TECHNICAL DESIGN CHOICES FOR A U.S. CENTRAL BANK DIGITAL CURRENCY SYSTEM

SEPTEMBER 2022

THE WHITE HOUSE
WASHINGTON

About this Document

Executive Order (EO) 14067 directed the Office of Science and Technology Policy to produce a technical evaluation to facilitate and support the introduction of a Central Bank Digital Currency (CBDC) system in the United States (U.S.), should one be proposed. This document provides an analysis of design choices that could inform the technical design of a U.S. CBDC system. This document is excerpted from a report titled *Technical Evaluation for a U.S. CBDC System,* also published by OSTP.[1, 2]

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at http://www.whitehouse.gov/ostp.

About the Interagency Process

The creation of the report titled *Technical Evaluation for a U.S. CBDC System*, including this set of technical design choices, was coordinated through an interagency process led by the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy, as described in Section 3 of EO 14067. A list of departments and agencies involved in that interagency process is located in Appendix B of the aforementioned full report.

Copyright Information

[1] Technical Evaluation for a U.S. CBDC System. (Sep. 2022). *Office of Science and Technology Policy.*
[2] In this document, references made to other parts of this report (e.g., Policy Objectives for a U.S. CBDC System) may not be contained within this document. To locate these cross-references, please refer to the full report referenced in footnote 1.

Contents

Technical Design Choices for a U.S. CBDC System

EO 14067 directed OSTP to submit to the President a report that addresses the technical aspects of the various CBDC designs, including with respect to emerging and future technological developments. This section provides a list of design choices that could inform the technical design of a U.S. CBDC system, as well as an analysis of their benefits and risks. This section focuses on 18 design choices, divided into six categories: Participants, Governance, Security, Transactions, Data, and Adjustments.

This section:

- Does not presuppose that a CBDC system would use any particular technology (e.g., a distributed ledger technology or a centrally managed database);
- Does not assume that a CBDC system would maintain identical functionality to cash;
- Does not take any position on whether establishing a CBDC system would be in the best interest of the United States;
- Does not prioritize the design choices in order of importance;
- Does not claim that the list of design choices is complete;
- Does not assume a particular distribution model, but does, for the sake of analysis, focus on design choices with more applicability for a retail CBDC system;[3]
- Does not assume that all applicable design features need to be incorporated into a CBDC system at initial deployment;
- Does emphasize that many design choices are linked to other design choices; and
- Does, for the sake of analysis, focus on the two endpoints for the spectrum of possibilities for a design choice, even though hybrid options are possible, or potentially desired.

In order to focus the analysis on the design choices that likely matter to policymakers, this section makes a few starting assumptions about the design of a U.S. CBDC system. While a U.S. CBDC system could, in theory, be mostly "permissionless"[4] from a governance standpoint, this design choice introduces a large number of technical complexities and practical limitations that strongly suggest that a permissionless approach does not make sense for a system that has at least one trusted entity (i.e., the central bank). It is possible that the technology underpinning a permissionless approach will improve significantly over time, which might make it more suitable to be used in a CBDC system. However, given the state of the technology, most of the analysis that follows assumes that there is a central authority and a permissioned CBDC system.

[3] Many of these design choices are likely also applicable to a wholesale or hybrid CBDC system.
[4] A CBDC system could either be managed by a set of trusted entities ("permissioned") or by a network of system participants ("permissionless"), or some combination of the two. This is discussed further in the permissioning design choice later in this report.

Deciding whether a CBDC is in the best interest of the United States will depend, in part, on the specific design choices contemplated for the CBDC system under consideration. The aim of this section is to help policymakers understand these technical design choices and their associated tradeoffs, especially with respect to the policy objectives for a U.S. CBDC system outlined in Section 4 of EO 14067 and expanded upon in the Policy Objectives section of this report. U.S. policymakers should read this section in conjunction with the Department of the Treasury's report titled *The Future of Money and Payments*, in order to get a fuller picture of the design choices important to the decision of whether to issue a CBDC.

Participants

Transport Layer: Less Intermediated vs. More Intermediated

What roles do intermediaries take on, and can people opt to pay each other without intermediaries in certain conditions? Who has access to the payment system technology and at what level?

The transport layer of a CBDC system determines whether a third party must facilitate transfers between two parties, and if so, who the third party or parties are.

A CBDC system could be less intermediated by allowing some amount of peer-to-peer (P2P) transactions, which are transactions that occur without the direct involvement of a financial intermediary.[5] Alternatively, the system could be more intermediated, which would mean that most or all transactions occur with the involvement of a financial intermediary (e.g., transfers made via a bank or private services). This is not a binary choice; there are many fine-grained design choices embedded in this question, including the option to support both less intermediated and more intermediated transactions under different conditions. Even if a P2P funds transfer could be completed without an intermediary, other functions of the system (e.g., account creation) could still require intermediation. Furthermore, though it is easy to imagine transactions being settled by current-day private sector intermediaries, such as banks, it is possible for other CBDC system functionalities to be fulfilled by non-traditional public or private intermediaries.[6]

This design choice is linked to the design choices on transactions, as the transport layer would set the foundation for who can facilitate transactions. This design choice is also linked to the Data design choices, as the transport layer would affect who gets write access to the ledger history, if it exists. This design choice is also linked to the governance design choices, as a less intermediated system would require a vastly different set of governance guidelines and

[5] Potential intermediaries for transaction processing include the central bank, commercial banks, and other third-party entities.

[6] A non-exhaustive list of possible intermediation functionalities includes issuing currency, distributing currency, custody and wallets for currency, validating transactions, settling transactions, provisioning access (e.g., user accounts, know your customer), providing user interfaces, providing customer service, conducting fraud detection, conducting AML/CFT compliance, and resolving disputes. Some of these functionalities would likely require compliance with banking laws and regulations, as well as other applicable laws, such as Federal securities laws. However, other functionalities (e.g., provisioning access) could have different eligibility criteria for intermediaries, allowing a broader range of private entities (e.g., pharmacies, grocery stores) and public entities (e.g., libraries, post offices) to provide these functionalities. In turn, this could help increase financial inclusion and equity, could bring more relevant expertise to bear on providing specific intermediary functionalities, and may promote more innovation in payments technology.

requirements (e.g., who conducts transaction-level remediation when there isn't an intermediate party facilitating transactions?). Finally, this design choice intersects with transaction signing, since multiple-signature transactions may make more sense for an intermediated transport layer.

Design choice benefits and drawbacks are described below:

Less intermediated:

- *Could improve the privacy of sensitive financial data:* A key feature of enabling P2P transactions is that it could mimic the cash-like experience in terms of anonymity and functionality.[7] P2P transactions may not need to be known or recorded by an intermediary, which may increase the CBDC system's capacity to protect the privacy of sensitive data. The privacy benefits would depend on the specific way the P2P system is set up; for example, if P2P transactions are recorded on a public ledger, then it may be easier to identify and track users than via a well-constructed intermediated system that does not record on a public ledger.
- *Could hamper compliance with AML/CFT requirements:* Pure P2P transactions can be designed either where tokens are bearer assets,[8] or where there is account creation. A P2P design with a bearer-asset type token could enable transactions without any intermediary and therefore complicate, and potentially circumvent, AML/CFT obligations even where registration and reporting obligations apply.[9] Alternatively, should transactions be recorded on a public ledger, investigators may be able to use analytics tools to trace transactions.
- *Could affect the improvement of payment systems:* A P2P system may have more limited intermediary[10] costs and fees (which would likely be passed on to participants), possibly making it easier to achieve more cost-efficient financial product and services. P2P transactions can also process small-amount retail transactions quickly and cheaply, freeing capacity for an intermediated layer to handle larger transactions. However, a less intermediated system may displace traditional financial intermediaries and their business models, which may have ripple effects – some potentially negative – throughout the American financial system.

More intermediated:

- *May provide traditional financial and digital protections:* CBDC intermediaries – such as financial institutions or new businesses created for processing CBDC transactions[11] – could help provide key requirements or benefits for a CBDC system, such as facilitating

[7] This could also help with CBDC adoption, and thus, financial inclusion. See, e.g., How America Banks: Household Use of Banking and Financial Services, 2019 FDIC Survey. (Oct. 2020). *Federal Deposit Insurance Corporation*, which notes that one of the top reasons cited by unbanked households for not having a bank account is a concern about privacy.
[8] Here, "bearer asset" refers to an asset where its value is derived from its own digital representation.
[9] In the current U.S. framework, Bank Secrecy Act (BSA) obligations are placed on financial intermediaries.
[10] Even if the CBDC system supports P2P transactions, the complexity needed to facilitate P2P transactions could lead consumers to seek out intermediaries, similar to what has happened in the present crypto-asset ecosystem.
[11] The Bank of England describes a potential industry of "Payment Interface Providers" (PIPs) for processing the commercial and retail sectors' CBDC transactions. See Central Bank Digital Currency: Opportunities, challenges and design. (Mar. 2020). *Bank of England*.

remediation, implementing AML/CFT controls, performing customer service functions, abiding by privacy regulations, and facilitating cross-border exchanges of currencies.[12]

- *Could provide additional benefits and mitigate risks for consumers, investors, and businesses:* An intermediated system could also promote payments innovation by creating incentives for intermediaries to provide new services that build on top of the CBDC system, thus promoting the improvement of payment systems. For example, intermediated exchange can facilitate additional cybersecurity safeguards to protect CBDC system assets. Enlisting intermediaries' existing expertise on this topic would likely benefit the servicing of CBDC system core activities. Furthermore, intermediaries may be better able to bear certain types of transaction risk, because laws and regulations require them to be better capitalized.
- *Could advance financial inclusion and equity:* This approach could allow for non-traditional, more accessible entities to fulfill various roles in the CBDC system, which could help expand access to the CBDC system. For example, there are a variety of intermediaries that have identity verification infrastructure, which could help play a role in increasing the accessibility of the CBDC.[13] It is also possible, however, that intermediaries could negatively affect financial inclusion (e.g., with high fees for CBDC-related services, by not providing equitable access to consumers), as has sometimes happened in the corresponding banking context.
- *May reduce security of CBDC system:* Intermediaries can be attractive targets for attacks. In an intermediated system, the security of the CBDC system as a whole could be harmed by the compromise of intermediaries with inadequate cybersecurity practices.

A CBDC system may also permit people to provision their own intermediary.[14] For example, while most people use intermediary services for email provision, it is possible to set up and host one's own email service. If the permissioning of intermediaries was flexible enough to include individuals, then that may reduce some of the downsides of intermediation by introducing more competition.[15] Additionally, a CBDC system could also make it easy to switch accounts between intermediaries, similar to how mobile phone users can switch between carriers while still keeping their phone numbers.

Aside from intermediation of individual payments, there is also a question of intermediation with the CBDC system itself. A CBDC system could allow retail users (e.g., consumers, businesses) access to CBDC directly from the CBDC system operator, via layers of intermediaries,[16] as a

---

[12] For example, the Monetary Authority of Singapore (MAS) and the Bank of Canada (BOC) explored an intermediated, blockchain-based multi-currency payment system that could facilitate international exchange of currencies. See Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies. (2019). *Bank of Canada and Monetary Authority of Singapore.*

[13] Note that a less intermediated system could be similarly accessible and be marketed by similar entities.

[14] Self-provisioning would not necessarily sidestep obligations under U.S. laws and regulations. Without a third party, these obligations potentially shift to the user designing, implementing, and/or operating as an intermediary. A full consideration of regulatory treatment of such self-provisioned intermediaries is outside the scope of this paper.

[15] A CBDC system could either be managed by a set of trusted entities ("permissioned") or by a network of system participants ("permissionless"), or some combination of the two. Here, permissioning refers to the act of designating an intermediary as a trusted entity.

[16] If this design choice is implemented, a key question concerns the number of layers of intermediaries. In a model where there is only one layer of intermediaries, banking institutions might interface with retail and wholesale

liability of intermediaries, or not at all. Much has been written about this distinction, often framed as a difference between "retail CBDC" and "wholesale CBDC," in other fora.[17]

Interoperability: Less vs. More Technical Interoperability with Other Payment Systems

Can CBDC be widely transferred such that private and public payment systems can be interlinked (including international CBDCs) so as not to fragment the payment system? What kind of interfaces should be built to interface with other payment systems?

Interoperability refers to whether and how a CBDC system can communicate, execute transactions, or transfer data with other payment systems (e.g., fiat systems, international payment systems, other CBDC systems, or other digital assets systems, such as stablecoins) while users may have limited knowledge of the unique characteristics (e.g., data structures) of other payment systems.[18] Here, interoperability is not the same as integration, as the former refers to systems that can talk to each other, while the latter refers to more direct access to other systems.

A CBDC system could be designed to prevent interoperation with other systems or it could be designed to allow for interoperation where appropriate. With less technical interoperability, it could be harder for a CBDC system to communicate, execute transactions, or transfer data with other payment systems. Alternatively, a CBDC system could have more technical interoperability with other payment systems, having the opposite effect.

Design choice benefits and drawbacks are described below:

Less interoperability:

- *May provide consumers with better financial protection:* By reducing interdependence with systems that increase or introduce new risks of cybersecurity and operational incidents, the CBDC system might better protect consumers from spillover effects of issues with other payment systems. Less interoperability can also protect against counterparty risk. There are also non-technical ways to protect consumers that are also relevant here. For example, a certain degree of centralization is beneficial to ensuring consumers can more easily exercise the financial protections they are accustomed to with the transfer of U.S. dollars, such as protections afforded by Regulation E. Additionally, if a U.S. CBDC system were connected with a foreign CBDC system that required different standards for a range of issues, such as privacy, U.S. consumers could lose protections.
- *May provide a more secure CBDC system:* A less technically interoperable CBDC system could provide better resilience during a wide-scale cyberattack. Interoperability

customers, as well as the CBDC system operator. In a model with more than one layer of intermediaries between the CBDC system operator and end users, different banking institutions may interact with different types of users; in this model, smaller banking institutions could interact with retail and potentially wholesale customers, and larger banking institutions could perform other activities necessary for the operating of the CBDC system.

[17] See, e.g., Auer, R. and Böhme. R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review, March*, 89.

[18] This definition of interoperability is derived from the International Organization for Standardization (ISO) definition of interoperability. See ISO/IEC 19763-1:2015(en).

could expand the attack surface, even if the CBDC is not directly integrated with other payment systems.

- *May provide a more functional CBDC system*: Interoperability has a number of challenges that make it relatively challenging to implement with full functionality. For example, in the international context, governance and standards alignment can provide a key roadblock to more interoperability. A less technically interoperable CBDC system may not have to deal with as many obstacles to achieve high functionality as expected.

More interoperability:

- *May improve payment systems:* A CBDC system designed to be technically interoperable with foreign payment systems including CBDCs could enable cross-border funds transfers and payments that are cheaper and faster. Envisioned international, private sector, and non-government organization CBDC system interlinkages have explored asset swaps through a trusted intermediary, interconnected CBDC ledgers, and holding multiple currencies within a single ledger. These interconnections could be difficult to manage, expand the attack surface, and likely require intermediaries to manage the associated risks.
- *May benefit financial inclusion and equity*: With easy interoperability with traditional stores of value, a CBDC system may receive increased uptake from communities and businesses that make limited use of the traditional financial system. Interoperability could also make cross-border payments, such as remittances, cheaper, quicker, more accessible, and more transparent.

The possibility of some interconnection would depend on the type of ledger and transaction structure. Interconnections could also depend on intermediaries or P2P options in the transport layer.

Decisions regarding interoperability should also consider if and how CBDC can be converted to non-CBDC currency on the spot, such as at a point of sale. This may be an important functionality to enable in order to mitigate certain risks, such as the challenge that holding limits might pose for businesses that hold or exchange large volumes of CBDC at a time. A potential solution to this risk might be to enable quick routing of CBDC to a commercial bank deposit account with ease.

Governance

Permissioning: Permissioned vs. Permissionless

Is the system permissioned (and if so, how) or permissionless?

A CBDC system could either be managed by a set of trusted entities ("permissioned") or by a network of system participants ("permissionless"), or some combination of the two.[19] This design choice does not assume the use of distributed ledger technology, but rather focuses on the governance structure of the system regardless of the technology used.

[19] For example, a CBDC system might allow permissionless management for most actions, but require heightened permissions for some actions.

In environments without trusted entities, permissionless systems often trade efficiency or other design features to potentially permit transactions to settle without established counterparty trust relationships or trusted third parties. By contrast, we assume that a U.S. CBDC system will rely on one or more trusted entities, such as the Federal Reserve.

Design choice benefits and drawbacks are described below:

Permissioned:

- *Often better protects privacy of sensitive financial data:* While permissionless systems often build trust and consensus using public ledgers, permissioned systems generally do not require a public ledger. This means that transaction history is generally only viewable by a small number of trusted entities, such as the Federal Reserve, and kept private with respect to others.[20]
- *Helps mitigate risks for consumers, investors, and businesses*: Permissioned systems can simplify transaction remediation, making it easier to protect consumers, investors, and businesses. They could also make it easier to prohibit migrating CBDC to non-compliant trading venues or other organizations engaged in misconduct or fraud, which can also help protect consumers, investors, and businesses.

Permissionless:

- *May have implications for the security of the CBDC system, and thus have effects on the resilience of the financial system:* A CBDC system needs to be highly resilient to vulnerabilities (e.g., insider threats, malicious actors, liquidity risks). A permissionless system invites additional types of malicious behavior, so many other permissionless payment systems have incorporated additional cybersecurity considerations into their design. That design philosophy may make the system more likely to stay operational if several entities go offline or malfunction at any point. It may also mitigate attacks related to trust in one or more trusted entities. However, in practice, vulnerabilities introduced by permissionless systems (e.g., 51% attacks, ambiguity from code forks in the case of a distributed ledger)[21] may offset the purported resiliency benefits from permissionless systems.[22]
- *May not be sustainable or support economic activity:* One of the best-known methods to maintain synchronicity between distributed ledgers – the proof-of-work consensus mechanism – uses a significant amount of energy.[23] Although a permissionless CBDC system would not be required to use proof-of-work, if a U.S. CBDC system did choose to use such a method to synchronize a ledger of transactions, it may not align with the policy objective that a CBDC system should be environmentally sustainable.

[20] This is true for P2P transactions too. A permissioned CBDC system could be designed to permit accessing after-the-fact transaction-level details of P2P transactions, in accordance with appropriate legal protections.
[21] For explanations of these terms and a greater discussion of cybersecurity vulnerabilities, see, e.g., Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, 29(2), e2060.
[22] For a more extensive discussion of vulnerabilities, see researched cited in DARPA-Funded Study Provides Insights into Blockchain Vulnerabilities. (Jun. 2022). *Defense Advanced Research Projects Agency*.
[23] See Climate and Energy Implications of Crypto-Assets in the United States. (Sep. 2022). *Office of Science and Technology Policy.*

Access Tiering: Tiering by User Account vs. Transaction Amount vs. Counterparty vs. None

Are there differences in how transactions or accounts are treated? If so, how are the tiers of accounts or transactions determined (e.g., user account, transaction amount) and for what purposes?

Access tiering refers to the various features that a CBDC system offers that vary based on the attributes of a given transaction.

Transactions could be tiered for a variety of purposes, such as privacy, security, financial inclusion, and promoting a risk-based approach to AML/CFT compliance. For example, a CBDC system could provide "lower" tier(s) where users who provided less identity verification information are subject to transaction limits, while providing "higher" tier(s) whereby users who opened an account and are subject to robust customer due diligence standards could transact without limitations. The tier used for a transaction could be based on the user accounts (e.g., level of customer due diligence) involved in the transaction, the amount being transacted, counterparties involved, or other criteria (e.g., characteristics of an intermediary). Transactions between two less risky accounts (e.g., two personal accounts with small balances) could be facilitated on a lower tier. Transactions below a certain amount (e.g., $3,000, $10,000, or some other dollar amount) could also be facilitated on a lower tier. [24] Transactions could be tiered based on counterparties (e.g., business-to-business payments could be one tier, business-to-consumer and consumer-to-business payments could be another tier, and consumer-to-consumer payments could be yet another tier). Hybrid options are also possible; for example, switching to a higher tier once the total amount transacted between two accounts exceeds a certain amount. Transactions could also not be tiered.

A tiered system has implications for the data design choices; a tiered system requires the ability to record different amounts of permanent and temporary history for different tiers. Access tiering might also be linked to offline transactions, where a lower tier may facilitate offline transactions and a higher tier may require online capabilities. Access tiering is linked to the transport layer, where a CBDC system could support P2P transactions for lower tiers but require intermediaries to facilitate higher tiers (though intermediaries could have the choice to only support certain tiers). Governance, along with whether the tiering needs to be universally adopted within the CBDC system, would also need to be addressed. Finally, access tiering may be linked to identity privacy, with lower tiers facilitating a higher level of privacy in transactions than higher tiers. This report does not address specific tiering thresholds or which entity in a CBDC system would be responsible for setting them.

Design choice benefits and drawbacks are described below:

[24] Canada and Sweden are considering tiering systems based on the value of the transaction. See Central Bank Digital Currency (CBDC): Retail Considerations. (2021). *Bank of Canada,* 13. Note that the specific dollar amount does not have to be taken from existing precedent in other types of financial transactions; a new threshold could be set for the CBDC system's access tiers, based on the unique AML/CFT risk profile of the CBDC system.

★ ★ ★ ★ ★ ★

Tiering based on user account:

- *Has implications for privacy and AML/CFT compliance:* Tiering based on user accounts, depending on how customer information is collected and stored, would promote a risk-based approach rather than solely the amount being transacted.[25]
- *Has implications for financial inclusion and equity:* Tiering based on actors could raise equity questions based on the types of criteria used to determine a customer risk profile.[26] For example, such a system might subject immigrants to enhanced due diligence, if they engage in more cross-border transactions to send money home. Alternatively, by allowing for simplified customer due diligence on lower tiers, financial inclusion might be increased by giving access to individuals who may have previously had problems getting access to an intermediary.

Tiering based on transaction amount:[27]

- *Has implications for privacy:* Tiering based on transaction amount allows for users to conduct lower-value transactions while not meeting other requirements to transact on a higher tier (e.g., providing more identity verification information).
- *Has implications for AML/CFT compliance:* Tiering based on amount would provide a unified way to assess risk, but given that some types of illicit finance transactions (e.g., terrorist financing) could regularly involve lower transaction amounts, this approach might create new vulnerabilities and might be difficult to implement.

Tiering based on counterparty:

- *Has implications for AML/CFT compliance:* Tiering based on counterparty makes it possible to better assess the nature of a transaction, rather than just the amount or accounts involved. This information can then be used as part of a risk-based approach to due diligence.

None:

- *Has implications for AML/CFT compliance:* A lack of tiering means that intermediaries would likely develop and implement their own risk-based compliance programs and incorporate simplified or enhanced due diligence in line with customer risk profiles.
- *Easier to make functional:* A lack of tiering means that only one transaction method must be developed, which then applies to all transactions.

Hybrid approaches are also possible. For example, if a form of self-custodied wallets were to be adopted, they could be limited to the lower tier with temporal restrictions on cumulative transfer amounts. It may be ideal to include these access tiers directly in the CBDC system's protocol, rather than allowing them to be easily adjusted through programmable functionality. This could help increase consumer trust that the CBDC system's rules will not be changed haphazardly, and

---

[25] The regulatory ramifications and scaffolding necessary for this approach are beyond the scope of this report.
[26] These equity concerns may be exacerbated when automated systems are used to make determinations about customer risk profiles.
[27] This could also be done as an amount over time. The tier could capture information about the sender and amount, but not retain information about the recipient. This might be facilitated more easily with zero-knowledge proofs.

this could also help protect the CBDC system from being abused during periods of high political volatility.

Identity Privacy: Known to Central Bank vs. Intermediary vs. No One

What aspects of identity are kept private/confidential, from whom, and under what circumstances?

Identity privacy concerns the extent to which individuals can keep various attributes related to their identity confidential from different parties, such as the central bank and intermediaries.

Identity-related information within transactions – such as payment addresses – could be known to the central bank, intermediaries, or no one.

Identity privacy is linked to access tiering, as identity privacy could vary between higher and lower tiers, allowing lower tiers to facilitate transactions while keeping more attributes confidential from specific actors.

This design choice applies for each piece of sensitive identity-related information. Hence, for each piece of sensitive identity-related information, the following design choice benefits and drawbacks should be considered:

Collected by central bank:

- *May harm human rights and democratic values:* Identity-related information known to the central bank for all or most transactions would represent a significant expansion of the central bank's access to customer information, which would raise significant privacy concerns. This centralized data must therefore not only have extensive cybersecurity protections, but also significant legal protections; for instance, it could be designed to be either legally or technologically (via use of encryption keys) challenging to view this data without judicial approval and oversight. Even if policies exist to prevent this harm at this time (e.g., law enforcement needing to seek a subpoena to get identity-related information from intermediaries), enabling this capacity could allow a future Administration to use the CBDC system to surveil the population in close detail, and cybersecurity compromise may still occur.
- *Has implications for privacy and AML/CFT compliance:* If "collected by central bank" was the design choice chosen for many pieces of sensitive identity-related information, it may place responsibility for AML/CFT compliance on the central bank, greatly increasing its responsibility. This would raise novel concerns about the central bank being subject to supervision for their compliance. This approach may provide users less privacy from the central bank and entities able to get information from it compared to the current system, but if combined with other design choices (e.g., access tiering), it may be possible to protect sensitive financial data from disclosure to most parties. If "collected by central bank" was the design choice chosen for many pieces of sensitive identity-related information, it may place a large burden on the central bank for AML/CFT Compliance; this may also raise novel concerns, since the central bank may need to be subject to supervision for compliance.
- *May not help expand equitable access to the financial system:* Consumer discomfort with central bank collection of identity-related information could discourage adoption and use

of the CBDC system, which may limit the potential for a CBDC system to expand equitable access to the financial system. Outside of the context of consumer use and adoption, decreased domestic and global use of the U.S. CBDC system may harm U.S. leadership in the global financial system and the global role of the dollar, and may also harm economic growth.

- *May introduce new risks:* This approach would be a significant departure from current models in the financial system and may introduce unforeseen risks.

Collected by intermediaries:

- *Has implications for privacy and AML/CFT compliance:* This approach is more similar to the current AML/CFT regulatory framework, where key reporting and recordkeeping obligations are generally imposed upon intermediaries, providing consistency with that approach. This approach has some key advantages, including many that are inverses of the drawbacks noted above. While this system may limit the amount of new risk introduced, it would also implicitly endorse an imperfect status quo.[28]

No one:

- *Has implications for privacy and AML/CFT compliance:* Keeping some pieces of identity-related information anonymous from the central bank and intermediaries could help enable cash-like privacy for those pieces of information. This may not be possible or sensible for some pieces of sensitive identity-related information. Given that a CBDC is not subject to the same physical limitations as cash, such an approach might make it harder to identify, trace, and disrupt money laundering and the financing of terrorism and for relevant financial institutions to comply with existing AML/CFT obligations. If "no one" was the design choice chosen for many pieces of sensitive identity-related information, it may functionally provide some level of anonymity, which may complicate intermediaries' compliance with AML/CFT obligations and may be out of line with global AML/CFT standards.[29]

A key question is what kind of information would be considered "identity-related information" for the purpose of this design choice. This design choice should be considered for all key pieces of identity-related information, and it is probably better for privacy and civil and human rights purposes for some pieces of information to be collected by intermediaries rather than the central bank. Additionally, not all intermediaries are the same, and criteria may need to be established to determine which types of intermediaries are allowed to collect which types of identity-related information.

Pseudonymous payment addresses may provide a privacy-enhancing feature, but they must be designed carefully so as not to be trivially linked back to individuals based on other information (e.g., transaction history). For example, it may be possible for intermediaries to hold or rotate pseudonymous keys on behalf of individuals such that external parties may not view or use them

---

[28] The United Nations Office on Drugs and Crime estimates that 2-5% of the global Gross Domestic Product is laundered every year, with the International Monetary Fund estimating that $1.6-4 trillion is laundered annually. See, Miller, R. (Apr. 2022). Overview of Correspondent Banking and "De-Risking" Issues. *Congressional Research Service*, 1.

[29] Whether this approach is legally possible in the context of current regulation and other obligations is outside of the scope of this report.

without sufficient authority. However, in general, vulnerabilities in pseudonymous methods could allow for deanonymization, and sufficiently motivated parties can often render pseudonymity ineffective. Still, for certain threat models, pseudonymity may provide a layer of privacy.

If identity-related information is known to some party, some entities likely need to verify the identity of an individual seeking to transact CBDC.[30] This could be done by intermediaries, establishing their own procedures and systems to verify identity, in line with regulatory obligations.

Crucially, it is worth noting that any privacy scheme will likely have some vulnerabilities, so even the "more private" choices will still not guarantee privacy. It is important to take a systems-level view of privacy, and not consider a system "private" just because information is being collected by intermediaries and not the central bank. Following best practices on privacy engineering – such as minimizing the amount of extraneous data collected in the first place – will likely be vital to minimizing the risk of unauthorized disclosures. Privacy-enhancing technologies could play a key role here, helping to ensure that privacy and AML/CFT objectives can be advanced in tandem.[31]

Remediation: On-ledger vs. Off-ledger

Does remediation (e.g., chargebacks, liens) get facilitated through core CBDC system functionality, or is it mandated through external governance processes? Who authorizes these actions, and what transparency is provided?

Remediation refers to the ability to fix mistakes made with the CBDC system, such as transactions that occurred accidentally or fraudulently.

We assume a CBDC system will be required to facilitate remediation, so that persons or entities can conduct activities such as recovering accounts, voiding transactions, ordering restitution, and conducting recovery and resolution activities. These functionalities could be primarily provided on-ledger, such that affordances for remediation are built into the CBDC system's protocol (e.g., transactions can be reversed until settlement is final, the central bank conducts remediation). Alternatively, these functionalities could be primarily provided off-ledger, so that remediation can be retroactively ordered (e.g., intermediaries settling disputes and conducting chargebacks equivalent to the incorrectly-transacted amount, courts mandating intermediaries to close accounts, etc.) and reflected by new offsetting transactions. For example, if Alice mistakenly pays Bob $100, an on-ledger remediation approach could simply void that transaction, leaving Alice and Bob the way they were before the transaction. Off-ledger remediation in this example would mean allowing the $100 transaction from Alice to Bob to settle but then, based on that off-ledger action, create a new transaction that pays $100 from Bob to Alice, again attempting to leave Alice and Bob where they were before the original transaction.

---

[30] If access tiering is used, this may only need to apply to individuals seeking to transact on higher tiers.

[31] The governments of the United States and the United Kingdom launched a set of innovation prize challenges in privacy-enhancing technologies to tackle financial crime, working with synthetic global transaction data created by SWIFT, the global provider of secure financial messaging services. See U.S. and U.K. Launch Innovation Prize Challenges in Privacy-Enhancing Technologies to Tackle Financial Crime and Public Health Emergencies. (Jul. 2022). *Office of Science and Technology Policy.*

The key questions here are *who* has the ability to authorize these actions, and what technical features would enable them to conduct these actions. Remediation would likely be easiest to implement in a permissioned and centralized CBDC system with intermediaries that have visibility onto a ledger and the ability to submit transactions. In this case, the primary challenge will likely lie in establishing the governance mechanism to determine the conditions that allow for remediation. Some of these procedures and principles can likely be drawn from an existing body of property, payment, contract, and banking law that spells out rules for settlement, finality, and liability. Additionally, remediation is also linked to offline transactions; if intermediaries are facilitating remediation in general, then P2P offline transactions may pose additional challenges. Finally, this also relates to access tiering, as higher tiers may want to use more of an on-ledger approach, in order to increase scrutiny for higher risk transactions.

Design choice benefits and drawbacks are described below:

On-ledger:

- *Provides additional financial protections:* Embedding remediation into the CBDC system's core architecture could provide additional guarantees for the ability to conduct remediation. For example, transactions could take a certain amount of time[32] to settle with finality, during which period parties may have the ability to seek remediation. While this approach would render some CBDC unusable for a period of time and may be a disincentive toward using the CBDC system, it would also ensure that the CBDC is not fully transferred until the validity of the transaction is verified.

- *May harm the improvement of payment systems:* Building remediation directly into the CBDC system's protocol would be challenging, as the central bank is not set up to conduct remediation in the same way private payment services can (e.g., chargebacks via a credit card company). This would raise governance concerns.

Off-ledger:

- *May improve payment systems by making the CBDC system faster to settle:* Providing remediation as a new offsetting transaction after the initial transaction has settled would likely allow for more speed for transaction settlement, as transactions could be made "final" more quickly.

- *May have implications for advancing financial inclusion and equity:* More off-ledger remediation would likely allow transfers to settle faster, meaning that Americans waiting for a payment would have access to that capital more quickly. This is particularly important for Americans living paycheck to paycheck, who may also be more vulnerable to predatory lending (e.g., payday loans). On the other hand, if intermediaries are tasked with facilitating remediation, then offline transactions without intermediaries would pose additional challenges for remediation.

[32] It may be possible to design a CBDC system where this amount of time could be specified per transaction. For example, a CBDC system might enable Alice to send money to her trusted friend Bob with no wait time, but if Alice wants to send money to untrusted merchant Charlie, then she could set a wait time of 3 days. This system would still support instant settlement, which is described as a core attribute of a CBDC system in The Future of Money and Payments. (Sep. 2022). *Department of the Treasury.*

★ ★ ★ ★ ★ ★

Security

Cryptography: Public-Key Cryptography vs. PKC with Zero-Knowledge Proofs vs. Other

What cryptographic techniques are used and for what purposes? How would quantum computers affect public-key cryptography systems and how would the system change post-quantum? How can the system be protected against abuses such as fraud and money laundering?

Cryptographic design choices are based upon the computationally intractable problems that invert and enable the secure storage, transmission, and usage of the information needed to operate a CBDC system.

A CBDC system could use public-key cryptography (PKC), in which users have a public key that represents a payment address to receive funds, and a private key that can authorize future payments to spend once funds are received, using digital signatures. A CBDC system could also use a PKC approach with zero-knowledge proofs (ZKPs) to help facilitate secrecy, where users send proof of knowledge and validity of particular data (e.g., transaction details such as recipients and amount), rather than sending the data. There are several other cryptographic methods (e.g., secure multiparty computation, private set intersection, homomorphic encryption) that could also enhance the security of the CBDC system, and these methods should also be considered if developing a CBDC system.

Cryptography design choices are vital to security as quantum computing becomes feasible at scale, as discussed below. The cryptography scheme chosen would also impact how privacy, fungibility, and programmability are designed as well.

Design choice benefits and drawbacks are described below:

PKC:

- *Likely to be more efficient:* PKC is an extensively tested and used cryptographic method, and there is familiarity with this approach among developers. It would be relatively easy to roll out a CBDC system with a functional and efficient PKC-based system using longstanding and well-tested code libraries, which would advance the policy objective of improving payment systems. As quantum-resistant cryptography protocols (discussed below) are standardized, libraries are tested and deployed, and adoption across government and industry become the norm, they can be integrated into the CBDC system.

PKC with ZKPs:

- *Provides increased privacy for sensitive financial data:* ZKPs can be used to provide enhanced privacy safeguards by verifying if attributes of a transaction are valid without revealing anything about the underlying data itself. By not needing to share this underlying data during transactions, it is generally easier to keep that data private.
- *May introduce complexities for AML/CFT compliance:* ZKPs may prevent discoverability information and the enforcement of AML/CFT regulations in general, unless combined with a scheme to facilitate compliance. This may increase the complexity of enforcing AML/CFT regulations.

- *Likely more secure:* ZKPs limit the amount of potentially-revealing information sent across networks, reducing potential security vulnerabilities. The use of ZKPs may advance the policy priority of improving payment systems. Furthermore, some ZKP approaches are quantum resistant while others are not, and choosing an approach will depend on the standardization process.
- *Possibly not as sustainable:* Executing ZKPs requires more computation than PKC by itself, especially in order to operate approaches that remain viable when cryptanalytically relevant quantum computers are developed. There are methods to improve the performance of ZKPs, so there may be reasonable mitigations of this concern. If this approach is chosen, it will be important that the hardware that generates ZKPs is sufficiently decentralized or protected (including from distributed denial-of-service attacks) in order to not invite targeted attacks.

The security of PKC is based on the inefficacy of certain computations using known algorithms; however, quantum computers are theoretically able to perform some of these computations quickly. Thus, many PKC protocols will be insecure when quantum computing becomes feasible at scale. The PKC systems that are resistant to attacks from such future "cryptanalytically-relevant quantum computers" are referred to as "quantum-resistant cryptography." National Security Memorandum 10 (NSM-10)[33] prioritizes the transition to quantum-resistant cryptography and sets the policy that agencies should only transition to quantum-resistant cryptography once the first set of NIST standards for quantum-resistant cryptography is complete (expected in 2024) and implemented in commercial products.

If a CBDC system were to be launched in the near future, a traditional non-quantum-resistant PKC system could be developed, with the concern that older transactions may be vulnerable to tampering from future cryptanalytically-relevant quantum computers. Alternatively, a longer-term strategy would be to develop a CBDC system with a quantum-resistant PKC system after standardization has been completed. Regardless of the cryptographic approach taken, consistent with NSM-10, the CBDC system should maintain "cryptographic agility" in that the system should allow for seamless updates for future cryptographic standards. Given this, further research and analysis should be conducted on possible challenges in upgrading any non-quantum-resistant cryptography protocols to quantum-resistant methods at a later date.

There is also policy[34] concerning the government's ability to retain and manage encrypted records. A relatively complex change in policies and regulations would take significant effort, and should be careful to align with recent Executive Orders and memoranda[35] regarding the Federal Government's posture toward cybersecurity.

---

[33] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. (2022). *The White House*.
[34] See, e.g., Bulletin 2007-02, Guidance concerning the use of Enterprise Rights Management (ERM) and other encryption-related software on Federal records. (Apr. 2007). *National Archives and Records Administration*.
[35] See, e.g., Executive Order 14028: Improving the Nation's Cybersecurity. (May 2021). *Federal Register*; M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. (Jan. 2022). *Office of Management and Budget.*

★ ★ ★ ★ ★ ★

Secure Hardware: More Hardware-Based vs. More Software-Based

Is there support for secure hardware interfaces?

Secure hardware refers to computing equipment (i.e., hardware) that is designed to protect data and computation, especially from other processes running on that equipment.

A CBDC system could base a large part of its security model on secure hardware-based approaches. This could include the use of a separate module (i.e., physically separated from other hardware) that isolates specific data and/or computations. This could also include the use of a trusted execution environment, where there are limitations placed on the code that can be executed on the equipment. Such a system could connect to a user's smartphone, could be made as a specialized part of the user's cellphone, or could function as a standalone device. A CBDC system could also run with limited or no secure hardware-based approaches, prioritizing software-based approaches to security.

Secure hardware is likely to be important for enabling offline transactions, in order to combat fraud and abuse (e.g., counterfeiting money) when transacting parties are offline.

Design choice benefits and drawbacks are described below:

More hardware-based:

- *Likely more secure:* This approach can better secure cryptographic keys and certify code performance, helping to provide higher levels of security.
- *May promote AML/CFT compliance and limit concerns with privacy of sensitive financial data:* Secure hardware could possibly be the place where encrypted transactions take place, and much of the information necessary for compliance with AML/CFT regulations may reside. This can provide additional mechanisms for limiting illicit activity while minimizing risks to the privacy of individuals, but would put additional pressure on the security of that hardware.
- *May harm the expansion of equitable access to the financial system:* Consumers may need to purchase a piece of hardware that would enable them to participate in the network, which would create a barrier to equitable access to the financial system. However, if there was widespread access to secure hardware-based approaches (e.g., if most cellphones had the appropriate capability), then secure hardware could possibly execute trusted code that ensures CBDC cannot be double-spent even without access to a network; this would help facilitate offline transactions, which may expand equitable access to the financial system.
- *Introduces new risks to security and sensitive financial data:* Secure hardware also sometimes still shares hardware with other parts of the system, allowing for data to leak onto insecure hardware. Without adequate protections, secure hardware may also be manipulated by those with physical access to the system. This could be counter to the policy objectives of having a secure CBDC system and keeping sensitive financial data private.
- *Exacerbates systemic risk:* It is vital that secure hardware can be trusted to be secure, and appropriate protections can be incorporated. However, secure hardware is only developed by a few key players, and there would be large incentives for those throughout the supply

chain (including end users) to exploit the system, as the reward could potentially be the ability to mint unlimited CBDC. This would also add another potential vulnerability for the CBDC system by increasing reliance on supply chain security beyond security through software only (which also has risks for supply chain attacks).

More software-based:

- *Likely provides more flexibility:* Software-based approaches to wallets or other cryptographic primitives allow a variety of platforms and languages to adopt implementations which can improve security, and interoperability of a protocol.
- *Supports expansion of equitable access to the financial system:* By providing lower barriers to entry for consumers who do not need secure hardware, it may encourage adoption from consumers not having to acquire hardware-based technologies.

If secure hardware is part of a CBDC system design, it should be layered on top of other security measures, and not be used as a standalone guarantor of CBDC system integrity.

Transactions

Signatures: No-signature vs. Single-signature vs. Multi-signature Signing

Do transactions use digital signatures, and if so, are transactions single-signed or multiple-signed? How do you protect threshold keys/signatures? What does signing confer to the transaction? What signing algorithm is the right one?

A CBDC system could require zero, one, or multiple digital signatures to execute a valid transaction.

The CBDC system could use a no-signature approach, where transactions are not signed with any verification of identity; this would rely on a custodian to provide a user account and facilitate access to funds. The CBDC system could use a single-signature approach, where only the payer is needed to authorize the transaction. In this process, a single individual—typically the payer in possession of a private key to a digital wallet—can execute a transfer of funds to another wallet. The CBDC system could also use a multi-signature approach, where multiple signatures are needed in order to execute the transaction. In this approach, multiple private keys – possibly held by separate actors[36] – must be used in a transaction before the CBDC is transferred. These options are not mutually exclusive; all three could be supported by the CBDC system in different circumstances. In a multi-signature approach, there will also be additional design choices concerning who holds the appropriate keys, and whether a threshold approach is to be adopted (i.e., requiring some subset of possible signatures to be given, rather than requiring all of them).

This design choice could be linked to access tiering, where higher tiers use multiple-signature or single-signature approaches, and lower tiers use single-signature or no-signature approaches. This design choice is closely linked to the cryptography and quantum-proofing design choices. This design choice is also linked to transaction privacy; for example, if the recipient is not one of

[36] The transaction recipient may want to hold one of these keys. Should a CBDC system grow to interoperate with digital assets from many sources, unsolicited assets might be sent to accounts. This could introduce off-ledger attack vectors (e.g., compromised privacy, phishing).

the signers of a transaction, a bad actor might try to send unsolicited assets to a target in order to glean information about them.

Design choice benefits and drawbacks are described below:

No-signature:

- *Likely less secure than other options:* If transactions do not require any direct authentication by the owner, there would be fewer safeguards to prevent the unauthorized transfer of CBDC.
- *May limit improvements to payment systems:* This approach may make it harder to introduce transaction programmability into the CBDC system, as signatures are a method to provide proof of ownership.

Single-signature:

- *Possibly less secure than multiple-signature approach:* This would be more secure than no-signature. However, because transactions only require one private key, there is a single point of failure. If a less intermediated transport layer is used, or if a private key is lost or stolen, that could lead to the loss of CBDC held in the associated wallet; similar to cash, once the asset has been lost or stolen, regaining possession can be difficult. This may not be as much of a problem with a multi-signature threshold approach, because that approach allows for "backup" keys to exist if some keys are lost or stolen. Fraud detection and prevention measures may also mitigate some of these problems.
- *Possibly more functional and efficient:* This approach is likely simple to understand and implement. Single-signature (and its analogs) are the default in the retail commerce environment (e.g., credit and debit card transactions, transferring money from individual bank accounts) and among many private sector-administered digital assets.

Multiple-signature:

- *Likely more secure than other options:* Multi-signature offers security enhancements over single-signature. In P2P transactions, the payer might hold two private keys on different devices that are needed to execute the transaction, providing additional security (similar to two-factor authentication). A threshold approach allows for, say, two of three possible signatures to be present; for example, the payer and the intermediary can each hold a key, and a third key is stored with a trusted third party in case either of the other keys is compromised. This could advance the policy objective of improving payment systems.
- *Possibly less functional and efficient:* Multi-signature requires more steps to complete a transaction, possibly adding roadblocks to easy use of CBDC. For example, if multi-signature is used for low-value transactions, the safety features may not outweigh the poorer customer experience (e.g., requiring two-factor authentication at every point-of-sale). Multi-signature would also require more effort to implement than single-signature. Additionally, more research will have to be done to determine what offline capabilities can be achieved with a multi-signature approach.
- *Possibly better for ensuring appropriate interoperability:* Multi-signature can provide a method to enable cross-border, cross-currency exchanges. In this model, one of the required signatures is from an intermediary that holds the transfer in escrow until all

transfer conditions are met. The multi-signature serves not only as an additional layer of security, but also as a facilitator of the transaction.

Transaction Privacy: More Private vs. More Observable Transactions vs. Layering

What level of transaction privacy is supported? What aspects of transactions are private, and from whom? Are amounts, destinations, and smart contracts private from the central bank? Can transactions be chained?

Transaction privacy concerns which entities are able to access which characteristics of transactions, including data privacy (e.g., account balances, location of participants, information about goods) and program privacy (e.g., source code and inputs used for a smart contract transaction).

A CBDC system could be more private, limiting access to sensitive data for legal reasons only (e.g., for compliance with AML/CFT regulations, to competent authorities for AML/CFT regulation and supervision). A CBDC system could be more observable, such as by maintaining a public record of all transactions associated with pseudonyms (e.g., the way that many private sector-administered digital assets work). A CBDC system could be a hybrid of these options, providing a public record of some characteristics and only allowing limited discoverability of others. A CBDC system could also support a layering approach, where intermediaries capture information about transactions or accounts that meet some established set of concerning characteristics, and that information could be retained for some fixed period of time during which proper legal authorities could petition to review that information in accordance with legal standards.

This design choice could be enabled in a variety of ways that intersect with other design choices. For example, if the cryptography design choice includes ZKPs, it may be possible to use ZKPs to facilitate transactions that require fewer entities to view sensitive data. Or, if the CBDC system has access tiering, design choices could be chosen for the lower tiers that provide greater transaction privacy. Additionally, if the CBDC system has intermediaries, these intermediaries could facilitate a layering approach.

Design choice benefits and drawbacks are described below:

More private:

- *Better protects the privacy of sensitive financial data:* This approach would limit the data and program information that is accessible to transacting parties and third parties. It also may increase public trust and financial inclusion in a CBDC system.
- *Might introduce challenges for promoting compliance with AML/CFT requirements:* Some methods for enabling transaction privacy (e.g., some ZKP-based approaches) have limitations in how much information would be saved for future discoverability. If this approach is chosen, thought should be given to how sufficient transaction information could be preserved and remain accessible only for a limited set of verified use cases (e.g., competent authorities or financial institutions for AML investigations or to comply with AML/CFT obligations). Limitations on data preservation or access could also have implications for existing recordkeeping obligations of relevant financial institutions.

More observable:

- *Promotes AML/CFT compliance:* This approach would increase the amount of information readily available for AML/CFT compliance purposes, albeit in pseudonymous form, to competent authorities and could support relevant financial institutions compliance with existing AML/CFT obligations. Competent authorities and relevant financial institutions would still need to be able to access and share, when appropriate, detailed transaction information to facilitate compliance with AML/CFT obligations.
- *Might reduce privacy of sensitive financial data:* Even if pseudonymous identities are used for transactions, vulnerabilities in pseudonymous methods could lead to deanonymization in the future. This could potentially reduce public trust and financial inclusion if deanonymization incurs privacy harms to innocent actors.
- *May help support economic activity:* Some public information about characteristics of transactions may be useful for understanding consumer preferences and promoting private sector innovation.

Layering:

- *Aims to protect privacy of sensitive financial data and promote AML/CFT compliance, via intermediaries:* In this approach, transaction information would be mostly unavailable to the general public, while intermediaries or programmatic rules would get access to transaction information necessary to support compliance with AML/CFT obligations, and data would be available to competent authorities. For example, AML/CFT compliance practices could be standardized at the CBDC system level (e.g., along the rails), which could increase the efficiency and effectiveness of AML/CFT processes, but may place a large burden on the CBDC system operator to be responsible for a large part of AML/CFT compliance. In addition, a one-size-fits-all AML/CFT program may not be aligned with the risk-based approach promoted by international standards. However, if intermediaries play a role in such a process, care would likely be required to ensure that intermediaries do not sell, transfer, or lose this sensitive financial data in a manner that unreasonably breaches privacy.
- *Possibly less secure:* Because intermediaries would need to access transaction information, this approach would have an access point that could be compromised, either directly (e.g., since the information is being captured somewhere) or indirectly (e.g., unauthorized access to intermediaries' databases).

Offline Transactions: Online Only vs. Both Online and Offline

How can offline capabilities be provided, such that some transactions can occur without connectivity to the broader CBDC system? Would tokens or debit cards tied to the CBDC operate as a tool to permit a higher level of privacy for some transactions?

Offline transactions refer to exchanges of CBDC that occur when the exchanging parties can communicate with each other, but they cannot communicate with the transaction processor.

One design choice is to forgo offline transactions, instead requiring some form of connectivity in order to complete a transaction of CBDC. Alternatively, offline transactions could be provided,

★ ★ ★ ★ ★ ★

for example, by using trusted execution environments for individuals to verify to each other that they have the CBDC they claim to have, and to facilitate the transaction securely.

This option is closely linked to the Secure Hardware design choice, as that might provide the guarantees needed to facilitate some transactions offline without the broader CBDC system's features and safeguards. It is also linked to the governance design choices, as there could be future punishments and remediation for offline transactions that were incorrect or malicious. Finally, the data model and fungibility of CBDC would also have an impact on the privacy implications of offline transactions.

Design choice benefits and drawbacks are described below:

Online only:

- *Could be more secure:* An online-only model would not introduce vulnerabilities from offline capabilities, such as flaws in a trusted execution environment that functionally allows individuals to create CBDC out of thin air. However, there are reasons that offline capability could also boost the CBDC system's security, as discussed below.
- *May harm financial inclusion and equity:* The requirement to have connectivity to the CBDC system would disproportionately disadvantage underserved communities that lack access to reliable and high-speed Internet. Additionally, the inability to use CBDC like physical cash may not be enticing to communities that have been particularly disenchanted with the traditional banking and financial systems.

Both online and offline:

- *Has implications for security and AML/CFT controls:* An offline-capable system would be more resilient if the network or intermediaries were rendered dysfunctional at any point. This resiliency would be important during potential attacks or failures, allowing CBDC to be exchanged while the system comes back online. However, if someone breaks the mechanism (e.g., secure hardware) that ensures CBDC cannot be spent twice, then it could be possible to counterfeit CBDC. In addition, offline transactions could presumably take place without being subject to real-time transaction monitoring or investigative tracing, which could complicate compliance with AML/CFT obligations.
- *Could be more private:* An offline system, based on how it is implemented, could offer more cash-like privacy in offline transactions. For example, if transactions are only recorded when they intersect with intermediaries, then CBDC could be exchanged between many hands offline before being re-tracked in the ledger.

There is a spectrum of options between fully online-only and fully offline-compatible. Limitations could also be placed on the amounts, frequency, or types of transactions that could occur offline. For example, third-party network transactions have a reporting requirement for transactions exceeding $600.[37] Furthermore, cash transactions in trade and business over $10,000 are required to be reported to the Internal Revenue Service (IRS) under current law; an analogous norm in offline CBDC transfers might mean that more than $10,000 cannot be transferred offline. However, P2P cash transactions not considered in the context of trade or business do not have this reporting requirement.

[37] Instructions for Form 1099-K. (Jan. 2022). *Internal Revenue Service.*

★ ★ ★ ★ ★ ★

Transaction Programmability: Supported vs. Not Supported

Are transaction-level application programming interfaces (APIs) supported? If so, can they be created in a permission-less manner, only by the CBDC authority, or somewhere in between? Who defines the API? Is there a governance process to determine API requirements?

Transaction programmability refers to whether, broadly, third-party developers are able to code rules into a CBDC system, such that those rules are executed when the predefined conditions are met.[38] This does not refer to the ability to uniquely identify specific CBDC units and place restrictions on their use; for a discussion of that design choice, refer to the fungibility design choice.

Transaction programmability can be supported, such that the CBDC system has smart contract programming capabilities that developers can use to develop programs to run on the CBDC system. Alternatively, transaction programmability could not be supported, so that most or all CBDC cannot be programmed to function in more specific ways. Hybrid options are also possible; for example, programmability could be supported for broad use cases (e.g., regulatory and monetary policy) and execution of some smart contracts could be extended to intermediaries, but direct programming against a ledger could be unsupported. Programmability could also be allowed for applications that use data from the CBDC system without having direct access to CBDC system infrastructure.

Trustworthy programmability is highly entangled with the cryptographic primitives that are chosen to enable security and trust. Because programmability can also have tradeoffs with privacy, the design choices about identity privacy and transaction privacy are also closely linked to programmability. The data model chosen is relevant here; for example, an unspent transaction outputs (UTXO) model, as described below, may make it harder to conduct auctions using smart contracts.[39] Finally, questions of governance are also important here – if transaction programmability is supported on a centralized system, it will likely be important to ensure that the central authority or authorities are verifiably committed to following and executing the rules.

Design choice benefits and drawbacks are described below:

Transaction programmability supported:

- *Likely supports payments innovation:* Allowing entities or developers to build in their own programs could enable new forms of payment technologies, similar to the ecosystem of innovation seen with smart contracts. This may not be fully realized if programmability is only partly supported (e.g., if the CBDC system is deployed with programmed rules established, but does not support third parties to build in their own programs).
- *May harm the privacy of sensitive financial data:* Programmability is often based on verifying that a certain set of conditions is true, which then initiates the execution of the smart contract. In order to verify that set of conditions, the smart contract needs access to

---

[38] Transaction programmability is often implemented through transaction-level APIs.
[39] Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., ... & Zhang, F. (Aug. 2020). Design choices for central bank digital currency: Policy and technical considerations (No. w27634). *National Bureau of Economic Research*, 51-2.

certain sets of data. This can lead to privacy risks to sensitive financial data, although various privacy-enhancing approaches (e.g., ZKPs) could help mitigate these risks.

- *May make the CBDC system less secure:* In the private sector use of smart contracts, there have been a number of bugs, mistakes, and hacks that have caused smart contracts to behave in unexpected or malicious ways. While this can be partly mitigated via controlled libraries for smart contract programming languages, upgradable code, and code verification, there will likely still remain key security risks with programmable CBDC.
- *May worsen systemic risk:* A network of smart contracts – and the potentially high interdependency between them – could create unexpected feedback loops, where the whole system triggering rules in parallel could collectively create systemic issues for the financial system.
- *May reduce financial protections for consumers:* Programmability might introduce challenges for stopping code execution in response to bankruptcy, recovery and resolution, or other court prescribed activities. The smart code execution is driven by standard external inputs and may have additional challenges for adjusting or accommodating "extraordinary" events such as bankruptcy or receivership, which could lead to violations of laws or regulations.

Transaction programmability not supported:

- The benefits and drawbacks of not implementing transaction programmability are the inverse of implementing it.

Data

Data Model: Unspent Transaction Outputs vs. Account Balances

What model is used to maintain records: Unspent Transaction Outputs (UTXOs) or Account Balances?

The data model refers to the method of keeping records about ownership of CBDC.

The CBDC system could use the UTXO data model, where the transfer of specific CBDC units is tracked (e.g., like coins being transferred between individuals). Alternatively, the CBDC system could use the Account Balances model, where it tracks the aggregate amounts of CBDC held in different places. The system could also use a hybrid of these approaches.

The data model is closely linked to many other design choices, including those involving the transport layer, identity privacy, transaction privacy, and offline capabilities.

Design choice benefits and drawbacks are described below:

Unspent Transaction Outputs (UTXOs)

- *May enable more privacy for sensitive financial data:* It is a bit easier to do privacy-preserving cryptography with this model. Individual UTXOs can be linked to unique keys, so that they are not all easily tied back to one individual's account. Meanwhile, with the Account Balances model, many people will likely use one account for their transactions, which means all transactions could be linked back to a single person more easily.

- *Likely easier to expand access for all Americans:* As a CBDC system scales, the UTXO data model is likely to make it easier to facilitate more transactions (e.g., transactions can happen in parallel without needing to sequence them to avoid double-spending). With the Account Balances model, transactions require editing a global state about account balances, and these edits likely have to happen sequentially so that money isn't double-spent; this might provide a challenge to scaling the CBDC system.

Account Balances:

- *May support certain types of payments innovation:* The Account Balances model could make it easier to reference outside states via oracles or smart contracts. Global account states would make it easier to incorporate transaction programmability. It is harder for a UTXO data model to reference the full global state of the CBDC system, which is likely a key feature for achieving extensive programmability (e.g., enabling the checking of other users' balances).

There is also a spectrum of designs between the UTXO and Account Balances data models. For example, some projects have used a hybrid approach that features a "collection of object states" as its data model.

Ledger History: None vs. Centralized vs. Distributed

Does the CBDC maintain a history of issuances and transactions, and what information is stored (e.g., value, issuer) and for how long? If a decentralized system is used, do nodes contain all or part of the transaction history (e.g., full versus light nodes) or partition the storage workload (e.g., sharding[40])?

Ledger history refers to the maintenance of a history of issuances and transactions in a CBDC system.

A CBDC system could not store ledger history; for example, a system of smart cards (e.g., mobile phone SIM cards) may not need a ledger. A CBDC system could store ledger history on a more centralized ledger, with the central bank providing the core infrastructure and with trusted intermediaries operating key features (e.g., adding transactions to the ledger). Alternatively, a CBDC system could store ledger history in a more decentralized manner, with trusted intermediaries or individuals being able to operate their own nodes to facilitate part of the CBDC system.

The specific questions about which information is recorded are addressed in previous sections on identity privacy, transaction privacy, remediation, and data. The choices made in those sections are highly relevant here; because different pieces of historical data could be accessed together, the risks to privacy and AML/CFT controls would be shaped by the specific pieces of information being stored. Additionally, remediation will likely be more challenging if a distributed ledger is chosen such that no trusted entities have unilateral write access to the ledger.

---

[40] Sharding refers to taking natural subsets of data in a database, often to help improve performance. See, e.g., Amiri, M. J., Agrawal, D., & El Abbadi, A. (Jul. 2019). On sharding permissioned blockchains. *2019 IEEE International Conference on Blockchain,* 282-5.

Design choice benefits and drawbacks are described below:

None:

- *May improve security and privacy of sensitive financial data:* A key way to protect privacy and security is to not capture information.[41] By not maintaining a ledger, there would be fewer places where sensitive financial data could be accessed.
- *May introduce risks for consumers, investors, and businesses:* It may be impossible to offer all the features and requirements of a central bank asset without any ledger. A lack of a ledger, even one that only temporarily records transactions, could make it harder to resolve critical failures and conduct remediation.
- *May have implications for expanding equitable access to the financial system:* A lack of any historical ledger directly tied into the core CBDC system could foster widespread distrust in the CBDC system, especially during its early adoption phase when there may be doubts as to whether the system works properly. Alternatively, because privacy concerns are one of the most-cited reasons for not having a bank account among unbanked households,[42] the lack of a ledger may help increase adoption of a CBDC among the unbanked and underbanked.

Centralized ledger:

- *Likely more functional and efficient:* A centralized ledger would likely be easier to build and operate, especially at the scale needed for a U.S. CBDC system.
- *May have implications for payments innovation and consumer protection:* Since a centralized ledger approach is similar to how electronic money transactions are currently tracked, this approach is more familiar and better tested. However, this familiarity may limit full consideration given to incorporating the latest features in areas like encryption and programmability, possibly limiting innovation, but also possibly better protecting consumers, investors, and businesses.

Distributed ledger*:*

- *May be less functional and efficient:* Further research would have to be performed to understand if distributed ledgers can support transaction rates and latency likely required by a U.S. CBDC system. This could build on the considerable energy that has been invested into research on additional technologies to enhance underlying distributed ledgers to provide them with the ability to transact (e.g., something similar to a "layer two" technology[43]). Additionally, many of distributed ledger technology's features—immutability, cryptography, programmability and smart contracts—can also be realized through a centralized ledger approach, if desired.

---

[41] See, e.g., Fanti, G., Kostiainen, K., Howlett, W., Lipsky, J., Moehr, O., Schnapper-Casteras, J., & Wolff, J. (Jun. 2022). Missing Key: The challenge of cybersecurity and central bank digital currency. *The Atlantic Council*. ("CBDCs with stronger privacy rules may generate and store less sensitive data in the first place. In turn, potential attackers have a smaller incentive to infiltrate the system.")
[42] How America Banks: Household Use of Banking and Financial Services, 2019 FDIC Survey. (Oct. 2020). *Federal Deposit Insurance Corporation*.
[43] See, e.g., Martinazzi, S., & Flori, A. (2020). The evolving topology of the Lightning Network: Centralization, efficiency, robustness, synchronization, and anonymity. *Plos one, 15*(1), e0225966.

- *May harm security and consumer protection:* When coupled with permissionless governance, distributed ledgers create new potential ways of attacking the system (e.g., 51% attacks). Some of the additional functionality that such systems have enabled in private sector-administered digital assets (e.g., transaction programmability) has been a prime target for attacks.
- *May promote payments innovation:* Incorporating a technology with significant industry research and development could have downstream effects on innovation in the CBDC system and the government as a whole. For example, assuming that distributed ledger technology has some role within the "ecosystem" of CBDC ledgers, it may enable increased innovation in programmable money and smart contracts.
- *May not be sustainable:* Some types of consensus mechanisms used to maintain synchronicity between distributed ledgers raise environmental concerns. If one of these consensus mechanisms were used in a CBDC system with a distributed ledger, this design choice may not align with the policy objective that a CBDC system should be sustainable.

The length of historical storage is also an important question. Ledger history would likely be required to be recorded for long enough to facilitate AML/CFT compliance and to ensure that offline transactions can be verified against the history of previous transactions. However, data would likely not be required to be stored indefinitely in order to enable any core parts of a CBDC system's functionality; for security and privacy purposes, it would make sense to store ledger history for as little time as required to fulfill policy objectives.

Adjustments

A CBDC system could facilitate a number of financial design choices, such as special purpose CBDC, holding limits, fees, and interest whose merit is outside the scope of this report.[44] This section focuses on analyzing the associated technical design choices that would enable those financial design choices.

Fungibility: Fungible vs. Non-Fungible Units

Can the CBDC system support non-fungible units?

A non-fungible unit is a discrete unit of CBDC that has a unique identifier (e.g., a serial code). For example, even though physical dollar bills are often considered fungible, under this definition, a physical dollar bill is a non-fungible object. Each physical dollar bill is a unique physical object that has a serial number, and can be held, destroyed, or exchanged for another unique physical dollar.

A CBDC system could support fungible units that are not unique, and thus function identically to each other. A CBDC system could also support non-fungible units, and thus can enable different

[44] For further consideration of some of these design choices, see The Future of Money and Payments. (Sep. 2022). *Department of the Treasury.*

★ ★ ★ ★ ★ ★

processes for their use.[45] A CBDC system could also use both approaches. In a corollary to cash as a unit of payment, cash can be serialized. If something is wrong, a participant can take it out of circulation and reprint that note with the same serial number with an annotation of reprint.

Fungibility will likely overlap with choices made about storage and the transaction model. Fungibility could also impact how CBDC is packaged for offline transactions, and how the CBDC system interoperates with other payment systems.

Design choice benefits and drawbacks are described below:

Fungible units:

- *May promote privacy of sensitive financial data:* Fungible units are not marked to be uniquely traceable down to specific CBDC units, potentially increasing the privacy afforded by the CBDC system. This could advance the policy objective of aligning with democratic values.
- *May promote increased interoperability:* Fungible units could be subdivided and exchanged with each other, as the uniqueness of any specific CBDC unit would not need to be preserved. This could advance the policy objective of ensuring the CBDC system should be appropriately interoperable.

Non-fungible units:

- *Likely helpful for economic activity:* Non-fungible units could enable the limiting of certain CBDC to be used toward more economically-beneficial uses, especially during times of recession. This could be a helpful tool for regulatory and monetary policy.
- *May promote national security, possibly at the risk of human rights and aligning with democratic values:* Specific CBDC units could be marked as “tainted” if they are used in illicit activity. Regulated entities could be prohibited from engaging with this tainted CBDC, which would reduce the market value of those CBDC units, thus making it less profitable to use the CBDC system for illicit activity. This could advance the policy objective of national security, although misuse of this power (e.g., to target political adversaries) could be counter to the policy objectives of protecting human rights and aligning with democratic values.[46]
- *Could affect human rights and democratic values:* Because non-fungible CBDC could enable some CBDC units to be treated differently than other CBDC units, this design choice could be used to restrict how individuals use CBDC. For example, some CBDC could only be able to be spent on travel or, in a more sinister example, could be limited to disallow certain lawful transactions, such as not allowing spending for religious causes. This may also limit adoption of the CBDC, which could be counter to the objectives of improving payment systems and U.S. leadership in the global financial system. On the other hand, programmability could also be used to prevent currency from being used in various ways that harm consumers or violate human rights.

---

[45] There are further technical specifications that could limit the actors that could treat different units of CBDC differently from each other. For example, CBDC could be serialized with numbers that are encrypted, such that only certain intermediaries are able to decrypt those numbers.

[46] This is not the only way to control usage of CBDC. Assets or accounts might be restricted from using CBDC in other ways, based on other design choices made for the CBDC system.

★ ★ ★ ★ ★ ★

It is also possible to operate a hybrid version, where some units are fungible and some units are non-fungible. For example, standard CBDC could be fungible while there could be some CBDC that is non-fungible (e.g., benefit disbursements for the Supplemental Nutrition Assistance Program, which could be non-fungible so it could be limited to being spent on SNAP-eligible purchases).

Holding Limits: Limits or No Limits

Are there limits on how much CBDC any particular entity can hold?

Holding limits refer to limits on how much CBDC any particular person or entity can hold.

The CBDC system could impose limits on how much any particular entity can hold in CBDC. Alternatively, the CBDC system could not have such limits. The CBDC system could likely enable this functionality if there are mechanisms, such as Consumer Due Diligence, requirements or costs, to prevent entities from creating multiple accounts.

This design choice is closely related to identity privacy, for the reason mentioned above. This design choice may also be linked to access tiering, as it is possible that holding limits could be imposed for some tiers and not for others.

Design choice benefits and drawbacks are described below:

Limits:

- *May help mitigate risks for consumers, investors, and businesses:* Limits would cap the damage that consumers, investors, and businesses might incur via the CBDC system.
- *May introduce risks for keeping sensitive financial data private:* Limits might be implemented in a way that requires intermediaries monitoring the balance of individual accounts, or by linking balances across accounts together; these approaches might harm privacy. However, more privacy-preserving approaches are possible; for example, ZKPs and secure hardware-based approaches could prevent transactions (including P2P ones) from completing if the recipient's balance would exceed a certain threshold.

No limits:

- *May limit benefits to economic activity:* No limits may be a benefit for businesses that hold or exchange large volumes of CBDC at a time. This might make it easier to use the CBDC system for economic activity. Though economic considerations are out of scope for this report, it is worth noting that there are important economic considerations here. For example, if a substantial portion of deposits are held in the CBDC system, this might reduce loan creation by financial intermediaries due to lower deposit volumes. Additionally, without appropriate safeguards, this could increase the likelihood, severity, and speed of bank runs, as a CBDC system could allow users to quickly withdraw deposits from a bank if they believe it might fail (even with the existence of deposit insurance).[47, 48]

---

[47] A recent paper finds that bank runs can be more frequent with a CBDC system. Williamson, S. D. (2021). Central bank digital currency and flight to safety. *Journal of Economic Dynamics and Control*, 104146.

[48] The European Central Bank simulated systemic runs on banks based on the recent experience by Greece and Cyprus; they found that no limit accounts can allow for faster and larger withdrawals. Adalid, R., Álvarez-Blázquez,

★ ★ ★ ★ ★ ★

Adjustments on Transactions: Fees vs. No Fees

Can the CBDC system support fees?

Adjustments on transactions refer to the costs imposed by the Federal Reserve, intermediaries, or other third parties for the use of the CBDC system.

The Federal Reserve or the appropriate entity could administer fees for using the CBDC system, or fees could be allowed to be charged by intermediaries as part of transactions in an intermediated system. Alternatively, the system could be built without the concept of fees and any such charges could be managed as separate transactions.

This design choice intersects with many other design choices. For example, the transport layer likely matters a lot; if intermediaries are involved, then fees might be levied on intermediaries rather than consumers directly. In a less intermediated system, fees may help solve efficiency and cybersecurity concerns that might otherwise be handled by intermediaries. Fees may also intersect with access tiering, where lower tiers may not involve fees, while higher tiers could involve fees.

Design choice benefits and drawbacks are described below:

Fees:

- *May improve efficiency:* Fees can help the CBDC system prioritize transactions. This is likely less of a concern in an intermediated system where intermediaries can institute their own processes to prioritize transactions.
- *May improve security:* Fees can also provide a disincentive for CBDC system users to spam the network with a large number of transactions. This is likely less of a concern in an intermediated system where intermediaries can institute their own processes to prevent spamming.
- *May improve functionality:* Fees can help recuperate some of the costs of operating the CBDC system. This would help the CBDC system function efficiently relative to the costs to operate. This may also be a requirement based on existing law and regulation.

No fees:

- *May help improve efficiency and extensibility:* Fees add complexity to a CBDC system. The lack of fees would allow for a more straightforward CBDC system, which may be more efficient and extensible.
- *May not help improve payment systems:* Fees would create an additional barrier to the use of the CBDC system, which may prevent all Americans from using the CBDC system. Even if fees were assessed on intermediaries, some of those costs would likely be passed on to consumers.

If fees are assessed, there would also be choices about how they are administered (e.g., a percentage of each transaction, a fixed fee to access the CBDC system for a certain period of time).

Adalid, R., Álvarez-Blázquez, Á., Assenmacher, K., Burlon, L., Dimou, M., López-Quiles, C., ... & Veghazy, A. V. (2022). Central bank digital currency and bank intermediation. *ECB Occasional Paper*, (2022/293), 36-41.

★ ★ ★ ★ ★ ★

Adjustments on Balances: Adjustable vs. Not Adjustable

Can the CBDC system support CBDC that is interest-bearing?

Adjustments on balances refers to whether account balances can be adjusted to facilitate features such as interest-bearing CBDCs or fees based on accounts.

Accounts could be adjustable outside of fund transfers or not. These adjustments could be made by the central bank, intermediaries, or other third parties. Alternatively, such adjustments could not be built into the CBDC system and accomplished through transfers instead. Either way, the CBDC system could likely enable this functionality, should it make sense from a monetary perspective.

This design choice intersects with the transport layer, as an intermediated system would provide more technological methods for creating an interest-bearing CBDC. This design choice also intersects with offline capabilities; if the interest rate is varied over time, it may be challenging – but may be technically possible – to provide interest on wallets that are not able to receive information about the updated interest rate.

Design choice benefits and drawbacks are described below:

Adjustable balance:

- *Increases technical and governance complexity:* A way to change balances outside of ordinary transfers will increase the technical complexity of the system and will add to the governance complexity as deciding who can make those decisions and when will be important. Implementation would be harder and overhead of system design would likely be much higher.
- *May have implications for financial inclusion and equity:* If adjustments require connectivity and are mostly positive, such adjustments may make offline functionality less desirable. On the other hand, an interest-bearing CBDC may provide a more accessible option for consumers to retain value for their CBDC and may help enable more options for monetary policy.
- *May reduce trust:* Depending on governance decisions, a direct monetary policy lever controlled by the central bank on accounts may reduce public trust in the CBDC system, particularly if negative changes are considered.
- *May help improve payment systems:* An interest-bearing incentive to hold may help bring more capital into storage in the CBDC system. This would help increase uptake of the CBDC system, which could help improve payment systems. However, this may also come at the expense of reducing deposits, which could exacerbate risks to loan creation and bank runs.

Not adjustable balance:

- The benefits and drawbacks of not implementing adjustable balances are the inverse of implementing it.