finality, non-interdiction, and censorship resistance, creates a criminogenic context that fosters the growth of ransomware. Transaction finality ensures that once a transaction is confirmed on the blockchain, it cannot be reversed. This gives ransomware attackers a sense of security in knowing that the ransom payment they receive is guaranteed and cannot be taken back. The decentralized[5] and encrypted nature of crypto assets makes it difficult for authorities to monitor or disrupt criminal activity, providing a safe haven for ransomware attackers to operate without fear of intervention. Additionally, the censorship-resistant design of blockchains allows for the free transfer of funds, regardless of the purpose or origin of the transaction. This provides a means for ransomware attackers to receive payment without the risk of the transaction being blocked or censored by authorities, thus making it a favored payment method for ransomware attacks. From a US national security perspective, dark crypto flows pose a number of national security concerns:

1. **Terrorism financing**: Dark crypto money flows can be used to finance terrorism and support extremist groups, posing a significant threat to US national security.
2. **Illicit trade and sanctions evasion**: Cryptocurrencies can be used to evade sanctions[6] and trade embargoes, as well as to facilitate the trade of illegal goods, such as weapons and drugs, undermining US domestic and foreign policy objectives.
3. **Money laundering and tax evasion**: Cryptocurrencies can be used to launder money and evade taxes, draining resources from the economy and potentially financing criminal or destabilizing activities.

4. **Ransomware**: The anonymity and decentralization provided by cryptocurrencies can make it easier for attackers to carry out ransomware attacks, extort payments, and steal sensitive data from US enterprises. These attacks can result in significant financial losses and damage to the reputation of the affected companies, undermining the competitiveness and stability of the US economy.

For the second category, crypto assets are presented as a form of investment that can be speculatively traded and held for its perceived value. However, the mechanics of such schemes rest on dubious economic assumptions. Unlike a stock or bond, a crypto asset offering does not represent a legal claim on any assets or future cashflows; the crypto asset itself fundamentally has no income and no intrinsic value, and its price is purely the expectation of what another market participant will pay for it based purely on sentiment. This type of investment scheme, sometimes called *Ponzi financing* or the *greater fool theory*, is fundamentally dependent on an ever-increasing inflow of new money into the market by which old investors are paid out from new investors. Any money one investor makes off this scheme is ultimately money that another has lost, all while the underlying scheme does not contribute to any form of productive enterprise, capital formation, or wealth creation. This type of scheme is thus completely based on naked speculation untethered to any real economic activity and exhibits properties more akin to gambling than investing.

For the third category, *stablecoin* crypto assets are a class of financial instruments in which an issuer maintains a pool of non-crypto collateral (dollars, treasuries, commercial paper, etc.) and is represented as a crypto asset whose value is, by various financial engineering techniques, pegged to an exogenous stable value—such as one dollar—such that one dollar-pegged token theoretically represents a claim to redeem one dollar from the underlying pool of assets by the issuer. Stablecoins have arisen out of the needs of the crypto industry to maintain dollar-denominated pseudo-accounts and have typically had difficulty getting access to actual dollars because the international and non-compliant nature of the crypto exchanges has led existing banking institutions to refuse to do business with high-risk crypto clients. Stablecoins have allowed crypto exchanges to avoid traditional financial controls and act as a form of metaphorical "casino token" for speculators who wish to move dollar-denominated accounts to speculate on offshore exchanges like FTX outside the remit of United States regulations.

Stablecoins present a challenge to regulators because, at face value, they present a similar customer experience to that of commercial bank money or traditional payment rails. However, this similarity is deceptive since stablecoins, unlike bank deposits or money market funds, are largely unregulated. While stablecoins may present as a safe alternative payment system, they mask several operation and counterparty risks that present grave concerns for consumers. Since the collateral underlying the stablecoin instrument is controlled by a single party, there are financial incentives for this party to misrepresent the underlying assets relative to the crypto asset issued, thus allowing the operator to abscond with customer money. The absence of mandated audits or transparency reports on these offerings has led to the present reality where many stablecoins are completely dark pools of offshore assets that United States investors are buying with no disclosures or insight into what constitutes the stablecoin they are buying, amounting to an exasperated and riskier form of offshore shadow banking[3]. This leads to both consumer protection risks and systemic risk problems if such assets are allowed to grow or become entangled with the wider financial system.

The second risk of stablecoin offerings is from the networks these stablecoins are offered on top of. Most stablecoins are so-called multi-chain tokens in which the stablecoin is issued on top of other crypto asset networks (often Ethereum, Algorand, Tezos, etc.) which operate as the "payment rail" on which tokens interact with other applications running on those networks. However, these underlying networks are typically of the second category of crypto investment assets which have both operational, market, and legal risks baked into their construction that they impart to any financial instruments built on top of them. Since many of these crypto networks constitute unlicensed investment contract offerings under United States securities law, using a non-compliant crypto platform as a mechanism for a widely used dollar-denominated stablecoin presents a challenge to regulators since they must deal with the legal issues surrounding both layers of networks simultaneously.

Any benefits stablecoins appear to offer over traditional commercial bank money are illusory and only a temporary mirage that arises out of their non-compliance with our existing CTF/KYC/AML frameworks, which may introduce friction in transactions but which are ultimately an essential tool of both national security and monetary sovereignty. The supposed advantages of stablecoins will ultimately become inconsequential once real-time payment systems like FedNow allow the United States to reach technical parity with other economies like India, the United Kingdom, the European Union, Australia, and Canada, which have successfully implemented non-blockchain real-time payment systems to widespread public use.

Apart from public blockchain technologies, there has been a continued interest in so-called *distributed ledger technologies* (DLT) applied in non-public settings to give rise to so-called *private blockchains*. There is no consistent definition of what this technology entails, but it most often amorphously refers to a family of append-only databases in which transactions are cryptographically verified and linked together via a consensus mechanism. At face value, private blockchains allege to solve the problem of allowing companies or consortiums to maintain data with trusted counterparties and to automatically reconcile data within a private network. These networks most often remove the offering of investment tokens as financial incentives to maintain the network and do not rely on censorship resistance for their operation since the network is maintained by either a single operator or a pool of trusted operators. The design of such systems most often aim to replace existing back office system such as existing enterprise resource planning, clearing, and accounting systems. However, these projects have seen few actual successes in practice, as best evidenced by the recent Australian Stock Exchange[15] blockchain transformation project, which resulted in a $150m project failure arising out of the unsuitability of private blockchain technology.

Private distributed ledgers or private blockchains are problematic from both a classification problem and viability perspective since there is no clear definition of what constitutes this technology and what differentiates it from existing databases. Traditional databases have been able to maintain audit logs and operate in an append-only manner for some forty years. Every feature of private blockchain functionality could easily be replicated by an off-the-shelf commercial database offered by major software vendors like Microsoft, Oracle, or IBM. As such, it remains entirely unclear whether this is a legitimate innovation or simply an obscurantist redefinition of software that already exists. When corporations discuss the so-called "underlying technology" of blockchain, or the use of "tokenization" on top of private blockchains, these efforts may simply be marketing or simply refer to routine digital transformation programs that have been in progress for decades inside most corporate IT departments and long predate crypto assets. The use of private blockchain technology remains controversial inside the software industry because of this obscurantist marketing; however unlike crypto offerings, as it does not fall under the remit of financial regulation. Policymakers should thus be wary of industry claims that appeal to the use cases of private blockchains in healthcare, supply chain management, manufacturing, and internet architecture, as the technology described for these applications is neither new, innovative, or in most cases, even suitable. Private blockchains have been most accurately described by many IT practitioners as a "solution in search of a problem,"[13] and lawmakers should avoid basing public policy on such speculative and tenuous claims about unproven technology. Private blockchains offer no unique value for advancing any technical goals or sector-specific application compared to the use of traditional databases.

Central bank digital currencies (CBDCs) are a largely theoretical class of digital forms of public money that are a direct liability of a central bank. By virtue of being centrally issued, most proposed models of CBDCs do not rely on distributed ledger solutions or blockchains and instead are managed by traditional database architecture, which can achieve a higher volume of transaction throughput and reliability. Nevertheless, the technical problems of creating a functional CBDC which is scalable to a nation-state level, incorporated offline capability, emulates the role of a bearer instrument, expands equitable access, promotes compliance with our AML/CFT requirements, and preserves a reasonable level of financial privacy present an extremely difficult technical problem. It may be the case that several of these criteria are mutually incompatible (i.e., simultaneous AML controls and a digital bearer instrument), and as such, it remains an open question whether such a system can be built. We should consider that an implementation that achieves all goals may not be technically realizable or practically desirable, lest the project become an unsustainable expenditure for a vast financial reconfiguration with no clear goals.

However, if such a system were to be developed, it would almost certainly depend on advances in several areas of computer science, including *privacy-enhancing technology* (PEC), *secure multi-party computation* (SMPC), *zero-knowledge proofs* (ZKPs), and *differential privacy* (DP) as outlined by the National Institute of Standards and Technology research summary *Toward a PEC Use-Case Suite* (https://csrc.nist.gov/CSRC/media/Projects/pec/documents/suite-draft1.pdf). The United States is already well-positioned as a leader in these fields of research and could allocate additional funding through DARPA and NSF to these areas to accelerate advancement.

The question that should drive funding for research and development on CBDCs should fundamentally be driven by demonstrable improvements over our current system combined with reasonable deadlines and expenditures. Our current hub and spoke model of central banks and commercial banks is remarkably robust and successfully operates as the transnational backbone of global macrofinance. Most importantly, commercial bank deposits are already digitized, and our existing banking and payments systems already satisfy most of the policy objectives proposed by the Biden-Harris CBDC policy proposal. It remains uncertain why a ground-up rethinking of the most successful financial system in human history is strictly necessary when a more holistic technical and structural incrementalism approach might have a better return on investment than a purely technical moon-shot CBDC solution. For instance, the goals of increasing financial inclusion[19] could alternatively be achieved by expanding or subsidizing our existing banking system to offer basic accounts services—as many European countries do—with lower KYC requirements, thus allowing traditionally marginalized groups easier access to accounts and digital payments.

In summary, blockchain is an unproven technology that is neither new nor particularly useful in practice. Stablecoins have little justification for their existence compared to traditional real-time payment systems derived from central bank-issued money. Crypto assets are a suboptimal form of private money or a highly risky gambling product disguised as investments, both of which are net-negative technology that introduce more harm the benefits to the American public and which are not aligned with either the financial or foreign policy interests of the United States. A comprehensive R&D program on digital assets should emphasize research directed towards digitization and efficiency improvements of existing regulated markets that advance the prosperity of American citizens and productive enterprises rather than directing resources toward crypto markets with unproven value propositions.

References

1. Weaver, Nicholas. 2018. 'Risks of Cryptocurrencies'. Communications of the ACM 61 (6): 20-24.
2. Hanley, Brian P. 2018. 'The False Premises and Promises of Bitcoin'. ArXiv:1312.2048 [Cs, q-Fin], July. http://arxiv.org/abs/1312.2048.
3. Allen, Hilary J. 2022. 'DeFi: Shadow Banking 2.0?' SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4038788.
4. Bernanke, Ben S. Non-monetary effects of the financial crisis in the propagation of the Great Depression. No. w1054. National Bureau of Economic Research, 1983.
5. Walch, Angela. 2019. 'Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems'. C. Brummer (Ed.), Crypto Assets: Legal and Monetary Perspectives, 1-36. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244
6. Orcutt, Mike. 2020. 'This Is How North Korea Uses Cutting-Edge Crypto Money Laundering to Steal Millions'. MIT Technology Review. MIT Technology Review. http://www.technologyreview.com/2020/03/05/916688/north-korean-hackers-cryptocurrency-money-laundering/
7. Rosenthal, David. 'Stanford Lecture on Cryptocurrency'. https://blog.dshr.org/2022/02/ee380-talk.html .
8. Taleb, Nassim Nicholas. 2021. 'Bitcoin, Currencies, and Fragility'. ArXiv:2106.14204 [Physics, q-Fin], July. http://arxiv.org/abs/2106.14204
9. Hockett, Robert C. 2019. 'Money's Past Is Fintech's Future: Wildcat Crypto, the Digital Dollar, and Citizen Central Banking'.
10. Mims, Christopher. 2022. 'NFTs, Cryptocurrencies and Web3 Are Multilevel Marketing Schemes for a New Generation - WSJ'. Wall Street Journal. 19 February 2022. https://www.wsj.com/articles/nfts-cryptocurrencies-and-web3-are-multilevel-marketing-schemes-for-a-new-generation-11645246824".
11. Steele, Graham. 2021. 'The Miner of Last Resort: Digital Currency, Shadow Money and the Role of the Central Bank'. Technology and Government, Emerald Studies in Media and Communications, Forthcoming.

12. Shiller, Robert J. 2017. 'What Is Bitcoin Really Worth? Don't Even Ask.' The New York Times, 15 December 2017, sec. Business. https://www.nytimes.com/2017/12/15/business/bitcoin-investing.html
13. Schneier, Bruce. 2019. 'There's No Good Reason to Trust Blockchain Technology'. Wired Magazine. https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/
14. Cecchetti, Stephen, and Kim Schoenholtz. "Let Crypto Burn." Financial Times, Financial Times, 17 Nov. 2022, https://www.ft.com/content/ac058ede-80cb-4aa6-8394-941443eec7e3.
15. Fildes, Nic. "Australian Stock Exchange Apologises for Dropping Botched Blockchain Upgrade." Subscribe to Read | Financial Times, Financial Times, 17 Nov. 2022, https://www.ft.com/content/029dd01f-eaf5-493c-b195-299408b62469.
16. Carmona, Tonantzin. "Debunking the Narratives about Cryptocurrency and Financial Inclusion." Brookings, Brookings, 26 Oct. 2022, https://www.brookings.edu/research/debunking-the-narratives-about-cryptocurrency-and-financial-inclusion/.
17. Todd H. Baker, Let's Stop Treating Crypto Trading as If It Were Finance, THE CLS BLUE SKY BLOG (Nov. 29, 2022), available at https://clsbluesky.law.columbia.edu/2022/11/29/lets-stop-treating-crypto-as-if-it-werefinance/
18. H., Todd. "Opinion | Crypto Is Money Without a Purpose." The Wall Street Journal, The Wall Street Journal, 19 Dec. 2022, https://www.wsj.com/articles/crypto-is-money-without-a-purpose-ftx-crash-trading-banking-finance-exchanges-brokers-lenders-money-profit-11671479669.
19. Howson, Peter, and Alex de Vries. "Preying on the poor? Opportunities and challenges for tackling the social and environmental threats of cryptocurrencies for vulnerable and low-income communities." Energy research & social science 84 (2022): 102394.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Tassat Group Inc. ("Tassat®")

Tassat

Rachel Wallace
Deputy General Counsel
Office of Science and Technology Policy
[redacted]

March 3, 2023

Re: Request for Information; Digital Assets Research and Development (88 FR 5043)

Dear Deputy General Counsel Wallace:

Tassat Group Inc. ("Tassat®") appreciates the opportunity to submit these comments in response to the Office of Science and Technology Policy's ("OSTP" or the "Office") notice and request for information with respect to a National Digital Assets Research and Development Agenda. Tassat's comments primarily focus on the existing and potential additional benefits offered by private permissioned blockchain-based payment platforms that operate within existing banking regulations. These comments also focus on how private permissioned blockchain-based payment platforms advance responsible innovation in banking, and how support and additional research related to private permissioned blockchains can help mid-size and community banks modernize, while keeping these institutions competitive in an increasingly digital economy.

Executive Summary

Not all uses of blockchain or distributed ledger technology are created equal. Some are revolutionizing the regulated financial services industry for the benefit of consumers and businesses, while others generate increased risk and expose consumers to fraud and financial harm. As OSTP engages in blockchain and digital asset-related research, it is critical that the Office acknowledge the difference between use cases that are transacted on private permissioned blockchains and are currently used by regulated financial institutions like banks and use cases that utilize public permissionless blockchains, such as cryptocurrencies and stablecoins.

Private permissioned blockchain-based solutions have the potential to help banks compete against un- and underregulated fintechs without the widely recognized risks posed by cryptocurrencies and stablecoins and are also better able to support risk management and compliance objectives compared to public permissionless blockchains. Private permissioned blockchains can enable even small and mid-size banks, which form the backbone of our financial system, to offer innovative and technologically advanced payment solutions in a safe and sound manner. This is in stark contrast to public blockchain-based solutions including risky cryptocurrencies and stablecoins, many of which exist outside of the U.S. regulatory perimeter. OSTP should focus its research on how private permissioned blockchains can be leveraged to support the financial services industry through increased security, advanced anti-money laundering capabilities, promoting interoperability and standard setting, financial inclusion, mitigating adverse impacts to climate change, and enabling stronger consumer protection.

We would also note that where private permissioned blockchains have been utilized by regulated financial institutions, these technological solutions have been more efficient and safer than both public blockchains and legacy technology. Private permissioned blockchain solutions also create the potential for customized financial service offerings that legacy technology struggles to provide and that can address the needs of community banks along with unbanked and underbanked communities. Last but not least, because blockchain technology creates a permanent, immutable, and digital record of all transactions, we believe private permissioned blockchain-based solutions create the potential for easier and more efficient regulatory compliance for banks and regulatory oversight for regulators.

Given the benefits of private permissioned blockchain technology, OSTP should consider incorporating the following four proposed guiding principles to frame its approach to building the Research and Development Agenda for blockchain technology and digital assets:

1. Research initiatives should distinguish between use cases and the underlying technology when contemplating how to advance a regulatory framework that is clear and fair. The benefits of the underlying technology, in this case, blockchain, should not be sacrificed or unnecessarily limited in the effort to address concerns specific to cryptocurrencies and stablecoins.
2. OSTP should promote and prioritize blockchain-based solutions that fit within existing regulatory frameworks, including private permissioned blockchain-based use cases that will benefit the financial system and that do not pose the heightened risks of public permissionless blockchain-based projects.
3. OSTP should be concerned that overregulation of blockchain-based solutions may prevent its adoption broadly and/or limit its adoption to only the largest U.S. banks and unregulated or lightly regulated shadow banks. The impact of overregulation would be three-fold: a) only the largest banks and shadow banks, and the customers they serve, benefit from blockchain technology; b) the United States falls further behind other developed nations, including most European and Asian countries, which are rapidly adopting regulatory compliant blockchain-based financial solutions; and c) individuals, corporations and industries of all sizes that are rapidly adopting blockchain-based technology solutions will look outside the U.S. banking industry and to shadow banks to meet their banking needs.
4. The federal government must consider how to facilitate research in this area and partner with private sector actors in a manner that does not pick winners and losers.

Private permissioned blockchain solutions operating entirely within existing U.S. banking regulations should be encouraged to modernize the U.S. banking industry in a manner which allows all banks, not just the largest U.S. banks and shadow banks, to compete to provide innovative financial services, including to communities that have little or no access to such services.

Introduction to Tassat Group

In order to ensure that our nation's banking industry continues to remain competitive - and that traditional financial services can compete on a level playing field with the fintech industry - Tassat was founded to provide American banks with the tools to compete in a modern global economy. Tassat develops private permissioned blockchain technology to facilitate secure instantaneous Business-to-Business ("B2B") fiat payments for banks, and Tassat's solutions operate entirely within the existing U.S. banking regulatory perimeter and do not involve the creation or transmission of any stablecoin or cryptocurrency. The banks that partner with Tassat are primarily mid-size and community banks that can take advantage of this underlying technology without having to deplete their own internal resources. As a result, these banks are able to compete with larger, better capitalized financial institutions as well as fintech alternatives operating outside of the U.S. banking regulatory perimeter.

In 2019, Tassat launched its first product - TassatPay®. TassatPay is an intrabank private permissioned blockchain solution to provide a participating bank's commercial customers with instantaneous, secure 24/7/365 fiat payments without any limitations on transaction size or volume. To date, Tassat's technology has facilitated over $1 trillion in secure blockchain-powered intrabank fiat payments and transfers.

TassatPay is delivered directly to bank clients via either a user interface or an API, which means the technology is integrated directly into the client's treasury management system, allowing banks to serve their clients better by delivering both secure, real-time payments 24/7/365 as well as Fedwire capability in one place. Tassat's technology is compatible with legacy banking systems, allowing client banks to give their customers access to the latest innovations without having to redesign or overhaul their existing systems, including serving as an onramp and "last mile" solution for the upcoming FedNow system. TassatPay is also very affordable for banks of all sizes and enables banks using TassatPay to capture an increasing share of a customer's banking activity.

Through its use of private permissioned blockchain technology, Tassat's solution also enables other value-added innovations in financial services such as the use of smart contracts to facilitate industry-specific use cases. Smart contracts enable Tassat's bank clients to compete with the most advanced fintechs and allow banks and their commercial customers to streamline, simplify, and automate their business processes, making the manual processing and tracking of purchase orders, invoices, discounting, and other payment policies more efficient while also reducing the potential for errors. Banks using this technology can empower their business customers to automate repetitive financial tasks and processes securely and without the need for costly third parties. In concert with its banking partners, Tassat has developed more than 20 different smart-contract use cases, for a variety of different verticals, including logistics, mortgage warehousing, commercial construction, private equity capital calls, as well as broader working capital applications for banks' corporate clients.

Tassat's team includes dedicated regulatory, network security, and cybersecurity staff, and it has implemented a comprehensive, audited information security program for TassatPay. Tassat is a Tier I vendor to banks and has received an unqualified audit opinion regarding its data SOC2, Type 2 data security compliance. The banks Tassat serves comply with all applicable regulatory requirements.

Tassat's payments technology will soon be used by the bank-owned Digital Interbank Network ("The Network"), permitting customers of participating banks to instantaneously send and receive payment and settlement instructions, through a secure private permissioned blockchain, resulting in faster fiat payments. The Network is not itself a bank, nor does it create or transmit funds, stablecoins, or cryptocurrencies. In the same way that TassatPay transactions are wholly contained within a participating bank's systems, The Network's payment instructions stay within the walled garden of The Network and require participation from FDIC-insured client banks and their commercial customers to facilitate transfers.

Private Permissioned Blockchains are Integral to the Future of Banking. (Questions 1 and 2)

Tassat is Helping Small and Mid-size Banks Modernize and Compete

There is a clear need to modernize our nation's payments and financial services infrastructure. Today, American businesses have limited options for transmitting funds to one another, even when they have accounts at the same bank, and many of the options currently available are slow, inefficient, operate on restricted schedules, and are very expensive to operate, maintain, and upgrade. As competition for facilitating faster and more technologically advanced payments increases, banks are increasingly at risk of being disrupted or displaced by emerging fintechs and other nonbanks that issue different types of payments, like stablecoins, cryptocurrencies, and other innovative, but un- or underregulated financial products.

This emerging trend is already adversely impacting the economic competitiveness of banks, which play a crucial role in our financial system and the entire U.S. economy, as both un- and underregulated fintechs and non-U.S. solution providers offer better alternatives. At the core of our banking system are small and mid-size banks that often have strong relationships with their customers, serve a diverse array of customers and businesses, and are deeply invested in their communities. These banks are engines for economic growth and job creation in this country. Consumers rely on borrowing to finance homes, cars, and other large purchases, while small business owners rely on borrowing, payments, and other financial services to run their businesses. According to the Independent Community Bankers Association, community banks provide 60% of all small business loans and make more than 80% of agricultural loans.[1]

Since 2000, there has been a 48% decline in the number of community banks[2] and most mid-size and community banks do not have the resources to keep up with the technology advancements of fintech challengers and megabanks. Not only does this make our nation's banking system less competitive, it also negatively impacts the communities that these banks serve, especially the small businesses and consumers that rely on these important institutions. These obstacles are expected to worsen as superior technology solutions continue to proliferate in both the United States and abroad outside of the regulated banking system.

Tassat's blockchain technology helps commercial banks, particularly mid-size and community banks, stay competitive against un- and under-regulated fintech challengers as well as avoid potential displacement by megabanks that have the resources to develop and implement their own private permissioned blockchain technology solutions but historically do not serve small and medium-sized businesses well. Banks using Tassat's technology have created strong corporate banking relationships, increased deposits, and opportunities to provide other profitable financial services.

Private permissioned blockchains that facilitate instantaneous transfers of funds between banks will support future bank competitiveness. Technological upgrades can be frequent and seamless, ensuring little to no disruption with a bank's customer accounts. Unfortunately, the same cannot be said when using outdated infrastructure. Despite its expense, legacy payment rails are also incapable of implementing and supporting new financial innovations such as smart contracts and sophisticated data analytics which represent the future of financial services in both the United States and abroad.

[1] ICBA, *About Community Banking*, https://www.icba.org/about/community-banking (last visited Feb. 21, 2023).
[2] The number of community banks decreased from 8,315 in 2020 to 4,277 in 2020. Matt Hanauer et al., Community Banks' Ongoing Role in the U.S. Economy, Table 1 (June 2021), https://www kansascityfed.org/Economic%20Review/documents/8159/EconomicReviewV106N2HanauerLytleSummersZiadeh.pdf.

How Tassat's Technology Compares to Risky Crypto-assets

Importantly, private permissioned blockchains provide the benefits of blockchain technology without many of the risks associated with stablecoins and cryptocurrencies. As the President's Working Group on Financial Markets identified in its Report on Stablecoins,[3] cryptocurrencies and stablecoins pose myriad risks to our financial system and to consumers. Unfortunately, as demonstrated by recent events, many of these risks are not hypothetical. As evidenced by the failures of FTX, Celsius, Voyager, Terra/Luna, and BlockFi, it is clear that cryptocurrencies, stablecoins, and companies engaged in crypto-related activity are sensitive to market events and their interconnectedness has the potential to accelerate the speed at which market losses occur. In addition to the collapse of these prominent assets and trading platforms, last year's collapse of the UST stablecoin resulted in a loss of $60 billion of investors' funds, many of whom were retail investors.[4]

Fortunately, the federal prudential banking regulators have issued statements and guidance regarding the risks of stablecoins and cryptocurrencies and have moved to insulate the financial system from shocks caused by adverse market events and contagion spreading through digital asset markets. Most recently, in January and February, the federal prudential banking regulators published joint statements on the risks of crypto-related activities, listing the various risks and vulnerabilities associated with these types of assets.[5] The regulators highlight in the first joint statement that "[b]ased on the agencies' current understanding and experience to date, the agencies believe that issuing or holding as principal crypto-assets that are issued, stored, or transferred on ***an open, public, and/or decentralized network, or similar system*** is highly likely to be inconsistent with safe and sound banking practices."[6] Notably, the regulators discuss how public permissionless blockchains, as opposed to private permissioned, involve heightened risks such as "lack of governance mechanisms establishing oversight of the systems" and "vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance."[7]

Likely due to the inherent and stark differences in the types and degrees of risk presented by public versus private blockchains, the January joint statement focused solely on the heightened risks of **public permissionless blockchains**. Tassat's technology not only mitigates the risks associated with public blockchains by enabling regulated banks to exert control over transactions, but it also promotes compliance by ensuring that bank customers are protected from losing access to their funds and positions banks to be innovators in serving their customers. Unlike stablecoins or even a CBDC, which both have the potential to displace commercial bank money and could drain bank deposits (including introducing potential run risk) by offering a competing product that will be transmissible on a peer-to-peer basis, technology like Tassat's also allows banks to continue to use commercial bank money. Continuing to use commercial bank money would keep deposits within the banking system, which helps bolster financial stability and helps banks stay competitive through lending, one of their core

---

[3] President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, Report on Stablecoins (Oct. 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

[4] MacKenzie Sigalos, *Some Investors Got Rich before a Popular Stablecoin Imploded, Erasing $60 Billion in Value*, CNBC, https://www.cnbc.com/2022/05/29/who-got-rich-before-terra-stablecoin-collapsed.html.

[5] FRB, FDIC, OCC, Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf; FRB, FDIC, OCC, Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities (Feb. 23, 2023), https://occ.gov/news-issuances/news-releases/2023/nr-ia-2023-18a.pdf.

[6] *Id.* (emphasis added.)

[7] *Id.*

functions. As discussed above, both consumers and small business owners rely on banks for borrowing to finance large purchases and run their businesses.

To alleviate some of the obstacles that banks face in today's tech-focused competitive landscape and level the playing field, OSTP should include as part of its research and development agenda focus on technology that enables private permissioned blockchain-based payments innovations occurring within the ambit of federal bank regulation. It is encouraging that policymakers and regulators are increasingly recognizing the benefits of permissioned blockchain technology and its potential applications, but more attention must be paid to using distributed ledger technology to support the role of the U.S. dollar and use of commercial bank money. The competitiveness of the U.S. economy hinges on a dynamic and innovative private sector, made possible by a diverse and strong banking system.

The Potential Adverse Impact of CBDCs

While we appreciate that the Federal Reserve has committed to 24x7x365 real time payments and is exploring a central bank digital currency ("CBDC"), the development of a CBDC is likely to exacerbate the risks currently facing small and mid-size banks discussed above. Even if a CBDC is intermediated by financial institutions, it will still necessarily displace commercial bank money and could drain deposits (including introducing potential run risk) by offering a competing product that will be transmissible on a peer-to-peer basis.

Implementing a CBDC may be unnecessary given the ability of private sector innovation to provide the same benefits. Private sector innovators are already providing banks and their customers the ability to facilitate secure, instantaneous, and programmable blockchain-based payments around the clock, which make American banks more effective in serving their customers and bring tremendous benefits and efficiencies to U.S. companies of all sizes.

In addition to being mindful of the potential adverse impacts that a CBDC may have on banks, the Federal Reserve should also consider how its, and its Reserve Banks,' approach to researching CBDC and its collaboration with megabanks and other private organizations that facilitate transfers of tokenized fiat currency may be inadvertently giving the impression that the Fed is picking winners and losers in this emerging area. The New York Federal Reserve Bank's participation in a pilot with megabanks and a private blockchain network appears to be testing the feasibility of a CBDC liability while also strengthening megabanks and their technology partners' hold on the banking system. This project has the potential to severely diminish the critically important role that U.S. commercial banks, especially mid-size and community banks, play in allocating capital to small and medium sized businesses.

Federal Research into Blockchain and Digital Assets Can Help Advance Responsible Innovation in Banking. (Questions 3 & 4)

Given the potential for blockchain technology to transform our financial system, more research should be conducted on the benefits of blockchain and especially private permissioned blockchains to improve financial services and increase small and mid-size bank competitiveness in the United States. The following areas are critical to protecting banking and financial services and should be prioritized for research: stronger information security, supporting law enforcement and national security objectives through advanced AML, scaling use cases through interoperability, banking the unbanked, and supporting climate objectives.

Information Security

Over the past few years, the pace of global digitalization has accelerated, particularly in financial services. This trend presents many benefits for users but also poses cybersecurity concerns as more information, including consumer financial information, is at risk of being exploited through hacks and other breaches, which are becoming more prevalent. While blockchains are typically more secure than legacy financial infrastructure, OSTP should examine how private permissioned blockchains can be used or improved to protect sensitive financial data. For example, private permissioned blockchain solutions where only a few entities have access to the platform are more secure compared to legacy technologies and public permissionless blockchains, where transaction data is publicly available and the underlying technology is accessible to any party, anywhere. These vulnerabilities with public blockchains and legacy technology expose users and the financial system to increased risks.

Advanced AML

The Office should consider how private permissioned blockchain-based payment platforms can be used and improved to support anti-money laundering/Bank Secrecy Act ("AML/BSA") obligations. As widely recognized, due to their lack of an intermediary, public permissionless blockchains have the potential to be used for illicit finance. Private permissioned blockchains, on the other hand, allow banks to enforce known identities for all participants and support Know-Your-Customer (KYC) and AML requirements. These features can help reduce money laundering and the potential for illicit finance to be facilitated through private blockchains, particularly when paired with instantaneous controls, use of artificial intelligence and pattern recognition administered by a regulated centralized entity such as a bank. Private permissioned blockchains also remove the need for pseudonymous transactions occurring over the blockchain since they cannot be viewed by the public and are protected by banks' cybersecurity. Research could help advance the inherent advantages of blockchain-based payment platforms to identify and prevent illicit financing and money laundering.

Interoperability

It is important that any product or service that uses emerging technology follows an industry-approved standard and/or regulations to protect consumers, businesses, and the financial system. Fortunately, banks already have a robust framework in place to ensure safety, security, and interoperability within payments. It is critical that as various payment platforms emerge, interoperability between systems remains. OSTP should consider how interoperability can be achieved as the payments landscape continues to evolve and what types of standards may need to be developed to enable seamless transactions.

Financial Inclusion

OSTP should examine how private permissioned blockchains and solutions such as Tassat's can support financial inclusion goals. For example, Tassat's technology is intended for banks of all sizes, and could have a particularly positive impact on community development financial institutions ("CDFIs") and minority depository institutions

("MDIs").[8] These banks focus on serving low-and-middle-income ("LMI") communities, which has the potential to increase financial inclusion. CDFIs and MDIs that use Tassat's technology, either through TassatPay or as a member of The Network, will be able to extend the benefits of more convenient, affordable, and instantaneous transfers to their customers, which means small businesses and consumers in the communities these banks serve will be impacted positively.

Whether some digital assets, such as cryptocurrencies and stablecoins, are able to increase financial inclusion continues to be questioned. Due to the inherent nature of cryptocurrencies and stablecoins, these continue to show significant risk and much volatility. As a result, what some tout as advancing financial inclusion may actually disadvantage the under- and unbanked because of the extraordinary volatility and potential for loss of stablecoins and cryptocurrencies. By making financial services more efficient and encouraging safe, secure innovation, private permissioned blockchain solutions like those offered by Tassat can be utilized by banks and their regulators to better serve un- and underbanked communities. Safe, well-regulated technological innovation has the potential to greatly benefit underserved communities.

Environment

OSTP should also consider the environmental benefits private permissioned blockchains are able to provide in comparison to some public permissionless blockchains. Specifically, OSTP should examine the amount of energy use and carbon emissions that result from transactions facilitated by proof-of-work consensus mechanisms, which is used by a number of high profile public permissionless blockchains, compared to proof-of-authority, which is more likely to be used on a private permissioned blockchain and which can be carbon neutral. Tassat estimates that its proof-of-authority consensus mechanism consumes less than 1% of the energy consumed by proof-of-work mechanisms. The greater efficiency and security of Tassat's payments platform would indicate that it is less energy intensive than legacy solutions as well.

Supporting Digital Asset-related Digitalization through Workforce Development (Question 5)

As OSTP examines the above topics with respect to its research and development agenda, it should also consider related factors such as workforce training and what skills will be needed to support growing digitization efforts in the financial services sector. In its report, Responsible Advancement of U.S. Competitiveness in Digital Assets, the U.S. Department of Commerce states that "[f]ostering a skilled workforce would contribute to the development of technologies and platforms that improve efficiencies for businesses and enhance competitiveness. Signature programs such as NSF's CyberCorps®: Scholarships for Service (SFS) and the Education designation within Secure and Trustworthy Cyberspace (SaTC), and the Small Business and Innovative Research (SBIR/STTR) Educational Technologies and Distributed Ledger Technology specific portfolios have long supported education and workforce development projects and naturally align with the goals"[9] of the report. O*NET OnLine, sponsored by the U.S. Department of Labor, assesses career outlooks on various occupations and

---

[8] Bank Policy Institute, *Statement for the Record Regarding MDIs and CDFIs Before the U.S. House Committee on Financial Services* (Feb. 16, 2022), https://bpi.com/statement-for-the-record-regarding-mdis-and-cdfis-before-the-u-s-house-committee-on-financial-services/#:~:text=The%20CDFI%20Fund%20has%20been,with%20the%20broader%20financial%20system.

[9] U.S. Department of Commerce, Responsible Advancement of U.S. Competitiveness in Digital Assets (Sept. 2022), https://www.commerce.gov/sites/default/files/2022-09/Digital-Asset-Competitiveness-Report.pdf.

identifies a "Bright Outlook" for blockchain engineers. It states that this occupation "is expected to grow rapidly and is a new and emerging occupation."[10] To meet increased needs for blockchain engineers, OSTP should examine whether current workforce development efforts are keeping pace with projected demand.

Conclusion

The strength of the U.S. economy is based on a dynamic and innovative private sector, made possible by a diverse, strong, and innovative banking system. At the core of our banking system and our economy are small and mid-size banks that often have strong relationships with their customers, serve a diverse array of customers and businesses, and are deeply invested in their communities. The communities and businesses these banks serve also drive innovation and employment growth in the U.S. economy. Of significant importance to this sector of the financial services industry is the ability to ensure technological innovations that allow these small and mid-size banks to compete with both the larger institutions and with the un- and underregulated nonbank financial companies that have more resources at their fingertips. The federal government should adopt policies and allocate resources to promote innovative and regulatorily compliant payment platforms and financial services continue to thrive.

Regulation of applications employing the underlying financial services infrastructure, in this case blockchain technology, should be designed and implemented in a manner which fosters and promotes innovation in financial services by all banks, not just megabanks, and enables regulated entities to compete with, and even displace, unregulated entities and unregulated alternatives. Further, the federal government should avoid picking winners and losers in this emerging area of financial services by partnering with only a few banks and technology providers. Increased research in this field through the OSTP may be able to support development and growth of the technology for improving financial services in a neutral manner. Combining private permissioned blockchain-based solutions with existing regulations makes this an achievable goal, resulting in a stronger, more dynamic, and fully modernized U.S. banking system better able to serve both companies and consumers while also making the American banking system and the U.S. economy more competitive internationally.

We look forward to serving as an ongoing resource on this important and complex topic.

Thank you for your time and consideration of this matter.

Very truly yours,

[redacted]

Kevin R. Greene
Chairman & CEO
Tassat Group

[10] O*Net OnLine, Blockchain Engineers (last visited Feb. 22, 2023), https://www.onetonline.org/link/summary/15-1299.07.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

TaxBit

Digital Assets.
Expert Compliance.
Endless Opportunity.

Request for Information
Digital Assets Research and Development

Office of Science and Technology Policy (OSTP)

TaxBit response to a request for information published 01/26/2023

Derek Smith, Solutions Architect
[redacted]

TaxBit is an Industry respondent.

February 28, 2023

In accordance with FAR Part 15.201, this submission is provided with the intent to exchange information with the Government the contents of which are consistent with procurement integrity requirements per FAR 3.104. Further, the content is not intended to be incorporated directly into the terms of a future competitive procurement.

About Taxbit

TaxBit is currently the leading issuer of Forms 1099 for digital asset platforms. TaxBit has been filing such forms, including Form 1099-B reporting digital asset dispositions, for digital asset exchanges since 2020 and filed tens of millions of these forms for the 2021 tax year.

As depicted in Figure 1, TaxBit provides industry-leading software platforms for digital asset tax and accounting to commercial businesses, governmental entities, and consumers.

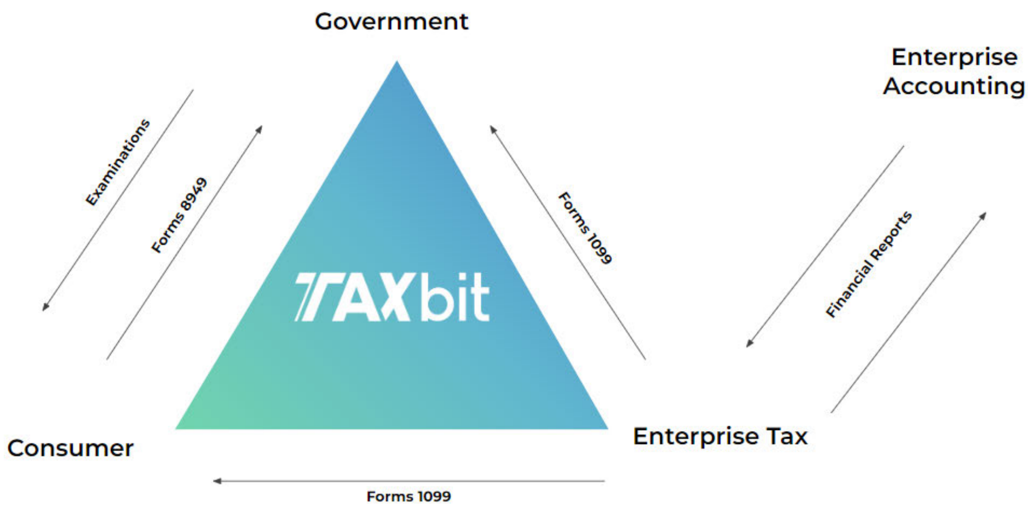


Figure 1: TaxBit Golden Triangle

TaxBit's commercial customers include both leading centralized and decentralized exchanges where it provides portfolio tracking, tax information, and Know Your Customer (KYC) tools for tax information reporting. TaxBit can track transaction data across both centralized and decentralized components of the digital asset ecosystem, including centralized exchanges, decentralized finance (DeFi) protocols, NFT marketplaces, wallet providers, and other digital platforms.

The Internal Revenue Service (IRS) hired TaxBit in 2020 to provide digital asset tax calculation support to the Small Business/Self-Employed (SB/SE) Examination Organization on a specific examination. In January 2021, the IRS awarded TaxBit a contract to provide tax calculation and support services for SB/SE, Large Business & International (LB&I), and the Criminal Investigation Division (CID) (indirectly) through a competitive bidding process. In December 2021, the IRS awarded TaxBit a second (current) contract for tax calculation and support services after another competitive bidding process.

TaxBit employs 600 Application Programming Interfaces (APIs) covering both on-chain and off-chain data, allowing it to perform these tasks in real-time, a system known as the TaxBit Network. In this network, data from the API feeds are validated and normalized by TaxBit's data ingestion/perfection pipeline, which uses state-of-the-art technology to instantly scale to meet workload demand. TaxBit's Subject Matter Expert (SME) team, which consists of tax attorneys, CPAs, and blockchains experts, validates the business rules and logic used in these processes.

The TaxBit Network is an industry-wide partner program for the most reputable digital asset platforms and part of an extensive compliance program allowing members to provide Forms 8949 to their users free of charge. Consumers receive a free tax-form download to facilitate Form 8949 creation for all the exchanges where they trade digital assets, as long as each exchange is part of the TaxBit Network.

Introduction

TaxBit focuses on tax and financial accounting compliance and has limited its responses to areas where its expertise can provide the most value. More specifically, we will discuss the following:

- Simplifying the digital asset tax process
- The challenge of tracking cost bases
- A technological KYC solution for DeFi exchanges
- Exchange health / Proof of reserves
- General commentary on balancing free markets with regulation

For purposes of context, TaxBit believes it is important to note the two distinct aspects of what has become known as the blockchain or cryptocurrency ecosystem—the enabling technology and the supported assets.

The ecosystem is supported by distributed ledger technology (DLT), which is the concept of spreading database-stored information across multiple computers (nodes) in a network. That distributed ledger can be structured in different ways with independent access restrictions on who can update the ledger (write or validate transactions) and who can view the ledger (accessibility). The rise of the cryptocurrency ecosystem has primarily focused on one subset of DLT—blockchain-based ledgers. In a blockchain-based system, information is stored in blocks that are appended to the ledger chronologically. However, it is important to understand that blockchain-based DLT is not the only type in existence and as the technology and its use cases develop, the government should be thinking about other variations such as blockless blockchains or so-called tangle chains.

Separate from the enabling technology are the assets to which the technology can give rise. Since the advent of bitcoin in 2009, the primary use case for DLT has been the creation of novel assets (crypto-assets) that exist to, at times, mimic economic activities that were historically handled by traditional assets. For example, bitcoin was intended to function like electronic cash, permitting peer-to-peer payments without a financial institution as an intermediary. Ether, the native coin of the Ethereum network, was intended to function as compensation (known as gas) to individuals supporting the activities occurring on that network. As such, digital assets created by DLT have been viewed as unique and, as a result, have been difficult to categorize in the context of traditional assets such as securities, commodities, or other instruments representative of legal title or contractual rights.

Evolution in this area will impact both the underlying technology and the assets supported by the technology. From a government standpoint, steps can be taken to promote development on both of these fronts. As the underlying technology evolves, it is likely to become more robust, permitting more flexibility with respect to cryptographic security, transaction validation, and access. Separately, DLT is likely to expand into the digitization or tokenization of traditional assets. For example, this RFI seeks information on the tokenization of fiat currency through a CBDC. The iteration of DLT used to support a CBDC may likely look different than what is employed by the Bitcoin network in terms of transaction validation and accessibility. The same is true for the tokenization of other financial instruments such as securities or commodities.

4. R&D that should be prioritized for digital assets:

Information about Federal research opportunities that could be introduced or modified to (a) advance the development of digital assets and/or (b) protect communities and U.S. national interests from risks or harms that digital assets might present. This includes topics for technical research, topics for research in the social sciences and across disciplinary boundaries, and opportunities for hardware and software development. This also includes information about emerging areas that could enable new opportunities to leverage digital assets, as well as information about technical limitations of digital assets and the associated business models and governance arrangements they often rely upon. Respondents are encouraged to, where relevant, describe how the discussed R&D topic could be useful in helping a potential U.S. CBDC system align with the Policy Objectives for a U.S. CBDC System. Respondents are also encouraged to share how the discussed R&D topic could help advance U.S. competitiveness and leadership in the world.

Response:

Federal research and development opportunities for digital assets are abundant and becoming more urgent as the ecosystem continues to evolve and adoption increases. Our response focuses on the financial, accounting, and tax aspects of the technology.

DLT and the digital assets it enables have already begun to augment traditional financial transactions. Assets, such as bitcoin, exist on networks that enable peer-to-peer payments and cross-border transactions with minimal cost and friction. Individuals that are un- or under-banked are able to gain access to funds or share value with distant family members,

Separately DLT, can (and is) being applied to traditional financial assets, where the digitization or tokenization of those assets on a distributed ledger can help facilitate transparency, increased settlement speed for transfers, and reduced settlement costs.

Use of distributed ledgers in these types of scenarios is consistent with the Department of Homeland Security, Science and Technology Directorate Flowchart included as Figure 6 of *National Institute of Standards and Technology Internal Report 8202*. In these situations stored information needs to be shared and an inherent lack of trust (evidenced by financial fraud) supports a need for a shared ledger that is historically immutable.

As unique and novel uses for financially-focused digital assets continue to increase, and as the transition of traditional financial assets into digitized assets gains momentum, a few risks do arise such as privacy concerns and data interpretation or understanding.

Although distributed ledger technology may be beneficial in financial accounting because it creates an historically accurate, immutable record of a company's financial transactions that can be shared and checked by external auditors or governmental entities, use of DLT creates a privacy risk if that ledger is publicly viewable for anyone to see. Moreover, review and interpretation of the DLT-based data can create friction. However, these issues are already being solved. Software tools have been created (as discussed below) that can read, interpret, and reconcile blockchain-based transactions for financial accounting in real-time. These software tools can solve some of the risks or difficulties associated with DLT. On the privacy front, research is already being undertaken in the area of zero-knowledge proofs and non-fungible tokens whereby an external auditor or governmental agency can validate the ownership or identity of DLT-based information without needing to publicly identify those owners.

Similar solutions exist in the tax reporting space. Digital assets enabled through DLT are an opportunity to open up financial investment opportunities to those who currently lack access due to socio-economic or other demographic factors. However, privacy and data comprehension issues still arise when those individuals need to prepare tax returns or related forms. Again, software (as discussed below) already exists that can review, interpret, organize, and seamlessly calculate tax return information for those individuals (or for the IRS when it needs to check for compliance).

Simplifying the Digital Asset Tax Process

Simplifying the tax process for digital assets can benefit both taxpayers and tax authorities alike by preventing unnecessary audits and reducing friction between taxpayers and tax enforcers. Here are some ways in which the process can be made simpler:

- Mitigate risks associated with the pseudo-anonymous nature of blockchain by simplifying KYC requirements. KYC is the process of verifying the identity of a customer or client in a financial transaction, making sure someone is the person he or she claims to be. In the context of digital asset exchanges, research opportunities exist for figuring out how to simplify this process so that it can seamlessly apply across various platforms for tax information reporting, anti-money laundering (AML) practices, and other applications. Generally speaking, DeFi platforms, along with some international centralized exchanges, do not collect KYC information from their users. While disagreement surely exists within the digital asset ecosystem about the need for gathering such KYC information, the lack of it necessarily leads to weaker AML enforcement and less tax information reporting. Research on how to employ blockchain technology to create less onerous KYC processes across different platforms would promote the adoption of KYC gathering by protocols and enhance government AML and tax-collection efforts.
- Automated Tax Calculation: Implementing automated systems for calculating and reporting taxes on digital assets can significantly reduce the time and effort required for taxpayers. This can include tools for calculating cost basis and generating tax forms such as Forms 1099 and Forms 8300.
- Standardized Reporting: Establishing standardized reporting requirements for digital assets can simplify the process for taxpayers and tax authorities alike. This can include the use of standard tax forms, such as Forms 1099 and Forms 8300, and the implementation of consistent reporting requirements across all digital asset exchanges.
- Integration with Tax Filing Systems: Integrating the reporting of digital assets with existing tax filing systems, such as those used by the IRS, can streamline the process for taxpayers. This can include the ability to report digital asset transactions alongside other forms of income and deductions on a tax return.
- Improved Data Sharing: Improving the sharing of data between digital asset exchanges, tax authorities, and taxpayers can simplify the process of calculating and reporting taxes on digital assets. This can include the sharing of information on transactions, cost basis, and other relevant tax data.

By researching and implementing the above measures, the tax process for digital assets can be made simpler, reducing the burden on taxpayers, and improving the efficiency of tax authorities. This can ultimately contribute to the growth and development of the digital asset industry, by creating a more favorable tax environment for digital assets and encouraging greater participation by individuals and businesses.

How TaxBit Can Help

TaxBit set out to help solve these problems through building tools and educating market participants, regulators, and policymakers. TaxBit began by offering a digital asset tax tool to consumers free of charge. However, it became clear over time that more systemic changes were required to truly reduce the complexity for all parties involved.

Thus, TaxBit now has over 600 API connections to exchanges and conducts Form 1099 reporting for almost all U.S. digital asset exchanges. Pursuant to the Infrastructure Investment and Jobs Act (IIJA), all digital asset exchanges must soon report capital gains on Forms 1099. This will require enhanced cost-basis tracking because of the mobile nature of digital assets, which users can easily move from exchange to exchange. To comply with the IIJA, each digital asset exchange either will have to send personally identifiable information (PII) and cost basis for every outbound transfer going to every other exchange, or they will have to file transfer statements with the IRS (as depicted in Figure 2 below).

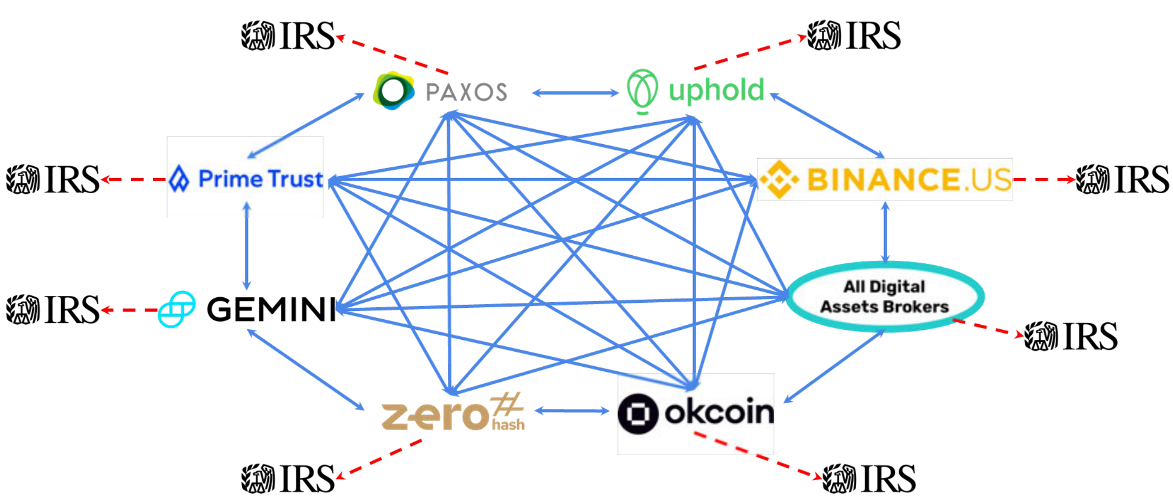


*Figure 2: Cost Basis Transfers **Without a Centralized Solution**.*

**This is a notional rendering of what could evolve with potential industry participants. This does not represent a TaxBit opinion or endorsement of any particular exchange or third-party entity.*

Without an industry solution, communicating across systems becomes messy and complex.

TaxBit Cost Basis Transfer Solution

TaxBit provides a SaaS capability to its commercial customers to address the IIJA requirements for digital asset transfer statements. This centralized, API-based solution greatly reduces touchpoints and solves the challenges associated with each individual broker having to implement their own new system.

TaxBit introduced the Cost Basis Interchange (CBI) to provide a central cost-basis transfer solution to our commercial exchange customers. TaxBit CBI integrates with each participating broker via API, hosts all data in a single location, and automatically transfers cost basis data between all brokers as depicted in Figure 3.

Figure 3: Cost Basis Transfers ***With a Centralized Solution***

**This is a notional rendering of what could evolve with potential industry participants. This does not represent a TaxBit opinion or endorsement of any particular exchange or third-party entity.*

CBI ensures that cost basis information is shared along with its related blockchain data when a digital asset is transferred. TaxBit's commercial CBI system can be configured and adopted to allow the IRS to receive the information required by IIJA without having to write new custom software.

The TaxBit CBI Solution has drastically reduced complexity and number of touchpoints as compared to the non-centralized solution depicted in Figure 2 and enables accurate transfer matching and portability of cost basis information between broker platforms. This permits brokers to meet the requirements of IIJA much more easily than solutions employed in traditional finance. TaxBit's CBI system can allow the IRS to receive the information required under IIJA and effectively validate, organize, and match transaction information to *reduce the digital asset data gap*.

TaxBit's SaaS can bulk load data into existing IRS systems or use API access for more modern systems. For example, the IRS Automated Underreporter system (AUR) could use TaxBit software to match and validate digital asset transactions on a return and aid in taxpayer letter notifications. The Return Review Program (RRP) could use APIs to query information to be used for real time fraud detection.

TaxBit KYC for DeFi

TaxBit is developing a technological solution to facilitate KYC on DeFi exchanges. Under that solution, users who wish to engage in DeFi activities on participating exchanges would be able to provide PII to TaxBit to KYC their wallets.

TaxBit would perform the KYC steps and mint a Soulbound Token (SBT) for each wallet of the user to represent they have been "KYC'd." Counterparties, protocols, projects, and other entities will be able to verify if a wallet address has been "KYC'd" by hashing a user's on-chain address and determining if a TaxBit minted SBT exists or not.

Important Distinctions

- Soulbound Tokens (SBTs) are non-transferable and cannot be bought or sold.
- User KYC data will be stored on-chain, but in an encrypted form.
- Counterparties will not be able to view actual user KYC data, only its encrypted form.
- Only TaxBit will be able to decrypt and view user KYC data.
- Counterparties such as regulators and tax authorities may be able to request documents from TaxBit.

Thus, exchanges that wish to KYC voluntarily or because they are required to do so will soon have access to a helpful tool provided by TaxBit. This tool could someday become the industry standard and enable a much more seamless KYC process for the ecosystem compared to a more disparate approach.

Exchange Health: Proof of Reserves

With the recent digital asset exchange bankruptcies, most notably FTX, proof of reserves has become an increasingly important topic. Proof of reserves is a method used by digital asset exchanges to help demonstrate the solvency of their platform. In other words, proof of reserves provides greater transparency and assurance to customers that an exchange holds sufficient funds to cover all customer deposits. This is important for several reasons:

- Consumer Protection: By demonstrating that they hold sufficient funds to cover customer deposits, digital asset exchanges can provide customers with assurance that their funds are safe and secure. This is particularly important in the digital asset industry, where exchanges have been subject to significant security breaches and loss of customer funds in the past.

- Maintaining Confidence: Proof of reserves helps to maintain confidence in the digital asset industry, by demonstrating to customers and regulators that digital asset exchanges are operating in a transparent and trustworthy manner.

- Increased Liquidity: Digital asset exchanges that demonstrate proof of reserves are likely to attract a larger number of customers, as customers are more likely to deposit funds on an exchange that is transparent and secure. This increased liquidity can in turn contribute to the growth and development of the digital asset industry.

- Improved Regulation: Proof of reserves can play a role in improving the regulation of the digital asset industry, by providing regulators with greater transparency into the operations of digital asset exchanges. This can help to ensure that digital asset exchanges are operating in a responsible and trustworthy manner and can ultimately contribute to the stability of the digital asset industry as a whole.

By implementing proof of reserves, digital asset exchanges can provide customers and regulators with greater transparency into their operations, and help to maintain confidence and stability in the digital asset industry. Additionally, a reserves subledger can roll up into more holistic reports such as full financial statements that can be furnished to regulators, tax authorities, and auditors.

TaxBit has a best-in-class SaaS-based accounting suite that can track digital asset exchange reserves in real-time and provide instantaneous reporting to regulators and even the general public. Should exchanges be hesitant to publish wallet addresses to the public, TaxBit, or regulators in conjunction with TaxBit software, can operate as a trusted intermediary to track and report reserves while keeping wallet addresses confidential. Additionally, should less frequent reserve reporting be desired, that can be accommodated.

Balancing Free Markets and Regulation

The balance between totally free markets and heavy regulation is an important consideration when it comes to digital assets. Digital assets, such as cryptocurrencies and tokens, are a relatively new and rapidly developing area, and there are differing views on the appropriate level of regulation required to protect investors and ensure market stability.

On one hand, a completely free market can provide a platform for innovation and competition and can potentially lead to faster growth and development. In a completely free market, digital assets can be created and traded with minimal restrictions, allowing for a wide range of products and services to be created and offered to consumers. This can be beneficial in fostering entrepreneurship and innovation.

However, a completely free market lacks oversight, leading to fraudulent or illegal activities, market manipulation, and instability. Investors may be subject to significant risks, and a lack of regulation can make it difficult to hold those responsible accountable for wrongdoing.

On the other hand, heavy regulation can provide protection to investors and promote market stability. By establishing clear guidelines and requirements for digital assets, regulations can help to prevent fraudulent and illegal activities, reduce market manipulation, and promote transparency. This can increase investor confidence and attract more capital to the market. However, excessive regulation can stifle innovation, slow development, limit the range of products and services available to consumers, and create barriers to entry for new businesses.

It is therefore important to strike a balance between totally free markets and heavy regulation when it comes to digital assets. A balanced approach should aim to protect investors and promote market stability, while also allowing for innovation and competition. This may involve establishing clear guidelines and requirements for digital assets, such as registration and disclosure requirements for issuers and exchanges, anti-money laundering and anti-fraud measures, and investor protection measures. It may also involve ongoing monitoring and enforcement to ensure that regulations are being followed, and that the market remains fair and transparent.

Should draconian regulations be implemented in the United States, it would cause top talent to leave the country in search of more favorable business environments. This could lead to a brain drain, as highly skilled individuals choose to take their expertise and ideas to other countries that are more welcoming to digital asset innovation. If the United States were to fall behind in digital asset innovation, it could have significant economic and social consequences. The world would continue to innovate, and other countries could quickly take the lead in digital asset development. As a result, the United States could lose its competitive edge, which could have ripple effects throughout the economy. This could lead to reduced economic growth, job losses, and a decline in the country's global standing.

In summary, finding the right balance between totally free markets and heavy regulation is crucial when it comes to digital assets. While a completely free market can provide opportunities for innovation, it can also create instability and increase investor risk. Conversely, heavy regulation can protect investors and promote market stability, but can also stifle innovation and limit competition. Finding a balance that promotes both innovation and protection is essential to realizing the potential of digital assets.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Tata Consultancy Services

Building on belief

TCS Response to the Office of Science and Technology Policy RFI

Digital Assets R&D Agenda

Submitted by: Karen Duvall

Capture Manager

TCS Ltd.

Tata America International Corp.

[redacted]

March 03rd, 2023

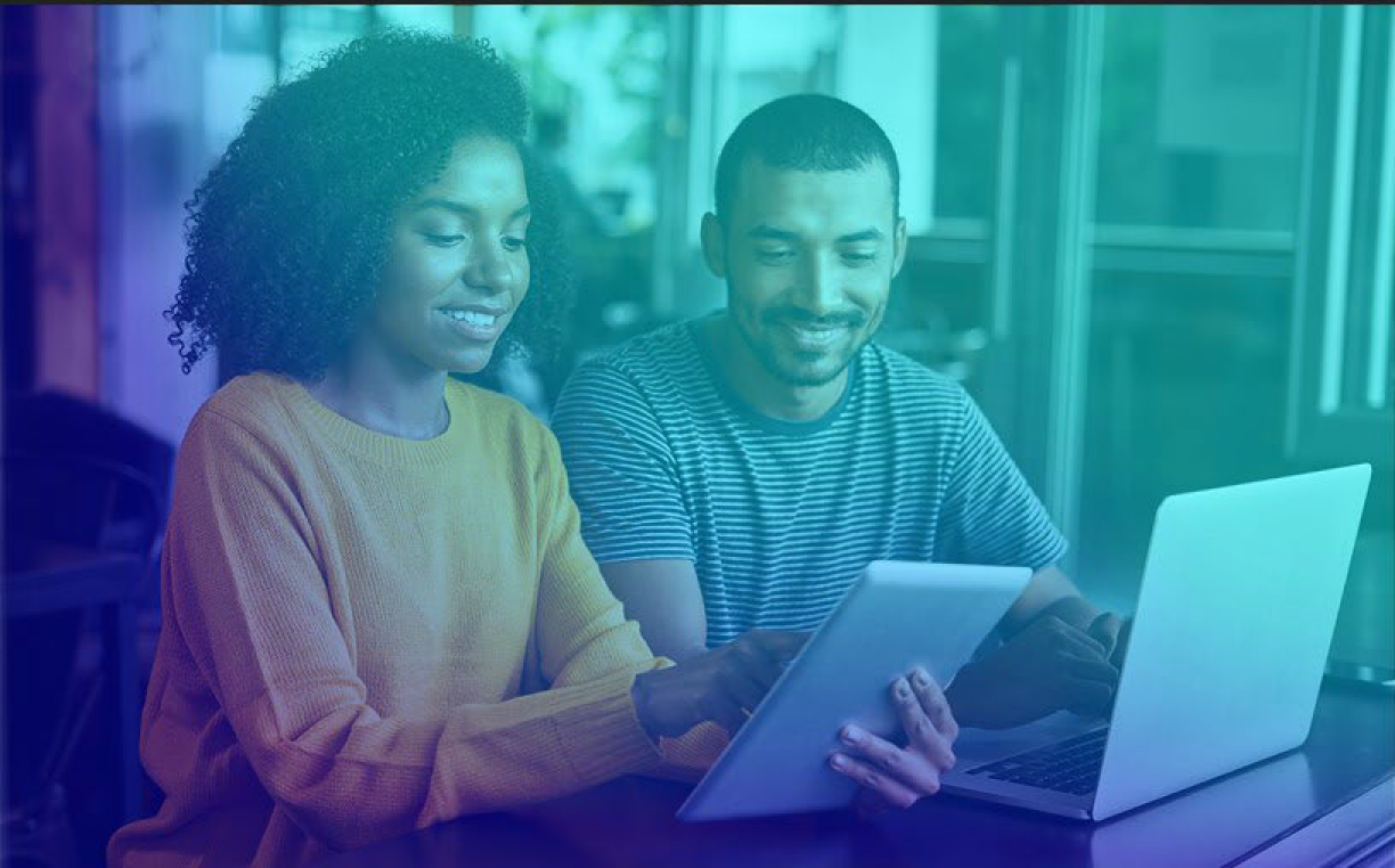


Table of Contents

1. Improvements to Goals, Sectors, or Applications

Goals, sectors, or applications that could be improved with digital assets and related technologies.

By representing real-world assets in the form of digital assets, TCS can enable our clients to discover new business opportunities and reduce the friction in the existing business landscape of financial services, real estate, automobile, payments, and so on.

- The tokenization of assets (such as equities, fixed income, and other financial products) brings atomicity in the settlement of these assets and automates the asset's lifecycle events. Tokenizing a financial asset helps fractionalize it, enabling retail investors to participate and bring more liquidity to the ecosystem.
- Tokenization can help achieve a firms' sustainability goals. Tokenized carbon credits and carbon offsets can help create a new dimension for the carbon marketplace. Institutional and retail investors can participate in this ecosystem in a more seamless way, bringing in more liquidity. Tokenization helps firms track their carbon footprint and attain net zero targets and emissions in an immutable manner.
- Central Bank Digital Currency (CBDC) represented as tokens for a retail scenario can augment the existing digital payment landscape with the reduction in the usage of cash amongst the public. CBDC can help the public to easily transact cash with the usage of wallet, help central banks reduce the operational overhead associated with printing money, monitor illicit transactions that may else occur with the use of fiat currency, and make cross border transactions more seamless.
- Cryptocurrencies has widespread adoption amongst the Gen Z investors, and institutions are willing to allocate cryptocurrencies as part of their portfolio. Cryptocurrencies have turned to be an asset, which can be used as a hedge against inflation.
- Using tokens to establish a digital connection to a physical good can maintain supply chain transparency for a range of use cases. The digital representation can help track the provenance of an asset, able to store the data as the asset moves across states.
- For retail investors, tokenization of real estate makes investing in properties more accessible. Fractionalization of the property brings in more liquidity as it enables investors to own a fraction of a land as an investment and can reap in benefits like rental income and land appreciation.
- Non-fungible tokens (NFTs) have the potential to revolutionize the automobile sector. Ownership of the cars can be recorded in NFTs and transferred across buyers. The data stored can be dynamic and enable secondary buyers to know about the service history and previous warranty claims.
- NTFs have potential across multiple sectors such as fashion, retail, sports, rewards, and so on. Use cases are built by integrating NFTs with Metaverse, thus creating a new customer touchpoint for merchants.

2. Risks to Goals, Sectors, or Applications

Goals, sectors, or applications where digital assets introduce risks or harms.

- **Volatility Risk** – The price of crypto assets is highly volatile. Investments in crypto assets are deemed high-risk speculative investments. The risk of material or total loss of assets do exist.
- **Technology Risk** – Digital asset technologies are likely to undergo significant changes in the future. Technological advances in cryptography, code breaking, or quantum computing may pose a risk to the security of digital assets.
- **Fraud** – Investors of any digital asset are directly exposed to fraud, theft, and cyber-attacks. Market manipulation and insider dealing by market participants, due to a lack of regulation, supervision, market control and liquidity.
- **Supervision Risk** – There is no authority or institution that may intervene in the digital asset market to stabilize the value of digital assets, and/or prevent, mitigate, or counter-attack irrational price developments of digital assets.
- **Credit & Counterparty Risk** – In the case of tokenized securities, the risk of default or bankruptcy of the underlying issuer is high, similar to traditional private equity and/or private debt investments.
- When a central bank introduces CBDC, there are chances where customers may move funds from deposits to CBDC accounts, which may pose liquidity risk for the banks due to lack of sufficient funds to lend.
- Digital assets may also pose risk in the form of illicit financing, money laundering, cybercrime, and terrorist financing.
- **Security Risk** – The digital asset ecosystem faces a significant cybersecurity risk. As seen with the examples of hacks on crypto exchanges, it is important to build a resilient system to overcome such risks.

3. Federal Research Opportunities

Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.

- The introduction of central bank digital currencies can help mitigate the risk of customers migrating to crypto currencies for payments. CBDCs offer a safe mode for digital payments and can be further nudged for utilization by the public.
- Regulation of digital assets (such as tokenized funds and bonds) can help enhance innovation in a regulatory environment and can help achieve synergies and efficiencies in the financial services sector.
- The development of a framework to adopt Institutional Decentralized Finance (DeFi) can flourish innovation, enable opportunities to create newer financial products, and create new ecosystem.
- The standardization of custody guidelines to safely store the digital assets and the creation of a governance mechanism can help mitigate the risks associated with the any unauthorized access to assets.
- The regulation of stablecoin issuance, and its dependence on collateral, must be monitored diligently.

There must be an international cooperation on regulating crypto and digital assets to have standardization across jurisdictions.

4. Prioritized R&D

R&D that should be prioritized for digital assets.

The opportunities that digital assets hold includes:

- Improving accessibility to current markets by new customers.
- Reducing complexity, reducing current (high) cost, improving efficiency of existing processes.
- Creating new business models, improving interoperability, and improving transparency.
- Reduction of intermediaries, saving costs and being able to participate in shaping the future of digital assets.

These are taken as a research area of digital assets which is to be enhanced further.

CBDCs may give central banks the ability to achieve a variety of systemic goals, including assuring financial inclusion, lowering fraud and money laundering, ensuring sovereign options for digital payments, encouraging local payments innovation, and developing a new monetary policy tool.

CBDC can be either wholesale or retail. From a wholesale point of view, the following experiments can be tried:

1. Atomic settlement against securities traded by financial institutions
2. Cross-border settlement with different CBDC's across geographies

From a retail CBDC standpoint:

1. Scalability and resilience of the payment network
2. Offline payment using CBDC
3. Programmability of CBDC

Every central bank should think about the below mentioned issues when they establish their priorities and decide how to best achieve them:

- Realistic adoption targets and market assessments of the existing and future payments landscape should serve as the foundation for business cases and scenarios.
- Regarding its role, the central bank's participation could be deep or light. The adoption goal may be best accomplished by establishing PPPs that leverage long-standing relationships with commercial banks and key corporate entities.
- It is notable that central banks will require new decision-making techniques. Requests for Proposals (RFP) procedures are useful tools for evaluating available technology. Central banks should also improve their change management procedures and hire new personnel with partnership development skills.
- Some of the above-mentioned aims would necessitate regulatory changes. It will be necessary to overcome obstacles in fiscal rights, commerce enablement, and regulation.

In addition to the points mentioned above, the designed CBDC should align to certain goals such as enhancing payment systems and guaranteeing that the global financial system has transparency, connectivity, and platform and architecture interoperability or transferability. Benefit consumers, investors, and businesses promote economic growth and financial stability. Additionally, the CBDC system should promote financial inclusion and equity, as well as safeguard national security.

Significant research and development need to be placed in the cross-border settlement. As the current process involves significant friction in the payments across jurisdictions, it is important to research in the cross-border payments arena. Usage of blockchain technology, CBDC, stablecoins and tokenized assets in the cross-border ecosystem need to be experimented.

As the country is moving towards T+1 settlement, instantaneous and real-time settlement of assets need to be experimented with for better efficiencies. Tokenized assets and tokenized currencies can help achieve atomic settlement. The smart contracts embedded with the business details can help automate the lifecycle and other events associated with the asset.

5. Opportunities to Advance Innovation

Opportunities to advance responsible innovation in the broader digital assets ecosystem.

The digital asset ecosystem is a basket of different classes secured by an underlying technology, known as blockchain. These include cryptocurrencies, stablecoins, CBDCs, asset-backed and security-backed tokens.

Non-Fungible Tokens (NFTs) have found significant relevance in the form of representing a unique real-world asset in the digital medium.

1. **Representation of Physical Goods (such as shoes and clothes) as NFT** – Customers have benefitted from both the physical and the digital asset.
2. **Circular Economy** – Tracking the plastic usage right from the manufacturing of an item until it has been recycled.
3. **Art** – Unique art and music issued as NFTs help creators monetize their work and ensure the distribution of royalties upon secondary sale.
4. **Sports** – Exclusive footage of a sporting event can be minted as a NFT, enabling consumers to own the moment.
5. **Digital Identity** – Each unique person can be given an NFT, which can be used as an identity with data referring to that individual.

Decentralized Finance (DeFi) can usher in innovation in the financial services landscape. DeFi can automate multiple processes that are currently executed by a centralized party in the capital markets sector.

Processes like order matching can be executed using Automated Market Makers (AMM). Customers with digital currencies can stake a liquidity pool to obtain the interest by lending it to potential borrowers.

Institutional DeFi offers a multitude of opportunities in the financial services sector that can be leveraged to achieve significant benefits in processes such as order matching, securities lending, and FX transfer.

However, innovation in this area is required to help regulate the usage of digital assets and to ensure there is minimal disruption to the existing participants of the ecosystem.

6. Other Information

Other information that should inform the R&D Agenda.

Governance tokens grant their holders permission to participate and influence protocol and other platform-related decisions, with the weight of their influence being proportional to the share of tokens held. Changes to a protocol can be proposed, after which they are vetted and voted. Using a token in this way is the case of Decentralized Autonomous Organizations (DAOs).

- By allowing DAO members to directly engage in the governance of their company, these decentralized governance frameworks enable cooperation in otherwise distrustful situations and flattened organizational hierarchies.
- Every member of the organization can have a say in the decision-making process and can suggest changes within the organization for the future.
- DAOs are underpinned by smart contracts, which establish the rules of the organization. Once created and set in place, the smart contract guarantees that all DAO activities abide by pre-coded rules. The smart contract can only be changed through a vote by all involved members.

DAOs are still a work in progress. Most DAOs are still testing their governance systems and trying to understand the best way to deal with imbalanced voting rights and reach full decentralization status.

Nevertheless, DAOs have a lot of potential— from putting power into the hands of its members and offering huge scalability to organizations, to giving them global accessibility by removing geographical barriers, and to providing a great platform for funding investments.

About Tata Consultancy Services (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For over 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge.

TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 616,000+ consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit www.tcs.com and follow TCS news at @TCS_News.

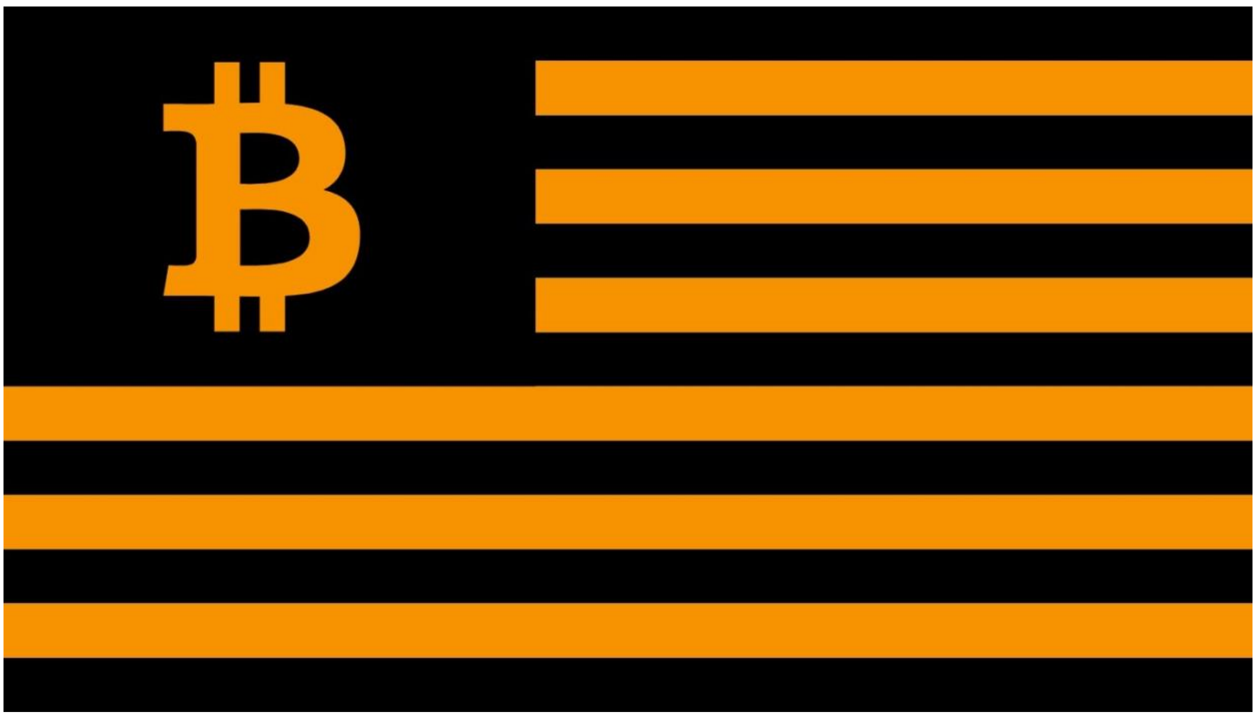
Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Thomas McCarthy

Bitcoin: Freedom Money

By:
Thomas McCarthy



Thomas McCarthy
Member of the Public
[redacted]

“You can resist an invading army, you cannot resist an idea whose time has come”

Victor Hugo

Introduction

The United States is known as the land of opportunity where anyone with a strong work ethic can accomplish their largest dreams and achieve the American Dream. Western media, schools, and U.S. institutions constantly reinforce the notion that the American Dream is accessible to all, regardless of social standing. My name is Thomas McCarthy and I’m a member of the public.

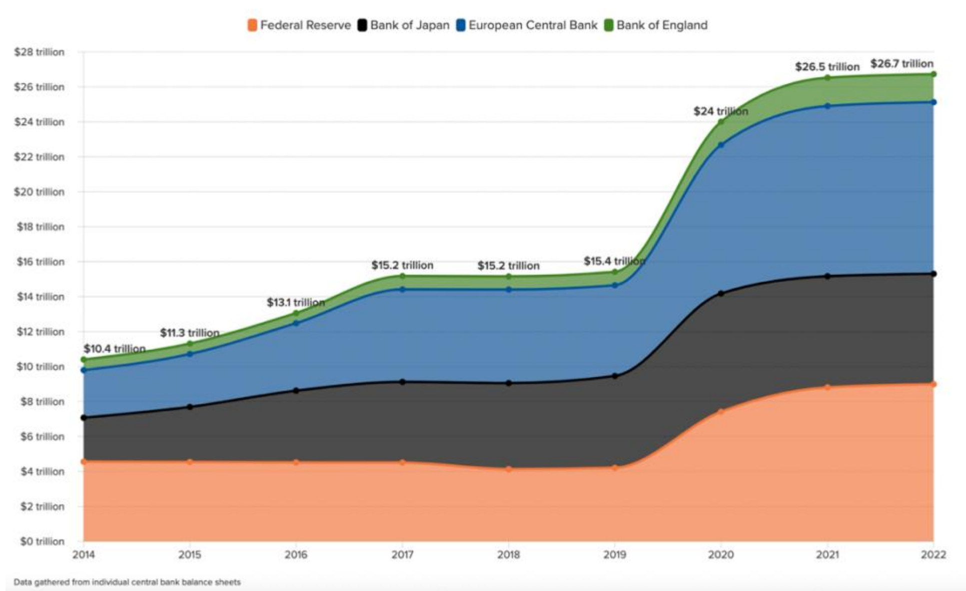
A defining moment in my life occurred in the midst of the Great Recession of 2008. A shattering realization unearthed when I understood the U.S. financial system contained systemic policies that overwhelmingly favored rich incumbents while suppressing everyone else. Witnessing the U.S. government in 2008 bailout Wall Street with taxpayer funds while individuals received home evictions forced me to begin questioning the validity of the American Dream. A society where powerful elites enact policies to protect themselves from bankruptcies using public money is not a land of equal opportunity. These actions diametrically oppose the American values of equality, open economic mobility, and free market capitalism. Although I was a fervent believer in the American Dream, I lost hope it existed – until I discovered Bitcoin.

The Bitcoin network is a decentralized global digital payment system not controlled by any person, company, or nation state. It is an open, monetary network where the same rules apply to all participants. The Bitcoin protocol avoids discrimination against an individual since it allows anyone with internet to transfer value, participate in governance, and validate transactions. Bitcoin embodies American values and breathes life to the American Dream by establishing a society that voids powerful individuals from manipulating the financial system, offers everyone an equal opportunity to achieve economic freedom, and provides a chance to build generational wealth for those who dive down the Bitcoin rabbit hole.

Bitcoin

Bitcoin's launch spawned a digital monetary network whose market capitalization in thirteen years grew from zero to over $1 trillion at its peak. Bitcoin (BTC) is a finite digital asset since there will only ever be 21,000,000 BTC in existence. As Benjamin Franklin famously stated, "in this world, nothing is certain except death and taxes" (NCC Staff, 2021). We can now add a third item – and that is 21 million BTC. Bitcoin is an immutable digital asset with provable scarcity, a decentralized store of value, and it serves as the monetary unit for the Bitcoin protocol. Digital gold, a common analogy for bitcoin (lowercase 'b' is the asset), fails to fully give justice to Bitcoin (uppercase 'B' is the network).

BTC attains its scarcity through math, code, energy, and the growing millions of Bitcoiners all around the world who believe in enforcing the hard-capped supply. No other asset class including oil, commodities, bonds, or equities can claim to have a fixed supply, and in most cases their supply increases. The transparent nature of Bitcoin's open-source code allows anyone to verifiably check both the existing and maximum supply of BTC. Bitcoin's monetary policy operates in stark contrast to central banks that change the supply of fiat currencies ($USD, €EUR, £GBP, etc.) on a whim.



Since 2020, the big 4 central banks have collectively printed around $11 trillion dollars which propped up asset prices at the expense of weakening the purchasing power of fiat currency (Atlantic Council Research Team). Fiat currencies are promissory notes, such as the United States Dollar (USD), that have value solely due to an issuing central authority deeming them to have monetary worth.

Central banks occupy a monopoly on monetary policy for fiat, and individuals have zero recourse to voice their opinion on the currency they own. Seven individuals comprise the Board of Governors at the Federal Reserve (Fed), and this small group controls the money supply for billions due to the dollar's global reserve currency status. Human actions are always susceptible to two outcomes: greed and human error. An example of greed at the Fed most recently showed itself with "the resignation of two Federal Reserve chiefs amid a stock-trading scandal" (Christopher Condon, 2021). Kristalina Georgieva, director at the International Monetary Fund, expressed concern with human miscalculations since central bankers "are not paying sufficient attention to the law of unintended consequences" when they print money (McMaken, 2022). Bitcoin is an alternative system, and its principles exemplify values of which America was founded upon.

Bitcoin & American Values

Bitcoin epitomizes American values since many of its key properties mirror the most important amendments in the U.S. Constitution concerning freedom. Bitcoin symbolizes the spirit of the U.S. Constitution through its protection of unreasonable seizures, free speech, and property rights. Americans are fortunate to live in a country with strong personal liberties, however, U.S. citizens and companies may still face violations of their rights.

In 2013, the Department of Justice engaged in Operation Chokepoint, which included "several independent federal agencies taking it upon themselves to shut legal businesses… out of the banking system" (Michel, 2018). The FDIC acknowledged this wicked behavior in their own press release stating that "certain employees acted in a manner inconsistent with FDIC policies" and this may have included “regulatory threats, undue pressure, coercion, and intimidation designed to restrict access to financial services for lawful businesses” (Robinson, 2019). These actions oppose America’s founding ideology of preventing government overreach. The fourth amendment in the Constitution states “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…” (Constitution of the United States). BTC is a seizure-resistant, digital-bearer monetary instrument. BTC held in self-hosted wallets (analogous to a physical wallet) prevents malicious governments from unreasonably seizing one’s money. This is thanks to Bitcoin’s protocol that provides storage and security without the need for centralized entities.

The Human Rights Foundation details how many “activists and NGOs find it very difficult to access traditional banking services” since “governments and banks can freeze their accounts” (Neuman, 2020). Once an activist group has access to their funds blocked, they can no longer pay their employees, vendors, and sustain operations, effectively grinding their organization to a halt. Bitcoin’s true power is the combination of an unseizable digital asset and a decentralized digital payment system, which allows aid groups to circumvent the problem mentioned above. In fact, the Human Rights Foundation even launched a donation fund to support Bitcoin software development “so that it can better serve as a financial tool for human rights activists, civil society organizations, and journalists around the world” (Human Rights Foundation, 2020).

All nations have centralized banking systems that give them the ability to seize most traditional assets including bank deposits, equities, and land at the snap of a finger. 2022 proved that unjust asset seizures can even occur in western democracies that were previously considered safe from authoritarian practices. Justin Trudeau, Canada’s prime minister, controversially invoked emergency powers to quell protestors and “as many as 210 [bank] accounts holding nearly $8 million were frozen” (Dress, 2022). The Canadian government weaponized the banking system on their own citizens and unilaterally blocked protestors and their supporters from accessing their own money. Individuals that peacefully protest their government should never be subject to financial oppression.

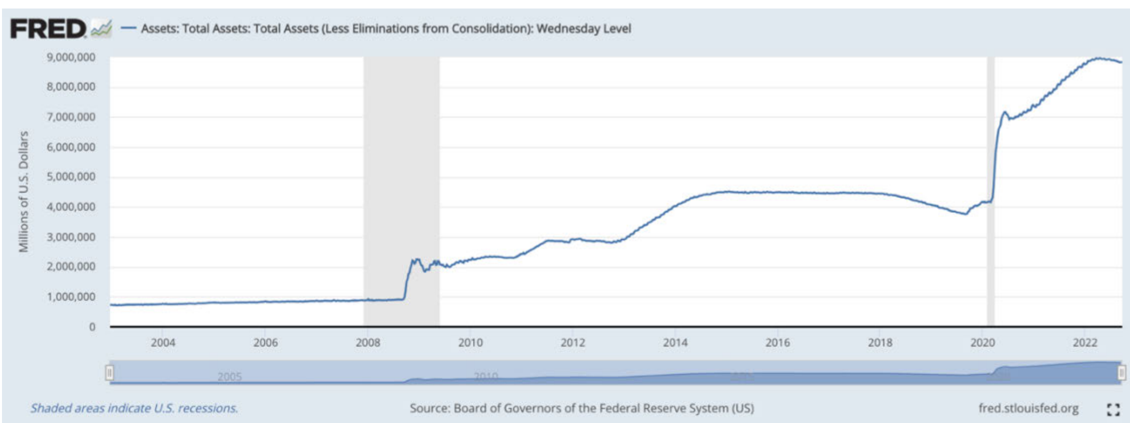
A key component to understanding Bitcoin's strong resiliency is that Bitcoin Core (Bitcoin's client software) is open-source software. Microsoft, Apple, and Google applications all use closed-source software, which makes their code unavailable to the public. "Open-source software operates with the underlying principles of peer production and mass collaboration", it is free to use and available to everyone (IBM). Open-source projects rely on a community to share ideas, review, and change the source code. In the 1996 *Bernstein v. Department of Justice* case, judge Patel stated that the "court can find no meaningful difference between computer language… and German or French… like music and mathematical equations, computer language is just, language" (Dame-Boyle, 2015). This important case laid the foundation to establishing code as free speech, which falls under the protection of the Constitution. The first amendment in the Constitution states "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech…" (Constitution of the United States). Bitcoin Core is the expression of language, and American values uphold free speech as a pillar to a functioning democratic society.

Another key pillar to a free society is property rights. Property rights "is the exclusive authority to determine how a resource is used" (Alchian). The fifth amendment in the U.S. Constitution outlines how no one should "be deprived of life, liberty, or property… nor shall private property be taken for public use…" (Constitution of the United States). Unfortunately, there are still billions of people living with a severe lack of property rights. This disproportionately negatively affects women since "half of the countries in the world are unable to assert equal land and property rights despite legal protections" (World Bank, 2019). Poor legal services, corrupt officials, and a weak rule of law prevents a large portion of humanity from obtaining basic liberties that many people in affluent countries take for granted.

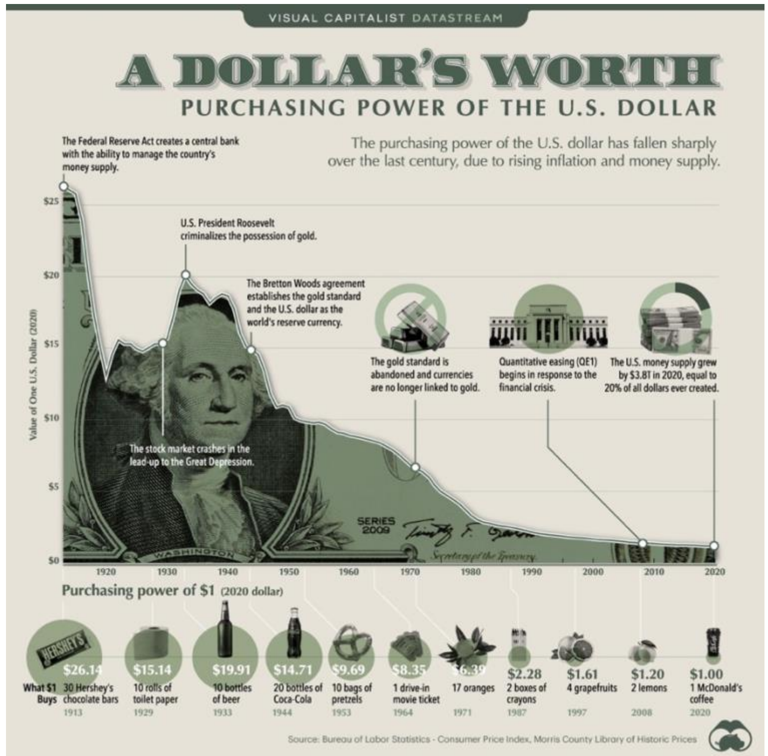
Bitcoin's structure inherently provides property rights to all BTC owners since they have complete sovereignty over their own money. Bitcoin's distributed public ledger allows everyone to agree on the network state without using a centralized party; thus, we can determine *who owns what, when*. Bitcoin achieves this through its native triple-entry accounting system, an extraordinary feature that many overlook. The protocol maintains a record of true bitcoin ownership, and individuals can feel safe knowing that the network (Bitcoin miners) will always defend their digital property rights. Bitcoin incorporates the moralities of freedom, and it is a monetary tool that can be used to escape authoritarian regimes.

Time & Money

One of the primary functions of money is to store value. The economic energy people output is stored in the money they receive, which can then be used to purchase items they desire in the future.



The picture above shows the Fed balance sheet expanding by roughly $4.8 trillion since September 2019. In the span of three years, the Fed printed more USD than the total amount of existing dollars prior to 2019. When the Fed debases USD, they confiscate economic energy from all USD holders and transfer it to themselves. Stolen economic energy refers to all the time and labor Americans expended that is robbed. Stolen economic energy means people lose the chance to spend time with



their loved ones, hobbies, passions, and enjoy all the wonders of life. Monetary policies that confiscate economic energy from working class Americans in order to entrench incumbents is not indicative of a free society.

Money is an evolving monetary technology that society uses to store value across time, and it is a tool we use to exchange for goods and services. Money contains properties which determine its strength: durability, divisibility, fungibility, portability, and scarcity. Bitcoin excels in all of these categories, and it contains advantages over other monies since Bitcoin has (1) a fixed supply, (2) divisible into smaller units, and (3) can be transferred at lightning speed. Bitcoin possesses the most superior properties of money, making it the strongest monetary technology to store value in human history.

	GOLD	BITCOIN	FIAT CURRENCY	
DURABLE	+	+	—	While all are physically durable, fiat currency over history has not maintained purchasing power durability
DIVISIBLE	—	+	+	Physical gold is only divisible to small pieces; bitcoin is divisible to eight decimals
FUNGIBLE	+	+	—	Gold and bitcoin are fungible, but fiat currency is not fungible with other fiat (US Dollar is not fungible with Canadian dollar)
PORTABLE	—	+	+	Gold has a high value to weight ratio, but compared to the others is still heavy and cumbersome to transport
VERIFIABLE	—	+	—	Both gold and fiat currency have been counterfeited; gold can be verified but only through cumbersome assay
SCARCE	+	+	—	Gold is scarce, bitcoin is scarce and finite; the only constraint on fiat currency is willingness of government or central bank
TRACK RECORD	+	—	—	Gold has the longest track record as money and maintaining purchasing power; bitcoin's history is the shortest; fiat currency has a poor track record[2]

Bitcoin has a hardcoded monetary policy and it runs on a neutral apolitical protocol. This contrasts starkly to the Fed structure, where a few people wield immense power over the inflationary supply schedule of USD. Bitcoin, on the other hand, *does not* care how much money and power you have, or the influential people you may know; the community of over 15,000 Bitcoin nodes from roughly 90 countries ensures that everyone follows the same network rules (Bitnodes, 2022). BTC is honest money where no one can steal economic energy, and everyone is protected from monetary debasement. Bitcoin reinvigorates the American Dream since it creates a more equitable society and offers everyone a chance to build generational wealth.

Bitcoin: the American Dream

Throughout my entire life, I have always been an optimist for America, but I will admit there was a short period of time when my faith in the American Dream faded. The driving force for my doubt stemmed from the 2008 Global Financial Crisis. It is highly unnerving that Americans were abandoned while Wall Street was saved since they were 'too big to fail'. Corrupt elites confiscated wealth from everyday Americans when they stimulated the economy through quantitative easing. At 23 years old, it felt demoralizing struggling in New York City while earning a minimum wage. I lost all hope; that is, until I discovered Bitcoin in 2017.

One of my favorite lessons my grandfather taught me is that *the only constant in life is change*. Society has progressed from the Industrial Age, and we are currently undergoing a transition into the Information Age. This introduces new unique wealth creation opportunities for millennials and Generation Z. The Bitcoin community believes that BTC offers one of the best opportunities to build generational wealth, and it also provides a path for individuals to achieve the American Dream.

A massive mischaracterization of journalists from mainstream media outlets on Bitcoiners is their claim that we buy BTC to purely become rich. Bitcoin is not a get-rich-quick scheme; rather, it is a social movement to enable economic freedom to the entire world through sound money and open access to decentralized financial services. Bitcoin does not discriminate based on social status, gender, ethnicity, sex, etc. Bitcoiners are building a world where people no longer must take on crushing debt to purchase a home, be a wage slave, or have their savings depreciate. Bitcoin offers anyone the chance to build generational wealth for their family and, for the first time in history, this opportunity is available to everyone on Earth. Financial freedom allows individuals to enjoy what I believe is the scarcest asset on Earth: time. Economic freedom will provide people with free time to spend it with their family, friends, passions, hobbies, accomplish their goals, and live a fulfilling happy life.

Conclusion

America's founding predicated on the belief in freedom, property rights, and personal liberties. Bitcoin allows anyone to obtain digital property rights, properly store wealth, exchange value, and possess unseizable money; the significance of this cannot be overstated. Bitcoin's decentralized digital financial network prevents dictators from confiscating money, denying banking services to their dissidents, and financially oppressing their citizens. The unstoppable digital presence of Bitcoin creates an opportunity for the U.S. to export American values to regions of the globe that were previously inaccessible. Increased global acceptance of American values expands U.S. global influence at a time when our leadership role in the world stage is under attack.

Bitcoin is the apex predator of money. When humanity adopts superior technology, we do not look back. Horses were previously the common transportation method until cars arrived, movies were stored in VHS -> DVD -> Streaming, music was in Vinyl -> Cassette -> CD -> Streaming. Bitcoin is a savings technology, and BTC is the optimal asset to preserve wealth, since it holds the strongest properties of money and its monetary policy cannot be co-opted.

The Bitcoin network will become more important as it embeds itself into the world economy, and the U.S. should embrace Bitcoin since it closely aligns with American values. The U.S. must enact pro Bitcoin policy to create a hospitable regulatory environment that supports this emerging critical industry. This situation mirrors closely to the 1990's when Congress passed legislation for a developing technology that was new and unfamiliar to everyone, the internet. The United States "helped ensure U.S. tech dominance by adhering to one simple maxim, *first, do no harm*" (Gonzalez, 2022). Sensible technology neutral regulations for the internet enabled developers to innovate inside the U.S. and led to the largest tech companies in the world to domicile inside America's border. The genie is out of the bottle regarding the next critical monetary evolution: the rise of non-sovereign decentralized digital money. Bitcoin can potentially achieve a $100 trillion market cap. At that level, 1 BTC will equal around $4.7 million and enormous opportunities still exist for people, businesses, and even nation states to capitalize. Early adopters will achieve financial freedom and pro Bitcoin economic zones will experience tremendous growth. The trillion dollar question is: *will this innovation occur inside the United States?*

Undergoing sweeping change or traversing unexplored land can be daunting, but fear has never stopped America from enhancing democratic values, and it should not be the reason we avoid innovation in the digital realm. Bitcoin critics should consider the value BTC brings to society: easy access to sound money, democratizing financial services, instilling property rights, equal opportunity for upward economic mobility, and introducing a monetary system where everyone must abide by the same rules. Bitcoin is hope for a better world, where money is not ruled by rulers; instead, money is built for the people, and the network is governed by the people. The Bitcoin community believes in building a decentralized financial system with freedom at its core. Bitcoin will usher in a world with higher degrees of economic equality, and it resurrects the American Dream. Now, people from across the world can participate and benefit from American values. Bitcoin is hope and freedom.

Fix the money, fix the world.

Works Cited

Alchian, A. (n.d.). *Property Rights*. Retrieved from Econlib: https://www.econlib.org/library/Enc/PropertyRights.html

Atlantic Council Research Team. (n.d.). *Global QE Tracker*. Retrieved January 2022, from Atlantic Council: https://www.atlanticcouncil.org/global-qe-tracker/

Bitnodes. (2022, May). *Reachable Bitcoin Nodes*. Retrieved from Bitnodes: https://bitnodes.io/

Christopher Condon, C. T. (2021, September 27). *Trading Scandal That Rocked the Fed Offers Chance to Reshape It*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-09-27/rosengren-exit-may-give-fed-board-more-sway-in-picking-successor

Constitution of the United States. (n.d.). *Constitution of the United States*. Retrieved from Constitution Annotated: https://constitution.congress.gov/constitution/amendment-1/#:~:text=Congress%20shall%20make%20no%20law,for%20a%20redress%20of%20grievances

Constitution of the United States. (n.d.). *Constitution of the United States Fifth Amendment*. Retrieved from Constitution Annotated: https://constitution.congress.gov/constitution/amendment-5/

Constitution of the United States. (n.d.). *Fourth Amendment*. Retrieved March 2022, from Constitution Annotated: https://constitution.congress.gov/constitution/amendment-4/

Dame-Boyle, A. (2015, April 16). *Electronic Frontier Foundation*. Retrieved from EFF at 25: Remembering the Case that Established Code as Speech: https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech#:~:text=One%20of%20EFF's%20first%20major,way%20for%20international%20e%2Dcommerce

Dress, B. (2022, February 23). *Freeze lifted on bank accounts linked to Canada protests*. Retrieved from The Hill: https://thehill.com/policy/international/595526-freeze-lifted-on-bank-accounts-linked-to-canada-protests/

Gonzalez, A. (2022, January 4). *Lessons learned from 1990s internet commerce regulation: First, do no harm*. Retrieved from The Hill: https://thehill.com/blogs/congress-blog/technology/588282-lessons-learned-from-1990s-internet-commerce-regulation-first/

Human Rights Foundation. (2020). *The Bitcoin Development Fund*. Retrieved from Human Rights Foundation: https://hrf.org/devfund

IBM. (n.d.). *Open source vs closed source software*. Retrieved April 2022, from IBM: https://www.ibm.com/topics/open-source

McMaken, R. (2022, May 10). *Mises Wire*. Retrieved from Mises Institute: https://mises.org/wire/biden-inflation-everybodys-fault-mine

Michel, N. (2018, November 5). *Newly Unsealed Documents Show Top FDIC Officials Running Operation Choke Point*. Retrieved from Forbes: https://www.forbes.com/sites/norbertmichel/2018/11/05/newly-unsealed-documents-show-top-fdic-officials-running-operation-choke-point/?sh=71740eaa1191

NCC Staff. (2021, November 13). *Benjamin Franklin's last great quote and the Constitution*. Retrieved from Constitution Daily: https://constitutioncenter.org/blog/benjamin-franklins-last-great-quote-and-the-constitution

Neuman, N. (2020). *Human Rights Foundation partners with Casa to strengthen Bitcoin security*. Retrieved from Casablog: https://blog.keys.casa/human-rights-foundation-partners-with-casa-to-strengthen-bitcoin-security/

Robinson, F. (2019, May 22). *Statement of the Federal Deposit Insurance Corporation* . Retrieved from FDIC: https://www.fdic.gov/news/press-releases/2019/pr19040a.pdf

World Bank. (2019, March 25). *Women in Half the World Still Denied Land, Property Rights Despite Laws*. Retrieved from The World Bank: https://www.worldbank.org/en/news/press-release/2019/03/25/women-in-half-the-world-still-denied-land-property-rights-despite-laws

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Tomicah Tillemann

TEN

How Digital Systems Will Transform the Future of Money and Development

Tomicah Tillemann

Open-source digital payment networks could not only revolutionize the financial sector, but also provide a foundation for whole-of-society digital transformation. The same technologies that enable frictionless, trusted financial transactions will unlock solutions to public corruption, digital identity verification, social benefits delivery, clean power markets, and even voting. Built correctly, these systems could reinvent the toolbox that government, the private sector, and civil society use to solve public problems.

The systems that societies use to carry out payments and financial transactions come with far-reaching consequences. In the same way a country's choice of transportation infrastructure affects traffic congestion, climate, public safety, and the ability to move people, a nation's choice of payments infrastructure influences economic growth, social mobility, and the ability to move assets.

If you are a member of the middle class in an advanced economy, you may

An exceptional community of thinkers, doers, builders, and problem-solvers provided insights and inspiration along the path to completing this chapter. My sincere gratitude goes to Dante Disparte, Daniel Radcliffe, Anit Mukherjee, Han Sheng Chia, Shimpei Taguchi, Paula Hunter, Lesley-Ann Vaughan, Anca Bogdana Rusu, and Xochitl Cazador for generously lending their time and genius during the journey. While I take sole responsibility for the content, praise should be directed to Ben Gregori and Jordan Sandman, whose diligent research and round-the-clock editing were indispensable to the success of the project. Would that every writing project were shepherded by such a capable team. Lastly, thanks go to my spouse, Sarah Tillemann, whose effervescent talent as an editor is eclipsed only by her superlative brilliance as a partner, friend, and enabler of every task worth doing.

think that the global financial system works reasonably well for you. You almost certainly have access to a government-insured bank account. You use financial products such as credit cards, mortgages, foreign currency exchanges, and loans to move funds, manage liquidity, and build a credit score. And you can transfer money digitally between the accounts of your family, friends, and businesses using services such as Zelle, Venmo, and PayPal.

Widespread reliance on this patchwork architecture to facilitate regular economic activity has led economists and development experts to focus on broadening access to cards, cash, and bank accounts as a means of increasing financial inclusion.[1] Policymakers and finance professionals have, in turn, pursued this goal based on the assumption that bringing more people into the existing financial system is the best way to expand access to the services it provides. However, the goal of universal financial inclusion has been stymied by inefficiencies embedded in legacy payments systems based on cards and cash.

A new generation of digital payment technology not only offers an opportunity to rethink how societies bring people into the financial system, but to reimagine the system itself. If digital payments solutions are deployed responsibly, they could catalyze a revolution in development. A growing variety of digital payment platforms are delivering groundbreaking progress in countries where they have been adopted. Many of these systems use existing technology such as mobile phones and text messaging to operate in low-capacity environments. Telecoms and government agencies are using mobile payments to leapfrog over card-based technologies and traditional financial institutions. Solutions such as M-Pesa in Kenya, BKash in Bangladesh, Bakong in Cambodia, and BHIM and NUUP in India are building a path for hundreds of millions of previously unbanked people to join the global economy. The pandemic accelerated the adoption of digital payment tools as physical banking centers closed and transactions conducted using cash increased the risk of contracting COVID-19.

Digital payment systems alone will not compensate for the effects of bad policy or revive dying industries, but they can significantly reduce levels of friction, corruption, and societal mistrust. As nations struggle to rebuild following the coronavirus pandemic, better payments architecture may prove indispensable to communities, companies, and households looking to deploy resources more efficiently. If these systems are built using open-source code and open standards, they will be able to scale quickly and at modest marginal cost to countries worldwide.[2]

The immediate upside for societies that embrace digital payments could be profound, from eliminating much of the US$30 billion spent each year on

1. World Bank.
2. Lerner.

remittance fees to recouping a portion of the US$3.1 trillion in government revenue lost to tax evasion.[3] In the long run, the benefits could go beyond providing hundreds of millions with access to more dynamic, equitable financial tools.[4]

Digital payment networks, particularly those based on open-source technology, could not only revolutionize the financial sector but also provide a foundation for whole-of-society digital transformation. The same technologies that enable frictionless, trusted financial transactions will unlock solutions to public corruption, digital identity verification, social benefits delivery, clean power markets, and even voting. Built correctly, these systems could reinvent the toolbox that government, the private sector, and civil society use to solve public problems.

This chapter provides an overview for policymakers, regulators, and development practitioners looking to harness the power and potential of these digital systems. It surveys the opportunities and challenges surrounding the use of payments solutions, including:

- The shortcomings of legacy systems;
- Promising cases where digital payment solutions have already been deployed at scale;
- Emerging technologies that could further alter the payments landscape;
- The risk that poor governance could undermine future progress in this space; and
- The ways digital payments infrastructure could enable societies to safely, securely validate and transact with a range of sensitive data and digital assets.

Challenges of the Status Quo

The centrality of outdated payments architecture in daily life and commerce is part of what makes old systems difficult to uproot. In contrast to horse-drawn carriages and telegrams, which long ago assumed their place as quaint relics of centuries past, outmoded payments solutions continue to serve as the foundation of many advanced and emerging economies. Change is hard under the best of circumstances, and change that requires mustering political will to unseat entrenched incumbents, overcome regulatory hurdles, and roll out national technology platforms may seem almost unattainable. As a result of these and other challenges to deploying digital payment systems, many countries simply

3. Cecchetti and Schoenholtz; Werdigier.
4. Demirgüç-Kunt.

layer newer solutions, such as plastic cards, on top of older, analog infrastructure such as cash and paper-based checking accounts. The resulting amalgams of old and new often prove slow, expensive, insecure, and prone to reinforcing economic inequities. These dynamics also make payments systems vulnerable to regulatory capture and, in many cases, the sector suffers from a profound lack of competition.

A number of critiques can be leveled against existing payments infrastructure. Among them, it is:

- *Slow.* Only a quarter of the world's countries have deployed real-time payments systems.[5] Use of instant digital transactions accelerated during the COVID-19 pandemic, but in many regions, including in the United States, only a portion of financial institutions have been able to access and adopt faster systems.[6] The costs associated with slow payments infrastructure fall disproportionately on low-income populations who live paycheck to paycheck. In the United States, the long waits required to process and clear transactions are a prime reason for the US$35 billion spent each year on check cashing, payday lending, and bank overdraft services.[7] Low-income, marginalized populations use these services at disproportionately high rates to access liquidity more quickly.[8] This phenomenon was particularly pronounced during the pandemic, when millions faced financial ruin as they waited weeks to receive paper checks with social benefits and unemployment insurance.[9]

- *Expensive.* In many advanced economies, interchange fees are approximately 2 percent of each transaction.[10] For the United States, that translates to over US$40 billion annually.[11] Like the costs of long delays in settling payments, the burdens associated with these fees fall regressively on low-income consumers.[12] These challenges can be far more acute in cash-based economies. Withdrawals from automated teller machines (ATMs) are often capped at low levels, and each transaction comes with fees equivalent to several dollars. Pulling out enough cash to accomplish even a simple task such as filling up an automobile gas tank may require multiple withdrawals

5. FIS.
6. Ibid.
7. Wilson and Wolkowitz.
8. Brown, Eftekthari, and Kurban.
9. Marbella and Miller; Iacurci.
10. Kansas City Fed.
11. *Motley Fool.*
12. Schuh, Shy, and Stavins.

from multiple ATMs, each with its own transaction costs. Similar dynamics pervade cross-border remittances, a crucial development tool used to transfer over US$500 billion per year to families worldwide.[13] Moving money internationally through financial institutions requires banks to establish trusted relationships with a series of intermediaries in order to convey funds to their intended recipient. The transfer fees charged by each intermediary total US$30 billion per year, money that never reaches the individuals and communities that remittances are intended to benefit.[14]

- *Insecure.* Cash, credit cards, and checks are vulnerable to exploitation on two fronts. First, to varying degrees these systems cannot guarantee that payee and payer make and receive payments as intended. Second, legacy systems can be co-opted and exploited by bad actors. Harvard economist Ken Rogoff has estimated that one-third of all U.S. currency in circulation is used for crimes and tax evasion.[15] Cash is so insecure that responsible regulators would likely never approve it for use today if it were suggested as a new medium of exchange.[16] Credit card fraud costs the global economy over US$27 billion annually, a number that is expected to reach US$35 billion by 2023.[17] Tens of millions of credit card users have also been subject to data breaches that increase their vulnerability to identity theft. Check fraud is an old problem, but it surged back into headlines in 2020, as governments distributed fiscal stimulus in the form of physical checks. When a final accounting is done, criminals may have stolen over US$100 billion in assistance funds intended for needy families following passage of the CARES Act.[18]

- *Prone to reinforcing existing economic inequities.* One-third of the world's population has no access to the formal financial institutions that serve as an on-ramp to the global economy.[19] Unbanked individuals often find it difficult or impossible to secure their assets and may be forced to stockpile cash at home—a risky, sometimes dangerous proposition—if they want to maintain a financial reserve. Alternatives, such as entering expensive or potentially exploitative relationships with rent-seeking middlemen, add to the already high costs of being poor. Surveys of unbanked individuals find

13. De and others.
14. Cecchetti and Schoenholtz.
15. Rogoff.
16. Polemitis.
17. *Nilson Report*.
18. Murphy and Rainey.
19. World Bank Development Research Group.

that the most frequent impediment to accessing bank accounts is cost.[20] In order to combat the fraud and abuse challenges mentioned above, cash- and card-based financial institutions are subject to regulatory requirements to "know your customer" (KYC). The accompanying compliance costs are often too high to serve poor populations profitably. Other barriers to financial access include physical distance to financial institutions, a lack of documentation to validate one's identity, and a lack of trust in available banking options.[21]

What's Working

Technologies to mitigate each of the challenges outlined above already exist. Governments, firms, and civil society organizations have deployed digital solutions that are significantly faster, more efficient, more secure, and more equitable than the systems they replace. The scope and ambition of some of these projects is sufficiently breathtaking to convince even jaded observers that change is possible.

Successful digital payment platforms come in a variety of shapes and sizes. Some are centralized systems deployed by governments. In other cases, a company with broad reach, such as a mobile carrier, may operate national payments infrastructure. As outlined below, these solutions are changing the lives of hundreds of millions of users that rely on them. In Kenya, digital payments have already lifted 2 percent of the country's population out of poverty.[22] However, even the best digital payments systems in use today come with tradeoffs.

Government-backed platforms require ongoing public investment and political support in order to function effectively. Private-sector solutions can easily morph into monopolies with attendant opportunities for rent-seeking. Centralized systems provide bad actors with a vantage point from which to conduct malevolent surveillance. And any digital platform can prove an attractive target for cybercriminals. The solutions highlighted in this section do not follow a specific formula. Rather, they reflect the expanding universe of approaches by countries adopting payment solutions that are fit for purpose in a digital age.

20. Demirgüç-Kunt.
21. Ibid
22. Jack and Suri.

Financial Inclusion in India

Aadhaar, the digital identity platform of the government of India, created the groundwork for a series of payment innovations that are providing financial access to hundreds of millions of the country's citizens. The biometric identity architecture made possible by Aadhaar serves as the foundation for the Aadhaar-Enabled Payment System (AEPS), a cash transfer mechanism that allows government agencies to utilize an electronic Know Your Customer (eKYC) services to deliver payments, along with basic banking services, to millions of Indians. The Unified Payment Interface (UPI), an open payment software that standardizes bank transfer processes, enables apps like the Bharat Interface for Money (BHIM) and BharatQR to facilitate almost 1.5 billion monthly transactions between smartphone users, customers, and businesses.[23] Even those without internet-enabled mobile phones can transfer up to ₹5,000 (approximately US$65) by entering *99#* on a regular, non-smartphone to access a protocol similar to an SMS. By supplying this core technology to a wide range of payment providers, UPI has grown rapidly to power more than half of all digital transactions in India.[24]

Accountable Public Administration in Estonia

Estonia prioritized interoperability to build a whole-of-government approach to digital payments and services. The country's digital platforms allow agencies and banks to offer a range of advanced services. Utility payments, pension contributions, and taxes all rely on common digital infrastructure to channel information between government agencies and citizens' bank accounts. At the core of the system is a digital identity and data exchange platform called X-Road, which securely moves information and assets between individuals, companies, and government agencies. The availability of a trusted digital identity solution streamlines KYC compliance for banks, and enables financial institutions to process mortgages, loans, and even requests to open new accounts entirely online. The system has powerful implications for public administration. By simply confirming the accuracy of information already stored in the system, citizens can file their taxes in under three minutes.[25] Estonia's X-Road framework also takes extensive precautions to safeguard personal data. Users see exactly who is accessing their information and what information has been accessed in order to help identify and deter any illicit use of the platform.

23. *Economic Times BFSI.*
24. Sharma.
25. Enterprise Estonia.

Universal QR Code Payments in Singapore

Singapore embarked on a transition from a card-and-cash-based society to a mobile-first digital economy by centering its payments infrastructure on QR (Quick Response) codes. Singapore's PayNow application uses mobile phone numbers and QR codes to facilitate peer-to-peer digital payments. The country's Government Technology Agency launched the world's first unified standard for using QR codes in digital payments between banks, merchants, consumers, and government agencies, a protocol known as Singapore Quick Response (SGQR). Customers of different banks can easily, instantly exchange funds with each other, pay bills, taxes, and purchase goods and services using just QR codes. Singaporeans rely on a variety of digital payment channels, including credit cards, Google and Apple Pay, and other QR-based payment apps, but half of all adults in Singapore have downloaded the PayNow and PayNow Corporate apps since 2017.[26] Government agencies and banks have also implemented national programs to boost adoption of the SGQR system in the wake of the COVID-19 pandemic, particularly in the food and healthcare industries.[27]

Repurposing Existing Networks in Kenya

Kenyan mobile phone providers leapfrogged the legacy banking system to create SMS-enabled mobile money services for their citizens. Instead of relying on formal financial institutions to serve as on-ramps and off-ramps for Kenyans looking to deposit and withdraw cash, the M-Pesa mobile phone–based money transfer service leverages a network of human agents located in cell phone kiosks across rural and urban areas to exchange cash for digital credits tracked by mobile network giants Vodafone and Safaricom. These agents act like independent ATMs, allowing M-Pesa users to move cash in and out of the M-Pesa system independent of banks. Many transactions traditionally completed using cash or bank payment services, like buying groceries or paying bills, can be accomplished solely with cell phones. Since its launch in 2007, nearly 96 percent of households in Kenya have gained access to mobile money services, lifting over a million people out of poverty thanks to the increased access to financial services.[28] M-Pesa does lock users into a specific mobile vendor, but it has successfully expanded to Tanzania, Mozambique, DRC, Lesotho, Ghana, Egypt, Afghanistan, and South Africa. Other mobile money services, including BKash in Bangladesh and Tigo

26. Monetary Authority of Singapore.
27. Sharwood.
28. Jack and Suri.

in Bolivia, now emulate M-Pesa's SMS-based model, taking advantage of its simplified infrastructure requirements and growing cellular network coverage.

Blockchain-Based Payments in Cambodia

Cambodia boasts a vibrant mobile money provider market, but the highly fragmented digital payment ecosystem elevates prices for financial services and restricts payments between users on different platforms. Bakong, a project by the National Bank of Cambodia, uses blockchain[29] technology to bridge banking systems so that interbank loans and retail banking transactions all occur on a unified settlement system.[30] Consumers and merchants that rely on different banks and payment apps can process transactions in real time, fostering greater adoption of mobile financial services for the unbanked and lowering the cost for new digital payment competitors. By linking payment apps and standardizing QR codes, Bakong will also enable migrant workers to securely and instantly transmit money across borders and submit payments for medical costs or utility bills for family members back home.[31]

Benefits of Digital Payment Platforms

Despite the broad range of approaches, architectures, and technologies outlined in the examples above, the benefits from successful digital payment solutions are remarkably similar across different geographies and contexts. In addition to technical advances such as reduced transaction times and lower costs, digital systems also demonstrate an impressive ability to reach and serve groups that were previously on the margins of an economy or society.

Broader Access

Over the last decade, mobile and digital payments have driven a meteoric rise in financial inclusion. An estimated 1.2 billion people have gained access to basic financial services, which helped many start-up businesses to purchase critical goods and services and build savings.[32] These benefits particularly affect rural communities previously unable to utilize financial services due to limited internet connectivity and the long distances between many rural brick and mortar banking

29. Tillemann.
30. Vireak.
31. Chea.
32. World Bank (2018b).

locations.[33] The gains from digital payment platforms have also aided women and migrant workers. In regions where legal and societal barriers prevented women from independently managing their finances and building wealth, digital payments have afforded women greater control of their income and assets. A study in Kenya showed that mobile money services increased savings by over 20 percent, allowed 185,000 women to transition from agricultural to business occupations, and led to a 22 percent decline in the share of women-led households living in extreme poverty.[34] Migrant workers have gained the ability to manage family finances from abroad and send digital remittances instantly, securely, and at lower cost.[35]

As with any digital solution, there is always a risk that new systems could exacerbate existing inequities. In fields such as digital identity, organizations, including ID2020, have worked to ensure that solutions work for those who lack internet connectivity. It is important for digital payments providers to take similar precautions and design their systems with marginalized individuals in mind. Governments may need to embrace a variety of different payments systems. No society should be entirely dependent on a single solution. Low competition in payment service markets enables operators to charge high prices for products that underserve their users. Whenever possible, digital platforms should give communities new options rather than restrict their freedom of choice.

Enhanced Efficiency

Digital payments are slowly eradicating the antiquated process of reconciling and settling transactions across disconnected financial institutions. Individuals who receive digital government cash transfers spend less time waiting in lines and traveling to collect benefits. Research in Niger concluded that the country's decision to administer its cash transfer program through mobile payments saved enough working hours to enable each participant in the program to feed a family of five for a day.[36] Time savings occur in more advanced economies as well. Estonia's efficiency gains from its X-Road system are equivalent to 2 percent of the country's GDP[37] and give citizens back the equivalent of an extra 844 working years[38] annually. Individuals' ability to repurpose time that was previously wasted visiting banks, government offices, and ATMs to engage in more productive economic and family activity is one of the most powerful benefits in countries where digital payments have been adopted.

33. Bughin and others.
34. Suri and Jack.
35. World Bank Development Research Group.
36. Boumnijel and others.
37. See www.ipinst.org/2016/05/information-technology-and-governance-estonia#3.
38. See https://e-estonia.com/solutions/interoperability-services/x-road/.

Reduced Transaction Costs

Mobile payments largely eliminate the need for expensive point-of-sale terminals and interchange fees paid to financial intermediaries. Just as telecom companies can transmit text messages at the marginal cost of 1/1000th of a cent, mobile payment networks drive the cost of facilitating a transaction close to zero.[39] Lower transaction costs are encouraging many countries that lack legacy payment systems to opt for digital solutions instead of card-based infrastructure. Decentralized digital interbank settlement systems such as Ripple and Corda also reduce the cost of existing financial infrastructure. In principle, the interoperability and lower transaction fees available through use of these platforms should allow banks to reduce compliance budgets and lower the cost of services for consumers. Low transaction costs can also open the door to micropayments, and the multitude of potentially revolutionary new business models they create for everyone from street vendors to journalists. An economy in which moving assets is as easy as moving information via text or e-mail could develop new market mechanisms and incentives that more accurately reward the creation of value across society.

Increased Accountability

Interoperable payments and identity verification systems can reduce waste, fraud, and abuse in public and private finance. Estonia's digital payments system allows its government to transfer funds to citizens with a high degree of confidence that the money will reach eligible, intended beneficiaries. India's digital identity and payments platforms eliminated an estimated 47 percent of leakage after it was introduced, amounting to US$9 billion of savings each year.[40] The better data that comes with the use of digital payments systems can also help governments deploy data-driven economic and social policies.

Ensuring Responsible Governance of Payments Architecture

The remarkable benefits afforded by digital payment platforms come with a caveat: their utility depends on ensuring that systems are used responsibly and safeguarded from bad actors. Along with electrical power and computer code, digital payment networks run on trust. People need to have confidence that the platforms they trust with their hard-earned funds will operate as intended. Government efforts to illicitly manipulate or surveil networks are a clear and present danger to the long-term efficacy of digital payment systems. The potential for

39. Barker.
40. *Business Today*.

cyberattacks that compromise platform availability or integrity represent another significant concern. Either risk could quickly undermine users' confidence—and the otherwise positive outcomes associated with the use of digital payments.

Effective, responsible platform governance is the best insurance against the challenges posed by bad actors. Its importance will escalate as authoritarian governments continue to develop and export payments solutions that are both highly innovative and extremely compromised.

Alipay and Tencent's WeChat Pay, the two dominant Chinese payment platforms, include tightly integrated access to everything from bill payment and bank account management to food delivery, social media, ride shares, transit tickets, insurance, digital ID, and document storage. These platforms are among the most ambitious, successful payments solutions available anywhere in the world, and the Chinese Communist Party (CCP) is encouraging their global adoption through its Digital Silk Road and Belt and Road Initiative.[41] The CCP is also piloting a Digital Yuan, which could allow party officials to surveil the transaction history of anyone who uses their digital currency and offer similar capabilities to friendly regimes across the world. Though the CCP claims to have introduced privacy protections as a feature of the Digital Yuan, party officials reserve the right to monitor for transactions they deem illegal or a threat to national security. These measures could assist efforts to limit the economic freedom of ethnic minorities or political dissidents. In societies dependent on digital payments, a government's ability to "de-platform" users by denying them access to funds or the ability to engage in transactions could provide a penalty almost as devastating as physical incarceration.

These trends should be deeply concerning to democratic governments. The United States, in particular, has exercised significant influence over the global financial system through SWIFT—the Society for Worldwide Interbank Financial Telecommunication—an international settlement mechanism that facilitates dollar-denominated payments between countries via U.S. banks. The United States has used SWIFT to freeze international payments by individuals and organizations that finance terrorism, engage in criminal behavior, and violate international laws. SWIFT maintains strict privacy policies and is designed to extend democratic values of transparency, accountability, and the rule of law through international financial markets.[42] If innovative systems developed by authoritarian governments outcompete aging, vulnerable financial structures like SWIFT, it could have profound implications for the global system. Going forward, a country's choice of digital payment systems and digital infrastructure

41. Olsen.
42. SWIFT.

may be as important to shaping its geopolitical orientation as membership in NATO or the Warsaw Pact was a generation earlier.

The responsible governance of digital payment architecture is too important to be left to governments alone. Ideally, multi-stakeholder models with oversight from civil society, academia, the private sector, and other independent institutions could help safeguard the privacy and security of platform users. Under any circumstance, citizens and democratic governments should be wary of the serious dangers posed by digital payment systems that lack adequate oversight, privacy protections, and accountability mechanisms.

The Frontiers of Digital Payment Architecture

Despite real governance concerns, existing digital payment technologies are delivering immense benefits. The potential reach and impact of the revolution in payments technology is poised to accelerate as new technologies nearing deployment begin to come online. These innovations could empower consumers to design their own financial tools, redefine the concept of money with programmable currency, and allow payments to cross borders seamlessly. As these technologies begin to take hold, they will reshape the concept of the global financial system along with initiatives aimed at financial inclusion.

Mojaloop: A Digital Payment System as a Digital Public Good

Virtually all payment systems are designed and controlled by governments, companies, or consortia. Thanks to a powerful new category of technology solution—digital public goods—that could soon change. Digital public goods are open-source software platforms with the potential to transform the "walled gardens" of proprietary payment systems into open ecosystems that are created and maintained for societal benefit. Mojaloop is an open-source software platform that bridges divides between siloed digital payment providers. Mobile networks such as Orange and MTN are using Mojaloop to connect 100 million registered mobile money accounts into an interoperable network. The government of Tanzania is leveraging Mojaloop to break down data silos between financial providers and reduce transaction costs among businesses and individuals.[43] Open-source development can improve transparency and security of critical systems while providing organizations of all sizes with access to high-quality, interoperable digital payment systems at extremely low cost.[44]

43. Dominguez; Hunter.
44. Lerner and others.

Direct Cross-Border Payments with Stablecoins

Historically, national borders have presented an exceptionally expensive barrier to financial transactions. Stablecoins, digital currencies that provide the benefits of instant processing and finality of transactions while ensuring the stability of a government-backed currency, may erode the costs of international transfers to the point of irrelevance. Instead of relying on expensive networks of intermediary banks, stablecoins take advantage of blockchain technology to create decentralized digital accounting systems. Stablecoins are pegged to fiat currencies and designed to avoid the price fluctuations that affect cryptocurrencies with market-based valuations, such as Bitcoin. The result is a stable currency that can be transmitted across continents without intermediaries and associated costs. Numerous stablecoins are preparing for launch or already in circulation. For development actors, two of the most significant are USDC (US Dollar Coin) and Diem.[45] Several other blockchains are being used to anchor stablecoins, including Stellar, Solana, and Celo.

USDC is a stablecoin developed by Circle, a fintech company based in Boston, and administered through the Centre consortium. As of mid-year 2021, there is over US$25 billion of USDC in circulation, and it is rapidly gaining traction as a regulated solution for applications that rely on a stable digital currency. Facebook incubated Diem, previously called Libra, before spinning out the project as a nominally independent social impact organization with multi-stakeholder governance. The engineering heft and global reach of the project's progenitor organization provides Diem with a big head start as it works to become the default digital currency for low-cost, instantaneous cross-border exchange. However, the platform has faced significant regulatory scrutiny along the way, largely as a consequence of its Facebook roots. Stellar is a multipurpose blockchain that allows users and institutions with different stablecoins (such as a digital dollar or a digital euro) to seamlessly transact without intermediaries, creating a global network of interoperable financial systems.[46] Celo and Solana are high performance open-source networks that allow users to buy and sell stablecoins by equipping developers with tools to build decentralized financial applications.[47] Solutions on the Celo platform include lending tools for refugees, integration with M-Pesa, and universal basic income systems for vulnerable communities.[48]

45. This chapter was originally drafted while the author was an employee at New America, a nonprofit organization. As of July 2021, the author became a partner at Andreessen Horowitz, which invests actively in this domain, including in Diem, Celo, and Solana, all of which are mentioned in this chapter.

46. Stellar Development Foundation.

47. Slavich.

48. See examples at Celo DApp Library (https://docs.celo.org/developer-guide/celo-dapp-gallery).

Empowering Government Economic Policy with Central Bank Digital Currencies

The advent of blockchain technology has pushed central banks to reimagine how they manage national currencies in the digital era. Central bank digital currencies (CBDCs) could equip national currencies with new properties and improve how central banks, policymakers, and financial regulators manage money supplies and economic policy. Programmable digital currency could give governments more control over how consumers use social benefits or stimulus payments. Policymakers could program expiration dates for using cash transfers to help spur growth during slowdowns or limit the use of funds to small businesses or vulnerable industries.[49] Nearly 80 percent of the world's central banks are exploring CBDCs at either the retail or wholesale levels, with Sweden's Riksbank, the People's Bank of China, and the European Central Bank among the growing number already pursuing efforts to operationalize CBDCs.[50] Multilateral institutions such as the IMF, World Bank, and G20 are actively assessing how CBDCs could transform governments' role in finance.[51] CBDCs will need to be managed responsibly in order to realize their potential. In the absence of effective governance, they could merely port the problems of analog currencies to the digital realm.

Digital Payment Platforms and Data Stewardship

In the same way nuclear energy can power a city or destroy it, and steel can be used to build hospitals or machetes, digital payments can advance human dignity or oppress and surveil entire populations. On their own, digital payment platforms are neutral. Against this backdrop, a new opportunity is emerging for societies to adopt data models that grant users more control over their payments data.

The world's governments currently rely on two models that govern financial data. Both are vulnerable to abuse and fail to ensure individuals have control over their information. Payments systems in India and China centralize control of transaction data in government agencies that are vulnerable to privacy breaches and manipulation for political purposes. Western democracies allow private firms to package and sell payment data to advertisers who then try to influence individual behavior. In a 2015 study, MIT researchers were able to identify individuals using credit card metadata with a 90 percent success rate if they knew

49. Yu.
50. Press Trust of India; Bharathan; European Central Bank.
51. Financial Stability Board.

the details of just four individual purchases.[52] As governments begin to leverage digital platforms to power their institutions, they should rethink data ownership and data protection rules to help citizens own and control their personal data.

Placing users at the center of public data architecture could give individuals more autonomy over how private firms, governments, and researchers use their transaction history. User-centered data models could also help individuals control and monetize the value of their financial data, maintain higher degrees of privacy, and prevent government overreach and use of personal data without individuals' consent.

From Digital Payments to Digital Assets

Estonia, India, and a growing list of other countries are demonstrating the vast potential that exists when societies link digital payment platforms and digital identity verification. These two foundational pieces of digital infrastructure, along with mechanisms for responsible data management, can unlock a multitude of next-generation tools to power more productive societies and effective institutions.

The technologies that support digital payments and digital identity allow users to securely verify and transfer not only currency, but any unique, valuable data. The digital payments systems that provide data rails for secure, online financial transactions could be repurposed to exchange digital votes, licenses, educational credentials, carbon credits, and public benefit vouchers, all while maintaining a high degree of confidence that these assets could not be duplicated, stolen, or altered.

Societies with the capacity to move digital assets easily between trusted actors will have massive advantages in solving some of the greatest challenges of the twenty-first century. Interoperable digital payments and identity infrastructure could:

- *Help public officials and civil society organizations reduce waste and combat corruption.* Digital infrastructure can help manage procurement processes, prevent misappropriation of public funds, and provide new, more efficient methods to collect taxes. Bringing accountability to public revenue management could help governments recover trillions of dollars in public assets currently lost to waste, tax evasion, and corruption.[53]
- *Support a new class of secure public registries.* Governments use registries to establish ownership of property and companies. Creating digital land titles

52. De Montjoye, Radaelli, Singh, and Pentland.
53. UN News.

could unlock the economic potential of the US$9.3 trillion in global land assets that are currently unsecured due to stolen or missing titles.[54] They could also facilitate digital credentials to verify vaccination records, educational credentials, and other licenses.

- *Create trusted digital voting systems.* Digital voter registration and voting systems could mitigate threats to election integrity and support more efficient, secure democratic processes. Voting applications could verify that votes are cast by the intended citizen and transmit votes securely for tabulation.
- *Issue public benefits.* Next-generation benefits distribution could remove cumbersome identification barriers that prevent otherwise eligible recipients from accessing public benefits. New systems could also include features that target assistance to better aid specific communities and businesses while ensuring that public assistance is not stolen or diverted to ineligible recipients.

A Digital Decade for the Sustainable Development Goals

As researchers map ongoing efforts to achieve the Global Goals, one point has become clear: deploying more effective digital platforms may be the only path to achieving the Sustainable Development Goals by 2030. Particularly in light of the COVID-19 pandemic, access to trusted digital systems will be essential to helping societies and institutions rebuild. Among governments responding effectively to the pandemic, virtually all rely on world-class digital systems that enable the frictionless movement of resources and data.

In September 2020, on the margins of the UN General Assembly, a group of key development stakeholders from around the world came together to launch a #DigitalDecade focused on developing open-source solutions to power more effective public institutions.[55] The prime minister of Norway, a president of the Bill & Melinda Gates Foundation, and leaders from across government, civil society, and the private sector all committed to working together to develop a new generation of digital infrastructure. New America's Digital Impact and Governance Initiative has been fortunate to be at the forefront of this work.

From Mesopotamian canals and Roman roads to transcontinental highways and the internet, infrastructure has long provided a catalyst for transforming the landscape of human development. Digital platforms, including digital payment platforms, are the transformational infrastructure of our time. As with any piece

54. Arsenault.
55. New America Foundation.

of monumental infrastructure, these platforms come with risks and the danger that they could be misused. But given the stakes for society and humanity, it is time to start building. For countries that do so responsibly and judiciously, the benefits will be immeasurable.

References

Arsenault, Chris. 2016. "Property Rights for World's Poor Could Unlock Trillions in 'Dead Capital': Economist." www.reuters.com/article/us-global-landrights-desoto-idUSKCN10C1C1.

Barker, Eric. 2012. "How Much Does It *Really* Cost to Send a Text Message?" *Business Insider*. November 12.

Bharathan, Vipin. 2020. "Central Bank Digital Currency: The First Nationwide CBDC in the World Has Been Launched by the Bahamas." *Forbes*. October 21.

Boumnijel, Rachid, and others. 2013. "How Do Electronic Transfers Compare? Evidence from a Mobile Money Cash Transfer Experiment in Niger." Working Paper. Tufts University. sites.tufts.edu/jennyaker/files/2010/02/Zap-it-to-Me_12sept2013_No-Appendices.pdf.

Brown, Nyanya, Bahreh Eftekthari, and Haydar Kurban. 2019. "The Impacts of Payday Loan Use on Financial Well-Being of the OASDI and SSI Beneficiaries." https://mrdrc.isr.umich.edu/publications/conference/pdf/2019RDRC%20P3%20Kurban.pdf.

Bughin, Jacques, and others. 2019. "Digital Identification: A Key to Inclusive Growth." McKinsey Global Institute. www.mckinsey.com/~/media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/mgi-digital-identification-a-key-to-inclusive-growth.ashx.

Business Today. 2017. "Aadhaar Helped Indian Government Save US$9 Billion, Says Nandan Nilekani." October 13.

Cecchetti, Stephen, and Kim Schoenholtz. 2018. "The Stubbornly High Costs of Remittances." https://voxeu.org/article/stubbornly-high-cost-remittances.

Chea, Serey. 2020. "Cambodia Edges toward Digital Payments." www.omfif.org/2020/06/cambodia-edges-towards-digital-payments/.

De Montjoye, Y.-A., L. Radaelli, V. K. Singh, and A. Pentland. 2015. "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata." *Science*, v. 347, no. 6221.

De, Supriyo, and others. 2020. "Migration and Development Brief 33: Phase II: Covid-19 Crisis through a Migration Lens." www.knomad.org/sites/default/files/2020-11/Migration%20%26%20Development_Brief%2033.pdf.

Demirgüç-Kunt, Asli, and others. 2018. "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution." Washington, D.C.: World Bank.

Dominguez, Juan. 2019. "Mowali Tackling Payment Interoperability in Africa." www.sofrecom.com/publications/mowali-tackling-payment-interoperability-in-africa.

Economic Times BFSI. 2020. "UPI Transactions Reach Their Peak in July with US$1.5 Billion."

Enterprise Estonia. "Business and Finance: E-Tax." https://e-estonia.com/solutions/business-and-finance/e-tax/.

European Central Bank. 2020. "Report on a Digital Euro." www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

Financial Stability Board. 2020. "Regulation, Supervision, and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations." www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/.

FIS. 2020. "Flavors of Fast 2020," 7th ed. www.fisglobal.com/en/flavors-of-fast.

Hunter, Paula. 2020. "The Blueprint for Financial Inclusion—Mojaloop's Vision for Solving the Unbanked Problem." https://thepaypers.com/interviews/the-blueprint-for-financial-inclusion-mojaloops-vision-for-solving-the-unbanked-problem—1245814.

Iacurci, Greg. 2020. "The 'Black Hole' of Unemployment Benefits: Six Months into the Pandemic, Some Are Still Waiting for Aid." CNBC. September 27.

Kansas City Fed. 2018. "Credit and Debit Card Interchange Fees in Various Countries." www.kansascityfed.org/~/media/files/publicat/psr/dataset/intl_if_august2018.pdf.

Lerner, Mark, and others. 2020. "Building and Reusing Open-Source Tools for Government." www.newamerica.org/digital-impact-governance-initiative/reports/building-and-reusing-open-source-tools-government/.

Marbella, Jean, and Hallie Miller. 2020. "Down to Their Last Dollars, Living off Family and Friends, These Marylanders Are Still Waiting for Unemployment Payments." *Baltimore Sun*, October 15.

Monetary Authority of Singapore. 2020. "MAS Urges Use of Digital Finance and E-Payments to Support COVID-19 Safe Distancing Measures." www.mas.gov.sg/news/media-releases/2020/mas-urges-use-of-digital-finance-and-e-payments-to-support-covid-19-safe-distancing-measures.

Motley Fool. 2017. "This Is How Credit Card Companies Hauled in US$163 Billion in 2016." NASDAQ. April 13.

Murphy, Katy, and Rebecca Rainey. 2020. "'Too Sweet of a Pie': Cybercriminals Steal US$8B in COVID Relief Funds." Politico, October 12. www.politico.com/news/2020/10/12/unemployment-fraud-coronavirus-428514.

New America Foundation. 2020. "[ONLINE]—Launching a #DigitalDecade to Strengthen Public Institutions." www.newamerica.org/digital-impact-governance-initiative/events/un-general-assembly-2020/.

Nilson Report. 2019. "Card Fraud Losses Reach US$27.85 Billion." https://nilsonreport.com/mention/407/1link/#.

Olsen, Sam. 2020. "China Is Winning the War for Global Tech Dominance." *The Hill*. October 4.

Peng, Chan Wai. 2019. "Singapore's Public Healthcare Agencies to Adopt SGQR Payments by End-2020." *Business Times.* November 11.

Polemitis, Antonis. 2014. "How Cash Would Be Seen by the Media if Invented Today." Coindesk, February 23. www.coindesk.com/cash-invented-seen-media-today.

Press Trust of India. 2020. "China's Official Digital Currency 'DC/EP' Begins Testing." *The Week*. April 20.

Rogoff, Kenneth. 2016. "The Curse of Cash." Princeton University Press.

Schuh, Scott, Oz Shy, and Joanna Stavins. 2010. "Who Gains and Who Loses from Credit Card Payments? Theory and Calibrations." Federal Reserve Bank of Boston.

Sharma, Niharika. 2019. "UPI Now Fulfills over Half of All Digital Payments in India." *Quartz India*. November 6.

Sharwood, Simon. 2020. "Singapore to Accelerate Digitalization of COVID-Kicked Economy," *Register.* July 1.

Slavich, Vanessa. 2019. "An Introductory Guide to Celo." https://medium.com/celoorg/an-introductory-guide-to-celo-b185c62d3067.

Stellar Development Foundation. 2020. "Stablecoins: The Future of Digital Money." www.stellar.org/blog/stablecoins-the-future-of-digital-money.

Suri, Tavneet, and William Jack. 2016. "The Long-Run Poverty and Gender Impacts of Mobile Money." *Science*, v. 354, no. 6317.

SWIFT. "SWIFT and Data." www.swift.com/about-us/swift-and-data.

Tillemann, Tomicah, and others. 2019. *The Blockchain Blueprint for Social Innovation.* www.newamerica.org/digital-impact-governance-initiative/blockchain-trust-accelerator/reports/blueprint-blockchain-and-social-innovation/.

UN News. 2018. "The Costs of Corruption: Values, Economic Development under Assault, Trillions Lost, Says Guterres." https://news.un.org/en/story/2018/12/1027971.

Vireak, Thou. 2020. "NBC Launched Bakong Inter-Bank Platform." *Phnom Penh Post.* October 28.

Werdigier, Julia. 2011. "Tax Evasion Costs Governments US$3.1 Trillion Annually, Report Says." *New York Times*, November 28.

Wilson, Eric, and Eva Wolkowitz. 2017. "2017 Financially Underserved Market Size Study." https://finhealthnetwork.org/research/2017-financially-underserved-market-size-study/.

World Bank Development Research Group. 2014. "The Opportunities of Digitizing Payments." https://btca-production-site.s3.amazonaws.com/documents/180/english_attachments/The_Opportunities_of_Digitizing_Payments.pdf.

World Bank. 2018. "Financial Inclusion on the Rise, but Gaps Remain, Global Findex Database Shows." www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows.

———. 2018b. "Financial Inclusion Overview." www.worldbank.org/en/topic/financialinclusion/overview.

Yu, Geoffrey. 2020. "China and the Dawn of Digital Currency." www.bnymellon.com/latam/en/insights/aerial-view-magazine/china-and-the-dawn-of-digital-currency.html.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Web3

Web3 for Health Working Group

March 3, 2023

The White House
Office of Science and Technology Policy (OSTP)
Eisenhower Executive Office Building
[redacted]
DARD-FTAC-RFI@nitrd.gov

RE: OSTP RFI Seeking Comments on Digital Assets Research and Development

Dear White House Representatives:

The Web3[1] for Health Working Group (W3H) is a group of volunteers with experience in the federal government, federal IT vendors, commercial health insurance, and/or health IT consulting. Each member of W3H has a passion for IT standards and believes that **blockchain technology holds great promise.**

W3H envisions a health information ecosystem enabled by Web3 and FHIR[2] where: patients can control their data and can easily find and obtain the services they need, providers' administrative burden and costs are minimal, and payers collaborate with each other on common tasks, to decrease administrative costs for all. This includes a focus on individual autonomy while improving collaboration.

In its first use case, W3H intends to reduce administrative costs in the **flow of healthcare endpoints**[3] by leveraging blockchain's architecture and incentive models to

---

1 By **Web3**, we mean the collection of decentralized technologies including blockchain, cryptocurrencies, NFTs, etc.

2 Fast Healthcare Interoperability Resources (**FHIR**) is the health data standard named in several recent RFIs and proposed regulations from the Centers for Medicare & Medicaid Services (CMS). ,

3 An **endpoint** is a digital address for a computer application/system.

Endpoint Example 1: Dr. Smith establishes a patient-access-API to allow her patients (through mobile phone apps compliant with CARIN standards) to obtain their medical record data. The URL of her patient-access API is an endpoint.

Endpoint Example 2: CMS built and operates a FHIR server/API for the Original Medicare program to receive prior authorization requests from healthcare providers. The URL of CMS' prior authorization FHIR server/API is an endpoint.

promote health data equity, simplify the experiences of patients, providers and payers, and information. W3H's planned deliverables for 2023 include developing open source Web3 protocols, implementation guides, and demonstrating a prototype endpoint registry– compliant with the HL7 National Directory of Healthcare for Providers and Services (NDH) Implementation Guide (IG)– at a FHIR Connectathon. Future use cases for the W3H could include: appointment scheduling, proving eligibility, requesting a cost estimate, moving a referral for an item/service from the referring provider to the rendering provider, claim submission, and many more

W3H thanks the OSTP for releasing this RFI on such an important topic.

General Comments

The healthcare industry produces staggering amounts of data. An August 2022 Health Affairs article finds that "billing and insurance–related costs are a significant source of wasteful health care spending" in the United States. The time spent on these administrative issues takes away from the time that healthcare providers spend on actual patient care. These complex healthcare processes also make it more difficult for patients/clients to access the information they need.

Millions of Americans face challenges daily because the healthcare industry has NOT kept up with other industries as it relates to efficient data exchange. To compare it with the financial industry, in 1969 the ATM was introduced which improved efficiency. And as technologies and consumer expectation adapted, the digital wallet has become more prominent. Since that time, additional financial solutions have allowed individuals to make payment at most any establishment, world wide. The healthcare industry has not kept pace. Today, the best way to make one's healthcare information available is to carry around paper copies or to ask Provider A to fax a medical document to Provider B.

But progress in the healthcare space is on the horizon. One standards development organization, HL7, has pulled organizations together to develop standardized procedures to enable the exchange of complex healthcare data – **interoperability** – between care providers, payers and patients. The new HL7 standard that will promote this interoperability is called "Fast Healthcare Interoperability Resources" (FHIR) and is pronounced "fire."

In the past, most healthcare payers and providers did not make patient data freely accessible via transactional standardized Application Programing Interfaces (APIs). Recent regulatory changes from the U.S. Department of Health and Human Services

(HHS) have required organizations to make this data more accessible using FHIR APIs to exchange healthcare information between:

- health care providers (doctors, pharmacists, hospitals, etc.),
- social care providers (meals on wheels, homeless shelters, etc.),
- health insurance payers, and
- patients/clients

The regulatory push for all providers and payers to make data accessible via API endpoints has been a great first step. But **creating a scalable app capable of accessing all those endpoints is nearly impossible today.** It would require integrating the app with every one of those care providers and payers. This is similar to having a library of books with no card catalog. Very few organizations have the budget required to overcome this barrier of entry.

Having a catalog of provider/payer information (also called a "shared directory" or "registry") is the first step industry needs to take to avoid much of this duplication and make the healthcare data truly accessible at a national scale. Please note: The Web3 for Health work will NOT replace the important FHIR implementation guide that already exist, most notably the HL7 National Directory of Healthcare for Providers and Services (NDH) IG. Instead, **W3H envisions the web3 initiatives supplementing and complementing the FHIR efforts.**

Information Sought in the RFI

1. ***Goals, sectors, or applications could be improved with digital assets and related technologies.***

   The healthcare sector could be greatly enhanced through digital assets and related technologies. Navigating today's complex healthcare system is daunting for most Americans and is even harder for those who do not speak English as their primary language, those experiencing mental health symptoms, and those struggling with financial challenges or homelessness.

   While FHIR is moving the American healthcare sector in the right direction, the movement towards FHIR-enabled data exchange is slow and thus far has required federal regulation to achieve even limited adoption by healthcare providers and commercial payers. **Adding blockchain's innovative governance models and incentive structures to the existing FHIR infrastructure could produce faster changes to support a patient-centered health IT environment.** Web3 technologies could help our country enhance health program integrity and reduce fraud, waste, and abuse and minimize "pay and chase."

There are also opportunities to combat fraud, waste and abuse using blockchain technologies since transactions would be more accessible for audit. Issues with the company FTX were identified earlier and shared more broadly for this reason. If FTX's transactions were not publicly accessible those illegal activities may have occurred longer and remained undetected. Similarly, Web3 technologies may provide the opportunity to detect, stop and prevent waste, fraud, and bause in medical claims which are often paid without review or – with a very small subset – audited months after they have been processed. Utilizing web3 technologies could enable auditing at a very large scale in near real-time.

The Original Medicare program found that the incentive models work in some parts of the healthcare sector. Recovery Audit Contractors (RACs) were introduced into the Original Medicare program in 2005 through a statutory pilot requirement with annual Reports to Congress. RACs are incentivized to find improper payments in Medicare and when they do, they retain a portion of the improper payments they find.

Web3 technologies such as novel inventive models, could offer a much larger space to prevent improper payments in healthcare. Today many software companies open source code and then offer "bounties" for people who find vulnerabilities.

2. *Goals, sectors, or applications where digital assets introduce risks or harms.*

Protected Health Information (PHI) should never be on public blockchains. And there will always be risks with any technology used to move administrative and clinical data. Some believe that Web3 technologies will produce fewer harms than current procedures which involve mailing and faxing healthcare data all over the country.

Regulatory uncertainty and federal procurement procedures are also something be aware of as we look at how to properly utilize web3 technologies. Lack of knowledge about blockchain among staff at many federal government agencies may stifle advancement. For example, when a federal agency's coordinating group for Health IT released a Request for Proposals for qualified health information networks, several provisions made it impossible for organizations with blockchain solutions to successfully bid.

Introducing blockchain and related technologies into the healthcare sector could introduce some perceived risks among the American public. Educating the public about the possible benefits of blockchain technology outside the financial space will be critical to achieving adoption. W3H believes that reports from federal oversight agencies (such as the GAO report entitled "Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges") would be helpful in educating the public and federal agencies about the possible uses of blockchain in non-financial use cases.

In addition, consideration should be given to the removing or significantly revising regulations that are no longer necessary.

OSTP should consider requiring each federal agency's Office of Inspector General (OIG) to issue a periodic report to OSTP on the possible uses of web3 technologies in the sector that the agency oversees.

3. ***Federal research opportunities that could be introduced or modified to support efforts to mitigate risks from digital assets.***
   In the past, federal agencies have used challenge prizes[4] to reward novel and innovative solutions developed by challenge participants. In fact, two members of the W3H were participants in the 2016 ONC challenge entitled "Use of Blockchain in Health IT and Health-related Research"

   OSTP should consider convening a number of federal agencies involved in healthcare (VA, SSA, CMS, ONC, HRSA, SAMSA, FDA) to hold a series of coordinated challenges for blockchain solutions in healthcare. Challenges could be focused on promoting health equity such as helping people from underserved communities find medical and social care providers, make appointments, receive a referral for specialist care.

4. ***R&D that should be prioritized for digital assets.***
   OSTP should prioritize web3 technologies and approaches in the health care sector for research and development. Approaches could include advanced incentive structures, Decentralized Autonomous Organizations, usage of Non Fungible Tokens (health care insurance card).

5. ***Opportunities to advance responsible innovation in the broader digital assets ecosystem.***
   OSTP should consider partnering with CMS' Center for Medicare and Medicaid Innovation (CMMI), or Center for Program Integrity (CPI) to pilot test the web 3 prototypes that appear most promising.

---

[4] This type of challenge is a thought leadership exercise meant to educate and inform the broader audience on the potential opportunities and implications of a technology. Current and past federal challenges can be found at Challenge.gov

6. *Other information that should inform the R&D Agenda.*

In the future, privacy will continue to be a regulatory focus (GDPR/CCPA)[5] as we become a more digital society. OSTP should research the privacy protecting aspects of innovations occurring in the web3 space with Zero Knowledge Proofs. These would enable data exchange which is critical for digital experiences while still protecting privacy and ensuring the owner of that data remains the steward of the information.

Melanie Combs-Dyer
Leader,
Web3 for Health Working Group

[redacted]

[5] GDPR = General Data Protection Regulation in the European Union.
CCPA = California Consumer Privacy Act.

Federal Register Notice 88 FR 5043, https://www.federalregister.gov/documents/2023/01/26/2023-01534/request-for-information-digital-assets-research-and-development, March 3rd, 2023

Request for Information on Federal Priorities for Digital Assets Research and Development

Washington Technology Industry Association (WTIA)

[redacted]

March 3, 2023

Office of Science and Technology Policy
Executive Office of the President
C/O Nik Marda, Anna Brady-Estevez, and James Joshi
Eisenhower Executive Office Building
[redacted]

To Whom It May Concern:

The Washington Technology Industry Association (WTIA) is a non-profit comprised of over 1,000 member companies in Washington state with a mission to build a robust, equity-centered technology sector that empowers thriving communities. Our members range from small, cutting-edge start-ups to large Fortune 500 companies that collectively employ a significant share of our state's workforce and drive the majority of our state's GDP growth. The technology sector accounts for over a quarter of all jobs in Washington state and represents a fifth of the state's job growth since 2010.

The WTIA Cascadia Blockchain Council is composed of entrepreneurs, technology leaders, companies, and other diverse stakeholders across the Cascadia region of Oregon, Washington, and British Columbia. In its first four years, the Cascadia Blockchain Council took on an expansive industry and policymaker educational effort. Today, it is working to build partnerships with key state executive agencies and legislators on identifying public policy levers to help grow the blockchain sector in the Pacific Northwest. You can learn more about our work via our website, washingtontechnology.org/blockchain.

Additionally, WTIA manages the Advanced Technology Cluster, funded by the Washington State Department of Commerce through a federal Economic Development Administration grant. The goal of the Advanced Technology Cluster is to promote cooperation and advance coordination between stakeholders in the blockchain/DLT and quantum information science space, with the long-term ambition of further elevating Washington into a global leader on these advanced technologies.

[redacted]

We appreciate the opportunity to provide comments on the request for information (RFI) your office issued on January 26, 2023 related to digital assets research and development. While our expertise is not specifically in research and development, the WTIA Cascadia Blockchain Council would like to respond to question one of the RFI, to enhance your understanding of the potential applications of digital assets and related technologies that could be furthered with additional research.

RFI Question 1. "Goals, sectors, or applications that could be improved with digital assets and related technologies: Information about goals, sectors, or applications where digital assets could provide significant value to the public, and examples of where benefits are already being delivered. This includes explanations of the current limitations in how those goals, sectors, and applications are currently advanced with limited use of digital assets and related technologies, and how increased or better use of digital assets could provide a specific advantage over existing approaches in advancing these objectives. Where relevant, respondents are encouraged to justify how digital assets provide unique value for advancing that goal, sector, or application compared to the use of traditional databases or other technologies (e.g., as outlined in National Institute of Standards and Technology Internal Report 8202, Figure 6)."

Broadly, there are opportunities to expand the use of tokens in different sectors, as well as to utilize the underlying technology of digital assets to support improvement and digitization of multiple essential applications.

Tokenization is the process of turning property, real property, and/or other assets into tokens, which are digital assets. It is the process of turning something with value into a unique, digital representation of that value. It also includes a process of removing sensitive information and data from existing business systems, replacing it with an indecipherable token, and then storing the original data in a secure data vault. Tokens cannot be reversed because there is not a specific relationship between the token and its original data. There are opportunities to use tokens in a variety of applications, such as for clean energy credits or real estate, but this is an area where significant research and development will advance the uses.

Additionally, there are many fundamental services, which currently rely on manual processes, that should be digitized and, in that process, would benefit from the inherent aspects of the distributed ledger technologies (DLT) that underpin many

[redacted]

digital assets. In many digital assets instances, DLT offers natively digital records that are stored one after the other in a continuous ledger across multiple sites or nodes. It provides significant privacy and security protection, given its pseudonymous properties. It also reduces manual processes and automates more complex processes that require significant coordination, creates an auditable trail that is cryptographically verified, and removes the need for unnecessary data to be collected and stored by third parties. Each of the following applications represent only some of the possible applications for DLT and would be enhanced when backed by this kind of technology:

- **Verifiable credentials - drivers' licenses, education certificates, employee identification, birth/marriage/death certificates, professional licensing**
    - A verifiable credential is a qualification, identification, achievement, or certification that can be cryptographically verified, often with the use of DLT. This removes the need for paper certificates or drivers' licenses, transferring the credential to a web-based application.
    - These are on-demand, natively digital certificates that can allow an outside party to see only necessary data to verify something specific about the holder. Ideally, it ensures that the holder maintains control of the information that is shared with outside parties.
    - It would also eliminate the need for customers to contact third parties every time they wish to get another copy of a credential. An example of this would be having to contact a college and paying a fee every time a person wants a copy of their school transcript. Verifiable credentials place ownership of the credential directly with the consumer, eliminating this time-consuming manual transaction.
    - At this time, limitations to adoption of verifiable credentials include the lack of a coherent unified trust framework under which companies can create the web-based applications to house the credentials. Companies need this kind of framework to ensure that the credentials are verified by the issuing party and to confirm authenticity with any third party viewing the credentials. A trust framework would also help create interoperability across organizations and states, while helping avoid vendor lock-in of one proprietary provider.

[redacted]

- **Healthcare - health insurance credentials, patient-centered health records**
  - There are multiple manual processes that hinder the customer experience with the healthcare system in the United States and leave customers vulnerable to data theft or malpractice.
  - In health insurance, use of DLT would increase communication between the insurance carrier, the medical provider, and the patient. It would reduce the manual steps a consumer would need to determine whether a provider is in-network and reduce the amount of sensitive information put on paper and then manually entered into various siloed databases with each new provider. It would also streamline the process of admitting patients in emergency situations.
  - In health records, use of DLT would put the control of this sensitive information back in the hands of patients, increasing data security and preventing sale of data to third parties. It would also provide one base system that all medical providers could access, in lieu of records being siloed by the company where a provider works.
  - The primary limitation to both of these use cases is a need for standardization and uniformity of definitions, processes, and forms between health insurance carrier networks and hospital and medical provider networks.

- **Real estate - transactions, titling**
  - The multiple parts of real estate transactions, which are currently done on paper, could be transitioned to using smart contracts. A smart contract is code written into a blockchain or DLT that executes the business rules, or terms of an agreement or contract, outside of the digital environment. It automates actions that would otherwise be completed by the parties in the agreement based on whether specific conditions are met, or not met.
  - In practice, in the context of a real estate transaction, a smart contract would act as the escrow agent, verifying the availability of funds and processing payments, issuing verifiable, digitally native titles, and automating the conditions under which an account would be frozen.
  - Using smart contracts for these transactions would increase accessibility, as computer code would ensure the contract was

[redacted]

- agnostic to the demographics like race, gender, sexual orientation, or age of the parties.
  - Limitations to adoption of DLT for this use case revolve around standardized definitions and processes, as well as acceptance of moving this kind of recording keeping into the natively digital realm.

- **Government processes - record keeping, benefits applications**
  - Government systems at every level are archaic - they require coordinated, time-intensive, costly, manual inputs, which are siloed between agencies and levels, and often do not have the necessary features to keep customer data secure.
  - Use of DLT and cryptography-based technologies to streamline application processes would enhance the user experience and create a one-stop portal for the customer while allowing all applicable agencies to receive information on the back end. It would do this all while keeping the customer's information safe.
  - Skepticism of the security of DLT and a lack of education to policymakers about it limit the uptake of this technology by government agencies.

We appreciate your time and consideration of our comments, and please do not hesitate to reach out in the future.

Sincerely,

Arry Yu
Chair, Cascadia Blockchain Council