

ROUNDTABLE SUMMARY

Digital Dollar Project

Privacy in the Age of Digital Money: Defining the Requirements for CBDCs

Summary Report on the Digital Dollar Project's
Roundtable Discussions on Privacy Requirements for a
U.S. Central Bank Digital Currency

June 2023

Privacy in the Age of Digital Money: Defining the Requirements for CBDCs

Summary Report on the Digital Dollar Project's Roundtable Discussions on Privacy Requirements for a U.S. Central Bank Digital Currency

As the United States evaluates the advantages and challenges of a central bank digital currency (CBDC), or digital dollar, privacy is at the center of the discussion. To begin defining requirements for a digital dollar that maintains all forms of privacy, the Digital Dollar Project hosted a series of roundtables in partnership with leading educational institutions, including MIT Connection Science and Engineering, UC Berkeley's Center for Responsible, Decentralized Intelligence, and the Georgetown University Law Center's Institute of International Economic Law. Throughout the series, academics and subject matter experts from the government, non-profits, and the private sector discussed and debated the technical and regulatory implications of privacy related to a digital dollar. The roundtables were guided by DDP's [Privacy Principles for a Digital Dollar](#), which was released for public consideration in October 2021:

Private: A U.S. CBDC should avoid subjecting users to undue corporate tracking or government surveillance and should allow users the ability to limit having their information shared with financial services providers. U.S. law should strictly control law enforcement and broader government access to public data.

Secure: A U.S. CBDC should provide robust security against theft, hacking, illegal seizure, and fraud. As such, it should provide a new way for people to handle money individually, utilizing a system that is both secure against attacks and legally protected.

Accessible: A U.S. CBDC should improve Americans' and global dollar users' access to financial services by increasing efficiency and lowering the cost of transacting. Widespread CBDC usage should spur competition in financial services to produce better services at lower costs. Additionally, accessible and low-cost digital wallets could serve as an on-ramp into the financial system for the un-and-under-banked.

Transparent: A U.S. CBDC system should have transparent operations to enable stakeholders to independently gain assurance about its technical functioning, security, and resistance to impermissible monitoring or other exploitation.

The roundtable series explored the concept of a digital dollar that prioritizes privacy protections, avoids undue surveillance, and empowers users to control how their information is shared with financial service providers. Each discussion centered on the importance of security, accessibility, and transparency in a potential U.S. CBDC system. Additionally, the roundtables highlighted the need for policies that complement technological designs and bridge the gap between technologists and policymakers. The following high-level takeaways focus on three main areas 1) the current state of financial privacy, 2) core design requirements for a U.S. CBDC, 3) the recommended approach for U.S. CBDC research.

1. Current State of Financial Privacy

Currently, digital payments exist only in the form of private commercial money, thereby compromising the level of privacy they afford. The erosion of privacy safeguards has been exacerbated by the rapid expansion of the commercial surveillance industry. This industry extensively collects detailed transactional and precise geolocation data, providing lucrative opportunities for commercial data brokers to exploit financial information due to the absence of robust privacy regulations. Alarming aspects of this scenario include the unrestricted availability of such data for purchase by various entities, including law enforcement agencies with little oversight or protections against the circumventions of existing constitutional protections against illegal searches and seizures. To help strike the appropriate balance under existing U.S. privacy laws while considering the uncertainties in federal, state-level and international privacy regimes, we must be dedicated to exploring opportunities to define and clarify the core requirements for the future of money and the financial surveillance landscape.

For more information on the current financial status quo, check out DDP's publications: [The Privacy and Data Security Regulatory Landscape for U.S. Financial Institutions and the Implications for a Digital Dollar](#) and [The U.S. Anti-Money Laundering and Economic Sanctions Regulatory Landscape and the Implications for a Digital Dollar](#).

2. Roundtable Takeaways: Core Design Requirements for a U.S. CBDC

Cash-like Characteristics: A retail digital dollar should possess privacy features that are at least on par with physical cash. Although physical cash is not completely private, it offers more individual privacy compared to digital alternatives like credit card transactions and app-based payments. A digital dollar should strive to enhance certain cash attributes by providing enhanced security, recoverability, and alternative mechanisms to mitigate financial surveillance.

Stable: Access to central bank money, which represents the safest and least risky form of currency, is and should continue to be a public good. While the use of physical cash is declining in the United States, albeit at a slower pace than in other developed economies, there is no evidence to suggest that this trend signifies a decreased demand for central bank money. To ensure continued access to central bank money and its adoption in an increasingly digitized economy, a digital dollar should look to preserve several fundamental characteristics of physical cash, including privacy, resistance to censorship, and resilience in the face of disasters.

Intermediated: There are numerous benefits that can be unlocked through technical designs of digital currencies; however, it is crucial to exercise careful consideration regarding access to these tools to ensure the preservation of the values of a free society. For instance, although programmability can offer significant advantages in the realm of digital currency, it should not be integrated into the core infrastructure of a CBDC system. Rather, programmability functionalities should be exclusively provided at the intermediated level to maintain the security and neutrality of the underlying infrastructure.

Free From Undue Surveillance: A CBDC should not be exploited to expand undue government surveillance capabilities.

Transparent: The viability of a CBDC, or any form of money, fundamentally relies on trust. To foster widespread adoption of a retail CBDC, the public must have confidence in its safety, effectiveness, and privacy as a payment instrument. Transparency and optionality play a critical role in this trust-building process. Given the prevailing low levels of trust in government institutions, which could hinder the public's acceptance of a CBDC, the Digital Dollar Project (DDP) asserts that a CBDC must embrace transparency, allowing anyone—not solely the government—to verify and trust its privacy safeguards.

Optionality: Users should have the freedom to choose their preferred payment methods based on their desired level of privacy and practical considerations. Therefore, it is vital to preserve alternative payment options such as physical cash, credit and debit cards, app-based services, and other digital currencies. Considering user perspectives and assessing their priorities is essential when considering the features of a CBDC.

Private by Default: The future of money should be designed for the default user. In today's digital-first world, many companies rely on disclosure agreements to address privacy concerns. However, consent in such cases often proves illusory. Therefore, it is crucial to prioritize data minimization as the default approach, whenever feasible, to prevent inadvertently creating a digital footprint even without personally identifiable information (PII) present.

Data Minimization: A digital dollar should strive to maintain significant separation between users' information and transaction data. Exploration should be given to CBDC models that minimize reliance on personal identifiers and instead embrace advancements in decentralized identity (DID) solutions.

3. Roundtable Takeaways: Recommended Approach for U.S. CBDC Research

Balanced: Attention should be given to achieving a balance between security and privacy, particularly concerning censorship and the response to criminal activities by bad actors. The proper handling of bad actors and the disclosure of their identity, as well as the potential censorship of their future transactions, remain open questions. If transaction censorship is possible, robust safeguards must be in place to prevent its abuse.

Pragmatic: While it is important to account for risks in a CBDC, it is unrealistic to eliminate all risks entirely. A practical approach involves maximizing the public benefits of a CBDC while accepting a tolerable level of risk. Rejecting CBDC outright risks consolidating private institution monopolies on digital currency and undermines the opportunity to reinstate financial law enforcement in line with American constitutional norms through technological advancements that may reduce the need for certain trade-offs, such as those between personal privacy and crime prevention.

Clear: When discussing privacy in the context of money and transactions, precise terminology and a consistent framework are crucial. Instead of using the term "privacy" broadly, it is essential to consider factors such as "private from whom, about what, for how long, and for what purpose." This approach allows us to better understand what privacy means under which specified conditions and better define

objectives and core requirements for a potential U.S. CBDC. For instance, distinguishing between anonymity and privacy highlights the importance of responsible handling of personal data rather than focusing solely on complete anonymity. Ultimately, privacy entails individuals' control over their information, emphasizing the need to provide autonomy and optionality, minimize data collection, and leverage innovations to prevent unauthorized use or leaks without consent.

Functional: While money initially served as a means to transact value, additional peripheral systems were added for security and tax purposes. When designing digital currency, it is crucial to consider how a new digital form can address societal objectives. This involves identifying areas where technology can aid in achieving such objectives, such as financial inclusion, and areas where it may be preferable to keep the system separate from the current monetary system, such as taxation. A collaborative design process, involving potential CBDC users, can help determine these functional needs.

Exploratory: Privacy-enhancing technologies (PETs) and encryption techniques, such as zero-knowledge proofs (ZKPs), homomorphic encryption, differential privacy, and trusted execution environments (TEEs), show promise in providing individuals with a high degree of privacy while minimizing trade-offs between privacy, financial inclusion and security. However, these solutions are still in the early stages, requiring strong U.S. leadership and research and development (R&D) efforts in both the public and private sectors. While it is important to adopt pragmatic approaches in the near term, it is crucial for both the private and public sectors to persist in exploring the range of technical possibilities for the future of digital currencies. This ongoing exploration is essential for advancing towards the overarching objective of achieving optimal levels of privacy and security.

Design Driven: The design of any CBDC should be driven by functional needs, recognizing that designs for wholesale and retail users may differ.

Open: Any CBDC design and infrastructure must provide ample room for the technology to evolve and grow over time rather than being overly present-biased.

Collaborative: Technology and policy considerations are integral to developing a U.S. CBDC system that ensures individual privacy. Given the relative immaturity of many PETs and technology solutions, policy choices must align with technology to establish privacy as the default in a digital dollar. Bridging the gap between technologists and policymakers is crucial to ensure that a potential U.S. CBDC system leverages solutions offered by new technological advancements.

Holistic: Privacy considerations and innovation should extend beyond currency design to encompass due process for data collection, usage, and critical considerations for the future of identity in an increasingly digital world.

Interoperable: If a digital dollar is intended to be accessible to consumers globally, its design must consider compliance with international privacy and data security regulations, such as the European Union's (EU) General Data Protection Regulation (GDPR). Active engagement in the global ecosystem is crucial for establishing universal norms that uphold the values of a free society. Regardless of whether the U.S. adopts a digital dollar, American citizens and multinational corporations will inevitably encounter Central Bank Digital Currencies (CBDCs) in the future. Restricting the U.S. from CBDC exploration will neither impede nor halt the worldwide deployment of CBDCs or U.S.-headquartered, multinational corporation engagement with them.

4. Roundtable Assumptions

Participants assumed that a digital dollar would be distributed to end users through banks and other regulated intermediaries and focused the discussion on a potential retail CBDC. Unlike a wholesale CBDC, which would be available only to large financial institutions, a retail CBDC would be available to the general public. A retail CBDC, which would be similar in uses to cash, could be used in a range of peer-to-peer, peer-to-business, and business-to-business transactions.

5. Next Steps

The issue of individual privacy is at the center of the Digital Dollar Project's exploration of a U.S. CBDC. In October 2021, the Digital Dollar Project published its initial privacy principles for a digital dollar: private, secure, transparent, and accessible. The Digital Dollar Project is developing a refined list of privacy requirements for a digital dollar that can be evaluated in real-world testing and pilots, as well as other research initiatives. To collect more data to inform the development of these requirements, the Digital Dollar Project will continue its research through a [privacy survey](#) for additional data collection.

If you have expertise in this area and would like to contribute, we welcome you to join the conversation by participating in our data collection process. Simply follow the [provided link](#) to engage in this important discussion.

About the Digital Dollar Project

A nonprofit organization, The Digital Dollar Project was created to encourage research and public discussion on the potential advantages and challenges of a U.S. CBDC – or a "digital dollar." The DDP will identify options for a CBDC solution to help enhance monetary policy effectiveness and financial stability; provide needed scalability, security and privacy in retail, wholesale and international payments; and integrate with existing financial infrastructures. The DDP believes it is key and will facilitate opportunities for the U.S. to engage in international standard-setting regardless of whether the U.S. eventually issues a CBDC or not.