Secure Adoption of a Digital Dollar

Operational and Compliance Risks for the U.S. Banking Sector

Working Paper Series No. 01

July 2023

THE DIGITAL DOLLAR PROJECT

The Digital Dollar Project (DDP) is a non-profit, non-governmental organization devoted to catalyzing research, exploration, and real-world experimentation of a potential digital dollar. The DDP believes that the dynamism and innovation of the private sector has a crucial role to play in the consideration of a digital dollar. Transparent private sector research and experimentation conducted in a neutral space is beneficial to policymakers, academics, technologists, economists, and the broader national interest. The decision of whether to digitize the dollar is no different than past U.S.-led technological innovations – including the space race and the creation of the Internet – in which both the public and private sectors contributed significantly.

To ensure that its work is guided by a diversity of experiences, perspectives, and expertise, the DDP assembled an Advisory Group that includes economists, business leaders, technologists, innovators, lawyers, academics, consumer advocacy and human rights experts, and ethicists. DDP aims to explore design options and approaches for evaluating a digital dollar through various means including convening topic-focused working groups from the Advisory Board. Working group results are released in working paper form, for broad public consideration and are meant to guide a public discourse on a U.S. digital dollar, often highlighting competing ideas and concepts for further exploration. Working papers are non-exhaustive and do not endorse final conclusions or solutions.

This working paper was prepared by The Digital Dollar Project, Inc. (DDP) in collaboration with the DDP Risk Working Group and Accenture, Inc. (Accenture) and is being published in accordance with the aforementioned intentions. This working paper is not intended to bind DDP, participants in the DDP Risk Working Group, or Accenture in any manner, and it is made freely available “as-is” without any express or implied warranties. This working paper is for informational purposes only and does not constitute legal or investment advice and you should not rely on any information or views contained in this white paper in evaluating any specific legal or investment needs you may have. This working paper is not authored by and does not reflect the views of any governmental agency.

Table of Contents

Glossary

CBDC – Central Bank Digital Currency, a digital form of central bank money widely available to the public

Consensus protocol – rules by which a network operates within a trustless blockchain system to verify the authenticity of transactions

CPMI-IOSCO – the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) - an organization that works to enhance the coordination of standard and policy development and implementation regarding clearing, settlement, and reporting arrangements, including financial market infrastructures worldwide

Decentralized exchange (DEX) – a peer-to-peer marketplace that connects cryptocurrency buyers and sellers without needing an intermediary to facilitate the transfer and custody of funds

Denial of Service attack (DoS) – an attack that is meant to shut down a machine or network by flooding the target with traffic or sending it information that triggers a crash, making it inaccessible to its users

Fungible – the nature of goods (or tokens) being functionally identical units that are freely exchangeable or replaceable, in contrast to non-fungible units with unique identifiers that prevent them from being copied, substituted, or subdivided

Multi-Factor Authentication (MFA) – an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN

Multi-Party Computation (MPC) – a cryptographic tool that allows multiple parties to make calculations using their combined data without revealing their individual input

Node – a computer that interacts with and is part of a blockchain network

Non-fungible – the nature of goods (or tokens) being functionally unique with unique identifiers that prevent them from being copied, substituted, or subdivided

Programmability – the ability to specify the automated behavior of a digital currency through code

Provenance – a record of the history of ownership

Regulation E – a basic framework that establishes participants' rights, liabilities, and responsibilities in electronic fund transfer and remittance systems

Smart contract – self-executing programs stored on a blockchain that run when predetermined conditions are met

Tokenization - turning an asset, good, right, or currency into a representation with properties that suffice to attest to and transfer ownership

Validator – a participant in a blockchain who is responsible for verifying new transactions

51% attack – when a malicious actor can compromise more than half of the validators on the network, the actor can execute fraudulent transactions

Acronyms

AML – Anti-Money Laundering

BIS – Bank for International Settlements

BSA – Bank Secrecy Act

CBDC – Central Bank Digital Currency

CCAR – Comprehensive Capital Analysis and Review

CFT – Countering the Financing of Terrorism

CLS – Continuous Linked Settlement

DEX – Decentralized Exchange

DID – Decentralized Identifiers

DoS – Denial of Service attack

DLT – Distributed Ledger Technology

ECB – European Central Bank

FATF – Financial Action Task Force

FDIC – Federal Deposit Insurance Corporation

FinCEN – Financial Crimes Enforcement Network

FSB – Financial Stability Board

FX – Foreign Exchange

IRS – Internal Revenue Service

ISO – International Organization for Standardization

IT – Information Technology

KYC – Know Your Customer

KYT – Know Your Transaction

MFA – Multi-Factor Authentication

MPC – Multi-Party Computing

NIST RMF – The National Institute of Standards and Technology Risk Management Framework

OCC – Office of the Comptroller of the Currency

OECD – Organization for Economic Cooperation and Development

OSTP – The White House Office of Science and Technology Policy

PFMI – Principles for Financial Market Infrastructures

TPRM – Third-party Risk Management

TRUST – Travel Rule Universal Solution Technology

Introduction

The March 2022 Executive Order (EO) on *Ensuring Responsible Development of Digital Assets* marked a period of increased focus by the United States on a potential central bank digital currency (U.S. CBDC), or a "digital dollar," and spurred ongoing digital currency research initiatives across federal agencies. While the United States has not decided whether it will deploy a CBDC, increased interest and rapidly accelerating foreign CBDC deployments have compelled the U.S. private sector to examine the risks and opportunities of a digital dollar. This working paper is not intended to advocate for the deployment of a U.S. CBDC but rather represents a first step to understanding the potential operational and compliance impacts to the U.S. banking sector posed by a digital dollar, either among financial intermediaries (wholesale CBDCs) or by the general public (retail CBDCs).[1]

A digital dollar could offer significant economic benefits, including faster payments, more inclusive financial access, reduced intraday exposure, operating efficiencies, and support for the dollar's role as the global reserve currency. It could also introduce new risks and exacerbate existing ones. The Digital Dollar Project (DDP), a non-profit organization dedicated to catalyzing private sector exploration of the advantages and challenges of a digital dollar, established a Risk Working Group (RWG) to begin evaluating these risks, opportunities and proposed mitigants. The RWG comprises recognized and non-partisan leaders from major financial institutions, payments companies, law firms, technology providers, non-profits, and think tanks. These participants developed this working paper to facilitate public discussion and inform policymakers on the operational impacts of a potential digital dollar on the private sector.

The RWG focused this initial paper on banks, given their current role in commercial and wholesale markets and potential future roles as distributors and custodians of digital dollars. Without extensive engagement with regulators and risk mitigation, banks could face a significant impact from deploying a digital dollar. Banks would need to carefully integrate this new form of digital money into their existing processes, technologies, and relationships–each of which could meaningfully effect their ability to absorb and handle operational and compliance risks.[2]

The RWG developed a preliminary risk framework, which includes an array of policy considerations and mitigation measures. The RWG primarily considered changes specific to federal- and state-chartered banks, as these institutions would be integral stakeholders in any digital dollar ecosystem. The RWG may expand its focus to evaluate potential risks and opportunities to other private sector participants, such as money transfer operators, fintechs, payment networks, and non-financial industries in the future–such future work might build on the baseline considerations included in this paper.

For the U.S. government to make informed policy decisions about a digital dollar, it must understand the full range of impacts–from benefits to risks and ways to mitigate those risks. In this context, the DDP believes that the private sector's perspectives must be considered in the national CBDC discussion. Industry members, academics, policymakers, trade associations, and other interested individuals and groups are invited to comment on this paper's findings by contacting info@digitaldollarproject.org.

---

[1] This working paper is iterative. Its findings are not final policy recommendations or indicative of CBDC design choices. While elements of distributed ledger technology (DLT) are explored to identify relevant risks, this paper should not be viewed as a technology recommendation for a digital dollar.

[2] Privacy-related risks have been omitted in this iteration as the DDP is convening a separate privacy roundtable series with industry leaders. Additionally, risks related to monetary policy and financial stability have been excluded.

Background

The DDP formed the RWG in September 2022 to produce working papers that facilitate continued public discussion and education on the operational and compliance implications of a digital dollar for the private sector. This paper, which includes a proposed risk framework, is the RWG's initial work product, which is intended to be broadly shared with policymakers and interested stakeholders. The risk framework also serves as a resource for the private sector to begin understanding business model impact of a potential retail and wholesale digital dollar.

The Digital Dollar Project Champion Model

In May 2020, the DDP proposed a "Champion Model" of a potential digital dollar for public consideration.[3] At the time, CBDCs were a relatively novel concept. Still, there was enough global research, evidence, and experiential perspective to develop a "champion-challenger" approach to DDP's research and experimentation. The DDP created the Champion Model by evaluating insights and best practices from digital currency initiatives worldwide. Through pilots and other research initiatives like this working paper, the DDP continues to test the potential benefits of a CBDC that reflect the Champion Model's core tenets (Tenets), which are the tenets used by the RWG as a basis for considering risks and corresponding mitigation measures:

1. **Tokenization:** A U.S. CBDC will be a tokenized form of the U.S. dollar.
2. **Third format of currency:** A U.S. CBDC will operate alongside existing fiat currency and commercial bank money. It will mirror many properties of physical money, including its ability to work alongside existing account-based systems.
3. **Maintenance of the two-tiered banking system:** A U.S. CBDC will be distributed through the existing two-tiered architecture of commercial banks and regulated financial technology and payments intermediaries.
4. **Privacy:** A U.S. CBDC will support a balance between individual privacy rights and necessary compliance and regulatory processes, decided upon by policymakers and consider Fourth Amendment precedent.
5. **Monetary policy-neutral:** A U.S. CBDC will not impact the Federal Reserve's ability to affect monetary policy and control inflation.
6. **Technology decisions and design choices driven by functional needs:** The policy and economic requirements of a U.S. CBDC will inform both the underlying technology and ultimate design choices.
7. **Future-proofing the architecture through flexibility:** The chosen technological architecture will offer the flexibility to adapt configurability based on policy and economic considerations.
8. **Continued private sector innovation:** A U.S. CBDC will act as a catalyst for innovation and will not be antithetical to the development of private sector initiatives.

[3] Digital Dollar Project. "Whitepaper 2.0"

Approach

The RWG followed a three-step approach:

1. **Identified Risks**: The RWG identified potential risks to federal and state-chartered banks presented by a potential digital dollar.
2. **Proposed Risk Mitigants**: The RWG proposed risk mitigations for banks related to CBDC integration and identified certain residual risks unaddressed by these recommended controls.
3. **Produced Policy Considerations**: The RWG proposed policy considerations designed to assist policymakers in better understanding CBDC-related risks and opportunities.

Key Assumptions

A digital dollar should enable the fair, open, and competitive marketplace that is the hallmark of the American economy. It should promote innovation and competition and support the identification and interdiction of illicit transactions and other bank compliance measures. Any potential benefits should be balanced against evolving risks and will require private and public sector mitigations.

Given the current lack of specificity regarding the potential design of a digital dollar and whether it would be a wholesale or retail CBDC, the RWG assumed the following:

- A digital dollar is a third and equal form of U.S. currency. It will have the same value, risk weighting, governance structure, and distribution model as existing cash and reserves.
- The digital dollar network will likely be built on DLT under a permissioned governance model where parties must be granted permission to join and transact. This technology model may significantly reduce many risks identified by financial regulators concerning banks' participation in digital asset activities, such as the governance risks outlined in the January 2023 Joint Statement on Crypto-Asset Risks to Banking Organizations.[4]
- This paper considers both a wholesale and retail CBDC to explore various kinds of potential risks.
- The digital dollar network will maintain the intermediated banking model whereby regulated financial institutions act as both distributors and potential custodians for digital dollars to benefit end users.

[4] The Federal Reserve, Federal Deposit Insurance Corporation, Office of The Comptroller of The Currency. "Joint Statement on Crypto-Asset Risks to Banking Organizations"

Out-of-Scope

To concentrate on the operational and compliance risks and opportunities that a potential digital dollar may pose to the private sector, the RWG deferred certain topics for later research. Topics that were fully or partially out-of-scope for this paper include:

- **Alternative CBDC Distribution Models:** Some financial industry stakeholders have expressed concern that banks could be disintermediated through alternative CBDC models whereby the Federal Reserve distributes digital dollars directly to individuals. The RWG chose not to evaluate such a CBDC design as the Federal Reserve and other policymakers have stated that a potential digital dollar should be intermediated. Moreover, the DDP's Champion Model hypothesizes that a digital dollar would be distributed to end users through regulated intermediaries, including banks.[5]
- **Cryptocurrencies:** The risks posed by cryptocurrencies are not included in this paper.
- **Elements of Potential Undue Surveillance and Privacy**: The RWG chose not to explore privacy issues in this paper. Instead, the DDP has convened a separate Privacy Working Group that considers crucial questions related to preserving all forms of privacy. This work includes revisiting the DDP's Privacy Principles for a Digital Dollar, published in late 2021.[6]
- **Financial Stability:** This paper does not address risks related to bank deposits through the introduction of CBDC, with related impacts on bank lending and the broader economy. The RWG acknowledges significant and novel financial stability risks associated with a digital dollar. Still, this topic requires an in-depth and highly data-driven analysis and is therefore not discussed in this paper.
- **Monetary Policy:** The DDP has previously stated that a digital dollar should not impact the Federal Reserve's ability to affect monetary policy and control inflation.
- **Programmability:** Programmability refers to the ability to control and manage the currency through code and includes smart contracts. While programmability could offer certain benefits and trade-offs, the RWG takes no position in this paper.

[5] Anneke Kosse and Ilaria Mattei, Bank for International Settlements, "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies"

[6] Digital Dollar Project. "Privacy Principles for a Digital Dollar"

Summary of Findings

The findings of this paper are not exhaustive and represent a first step in documenting potential risks, mitigants and opportunities. Identified risks may cover both retail and wholesale CBDCs.

Six risk themes are mapped to the Tenets and summarized below. Detailed findings are further discussed in the Risks and Policy Considerations section.

Tenet	Identified Risks	Proposed Risk Mitigants	Policy Considerations
Tokenization	**Token Provenance** • Unclear traceability obligations for financial institutions • Obfuscation of token provenance through mixers and tumblers	• Banks should explore emerging forms of transaction monitoring, such as Know Your Transaction and Know Your Coin	• Consider a non-fungible token model to support traceability requirements • Provide guidelines for the traceability of funds • Study the benefits and risks posed by mixers and tumblers
	Onboarding Bad Actors • Potential reliance on the customer onboarding and verification processes of other financial institutions	• Banks should establish common customer onboarding practices (e.g., KYC compliance) • Banks should explore emerging forms of customer verification, such as digital identities	• Evaluate the feasibility of inter-organizational customer onboarding and verification
	Counterfeit and Double Spend • Potential for counterfeiting existing tokens or creating fake tokens with new identifiers	• Banks should explore a liability-shifting framework that incentivizes parties to mitigate risk • Banks should explore cryptographic checks on transactions (e.g., zero-knowledge proofs) • Banks should enhance transaction monitoring to detect suspicious transactions	• Confirm native functionality to prevent counterfeiting • Establish strict and clear validator node requirements to prevent unauthorized copies

Tenet	Identified Risks	Proposed Risk Mitigants	Policy Considerations
Third format of money	**Recordkeeping and Reporting** • Potential for difficulty complying with federal recordkeeping rules and requirements	• Banks should update recordkeeping functions to integrate with token-based systems • Banks should enhance data governance capabilities to accommodate various custodial arrangements	• Update relevant laws and regulations to account for tokenized digital dollars and provide clear guidance to banks to ensure compliance
	Convertibility • Currency and settlement risk resulting from cross-CBDC and non-CBDC trading • Credit and liquidity risk related to CBDC convertibility to/from stablecoins • Operational risks related to CBDC convertibility to/from deposit accounts	• Banks should explore technology and trading controls • Banks should perform robust issuer/ counterparty reviews • Banks should integrate custody, deposit, and payment systems	• Promote interoperability through technical standards and payment system rules
Maintenance of a two-tiered banking system	**Erroneous and Misdirected Transactions** • Lack of adoption driven by the inability to recover erroneous transactions • Unclear relationship between existing regulations and card chargebacks to CBDCs and wallets	• Banks should explore the payment industry's model for risk-shifting to balance risk-reward and incentivize parties to mitigate risks	• Consider allowing transaction reversals under certain conditions • Review Reg E to provide digital wallet-specific rules.[7]
	Digital Financial Literacy • Lack of adoption driven by lack of familiarity with digital assets	• Banks should invest in customer education and strengthen the user experience of CBDC wallets	• Broad education specific to CBDCs to educate customers on the risks and obligations involved

[7] Regulation E, also known as Reg E, is a federal regulation that governs electronic fund transfers conducted by consumers. It establishes the rights, responsibilities, and liabilities of consumers and financial institutions.

Tenet	Identified Risks	Proposed Risk Mitigants	Policy Considerations
Technology decisions and design choices driven by functional needs	**Custodial Key Management** • Lack of adoption driven by lack of familiarity with custody relationships and user errors concerning cryptographic keys	• Banks should explore controls like multi-signature to execute certain transactions • Banks should consider controls to codify clear lines of liability regarding key management	• Provide clarity on usage and availability of self-custody option
	Wallet Takeovers • Lack of adoption driven by limited familiarity with custody relationships and user errors (e.g., passphrase disclosure)	• Banks should explore multi-party computation (MPC), multi-factor authentication (MFA), and suspicious behavior controls to secure wallets • Banks should also explore best practices for securely sharing customer information with required counterparties	• Share guidance on potential transaction value limits • Provide clear technical security standards
Future-proofing the architecture through flexibility	**Secure Infrastructure** • Risk of network reliability issues or technical compromises (e.g., encryption errors, malware, DDoS attacks, and hardware breaches)	• Banks should use appropriate traditional risk frameworks for baseline controls for DLT infrastructures and interfaces • Banks should engage in industry forums to support industry infrastructure standards	• Provide guidance for privacy incident management, robust contingency plans, and continuity plans • Provide transparent and measurable validator node requirements • Test network resiliency frequently
	Offline Transactions • Risk of offline payments avoiding anti-money laundering (AML) and countering the financing of terrorism (CFT) measures	• Banks should explore device controls, such as MFA • Banks should explore infrastructure controls, such as tamper-resistant certified hardware chips	• Provide guidance on offline payments standards, resiliency expectations, and transaction value limits, if any

Tenet	Identified Risks	Proposed Risk Mitigants	Policy Considerations
Continued private sector innovation	**Third-Party Risk Management** • Inadequate oversight of critical third-party vendors, including inconsistent third-party risk management (TPRM) • Increased reliance on third-party infrastructure and applications with no direct monitoring or accountability	• Banks should examine third-party risk management frameworks and develop a tailored model for a digital dollar • Banks should participate in standards development to drive consistent third-party interoperability and oversight	• Provide third-party risk management guidance for the CBDC network and expand the use of coordinated service provider examinations

Risks and Policy Considerations

The risk framework above was further developed to identify private sector mitigants and policy considerations in accordance with the Tenets.

1) Tokenization

In September 2022, the White House Office of Science and Technology Policy (OSTP) published a technical evaluation of a potential digital dollar system that included an analysis of the fungibility of a digital dollar.[8] According to the OSTP, whether a digital dollar system supports fungible and functionally identical units, non-fungible discrete units, or both is a fundamental consideration when designing mechanisms to determine the authenticity of a token. While each option offers benefits, it also introduces new opportunities for financial crime. These risks may include new traceability obligations and the potential onboarding of riskier customers, including cybercriminals and fraudsters.

Token Provenance

For the paper, the RWG assumed that a digital dollar would likely be built on DLT under a permissioned network governance model. The permanence of DLT raises the question regarding the role of financial institutions in determining the provenance of a token (e.g., the number of transaction legs). In a digital dollar system, banks granted access to funds should have a degree of transparency in the movement of those funds within the network to comply with internal and external rules or compliance standards. In tokenized ecosystems, malicious actors can obfuscate the origin of funds using a mixer or tumbler, such as the now-sanctioned Tornado Cash, by obscuring the ability to trace steps across a series of transactions.[9] Bad actors can also generate returns from these illicit funds as they obfuscate the source

[8] The White House Office of Science and Technology Policy (OSTP), Technical Evaluation for a U.S. Central Bank Digital Currency System

[9] U.S. Department of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash

and destination through decentralized exchange (DEX) liquidity pools.[10] However, the existence of mixers and tumblers on permissionless networks does not presuppose their presence on a permissioned network, which grants network operators the option to seize funds as part of government sanctions and otherwise mitigate financial crimes.

Bank compliance and operations teams that manage money laundering detection systems should explore emerging forms of detection to address these novel risks. Statistical methods and advanced tools are often required to trace the provenance of funds. Examples of such transaction monitoring processes include Know Your Transaction (KYT) and Know Your Coin techniques.[11] Banks should then mature and scale these processes for continued relevance and efficacy in a future CBDC environment to mitigate the risk of inadvertently funding customer accounts with laundered money. These advanced methods are often necessary as sophisticated bad actors can utilize techniques to obfuscate their transactions and identities across wallets, exchanges, and custodians.

Onboarding Bad Actors

It is impossible to eliminate bad actors from the financial system; however, banks commit substantial resources to prevent onboarding them. In a recent survey, two-thirds of C-suite bank executives said a single customer review costs between $1,501 and $3,500, which for banks onboarding 10,000 new customers can result in $35M costs for KYC per annum.[12] In a digital dollar system, there is a perceived risk that banks will need to rely on the customer identification processes of other institutions, which raises questions about the impacts of a potential inter-organizational reliance. There are novel risks associated with a distributed network of intermediaries being granted the ability to bring customers onto the network using varying standards to screen customers. Further, should an “allowlist” approach be adopted, it would codify and accentuate this risk.[13]

In such a model, establishing standards for inter-organizational reliance on Know Your Customer (KYC) will be critical for a successful digital dollar system. Challenges may arise when KYC standards are not enforced to the level that Bank B expects or if falsified credentials are used to bypass checks. Clear regulatory guidance on this potential inter-organizational reliance will aid responsible organizations in complying with AML/Countering the Financing of Terrorism (CFT) rules and regulations.[14]

---

[10] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance,

[11] KYT is a DLT transaction screening method that financial institutions use to flag, review, and restrict bad actors based on the assigned risk score of the sender and receiver. Know Your Coin uses coin-specific risk parameters to flag suspicious transactions. For example, tokens used by sanctioned entities may warrant a higher risk rating.

[12] Fenergo Research, KYC in 2022: A Final Frontier for Digital Transformation in Financial Services

[13] In this context, an allowlist is a list of customers who have been onboarded onto the network in accordance with the designated bank’s standard account-opening procedure. See generally, Anti-Money Laundering / Countering The Financing Of Terrorism (AML/CFT),

[14] Decentralized Identifiers are further explored by the World Wide Web Consortium (W3C), an international community that develops open standards to ensure the long-term growth of the Web.

Banks should also explore self-governance standards for digital identities and transaction monitoring to mitigate the inter-organizational or network risks of onboarding bad actors. Such self-governance can involve industry forums to define processes for gathering and investigating required customer information to form a single customer view. Banks should explore defining mutually agreed-upon approaches to verify a customer and issue the appropriate credentials to be verified by other parties. Discoverable and verifiable customer data on the digital dollar network could equip permissioned parties with the visibility needed to detect bad actors. Advances in decentralized identifiers (DIDs) could provide the network with such visibility without exposing the entirety of an individual's data. [15]

Despite these mitigants, the digital dollar may continue to be vulnerable to malicious actors in the same way as traditional currency. Therefore, compliance teams and network operators should collaborate to monitor and adapt to the technology and minimize Bank Secrecy Act (BSA) risk.

Counterfeit and Double Spend

Another financial crime that warrants consideration is the possibility of compromising the digital dollar system by authorizing invalid transactions with counterfeit CBDCs. Although measures will likely be implemented to prevent unauthorized copies of digital dollars, Sweden's Riksbank outlined two ways a CBDCs could be counterfeited: by making copies of existing tokens or by creating unauthorized tokens.[16] The former, known as the double spending problem, entails copying the underlying code of a CBDC token and spending it more than once. The latter, more difficult to achieve, entails a bad actor generating a new serial number for the token that does not cryptographically correspond to an existing token.

While the design of the digital dollar system should natively mitigate against counterfeit digital dollars, the question of who the responsible party is should unauthorized tokens be minted remains. Several mitigation measures could reduce the counterfeit CBDC and double-spending risk. First, banks could implement cryptographic checks on transactions and regularly screen customer wallets to verify that all security protocols are updated.[17] Second, banks could set up compliance measures to detect illicit transactions using counterfeit tokens, such as processes for authenticating digital dollars and reporting and investigating cases of potential counterfeiting. Finally, to clarify the responsible party in scenarios where counterfeit tokens are created, banks should establish a liability-shifting framework akin to the card industry's model for assigning responsibilities for token authentication based on financial motivators.[18]

---

[15] Decentralized Identifiers are further explored by the World Wide Web Consortium (W3C), an international community that develops open standards to ensure the long-term growth of the Web.

[16] Hanna Armelius, Carl Andreas Claussen, and Isaiah Hui, Sveriges Riksbank, "On the possibility of a cash-like CBDC"

[17] A cryptographic check typically refers to a mechanism used to verify the integrity and authenticity of digital data using cryptographic techniques. It involves the use of cryptographic algorithms and keys to ensure that the data has not been tampered with or modified in transit or storage.

[18] Douglass, Duncan, Federal Reserve Bank of Chicago, "An examination of the fraud liability shift in consumer card-based payment systems."

Policy Considerations

- To enable effective AML/KYC measures, sanction investigations, and fraud mitigation, a digital dollar should consider adopting the non-fungible tokenization model, as defined above. Non-fungible tokens would be assigned unique token identifiers, or serial numbers, which could support tracing the provenance of digital dollars across transactions. Adopting a non-fungible tokenization model could also hinder the ability of mixers and tumblers to mask the unique token identifier. Striking a balance between the risks and rewards of the traceability of funds is critical to the design of a digital dollar.
- If the United States launches a digital dollar, the U.S. Department of the Treasury should comprehensively review existing AML, sanctions, and fraud-related laws and regulations for potential updates to reflect current technology and the digital dollar system. The Department of Treasury should also explore how innovative technologies, like blockchain and DLT, could potentially change the requirements and scope of regulation, given their inherent features of transparency and immutability.
- When considering updated KYC/AML rules relevant to a potential digital dollar system, the U.S. government should consider using existing best practices and guidance, when possible, for initial consideration. For example, several federal departments and agencies, including the Department of the Treasury, the Department of Justice, the Department of Homeland Security, and the National Science Foundation, have drafted comprehensive risk assessments for digital assets' illicit finance risks.[19] Banks and customers could benefit from a comprehensive review analyzing whether this assessment applies to potential money laundering and terrorist financing risks related to a digital dollar system and, if not, whether new assessments would be useful.
- The Federal Reserve, Department of the Treasury, and Department of Justice should study the potential advantages for user privacy offered by tumblers and mixers and evaluate compliance and law enforcement trade-offs. These advantages should be weighed against potential compliance and law enforcement trade-offs, such as the ability of tumblers and mixers to prevent the network from preserving funds provenance when necessary for critical bank practices like sanctions investigations.
- The Financial Crimes Enforcement Network (FinCEN) and Financial Action Task Force (FATF) should consider the benefits of an "allowlist" for banks to list known CBDC addresses to comply with AML recommendations.[20]

[19] See Fighting Illicit Finance, White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets
[20] Financial Action Task Force leads global action to tackle money laundering, terrorist, and proliferation financing. It is an inter-governmental and policy body that sets international standards to prevent illegal financial activities.

- The U.S. government, including law enforcement agencies, should remain vigilant about the potential for bad actors and foreign governments to engage in counterfeiting practices, including skimming and destabilization, which could disproportionately affect banks. The Department of the Treasury and Federal Reserve Board should develop clear and strict validator node requirements to further reduce the risk of counterfeiting.
- Assuming the U.S. Department of the Treasury handles "printing" and therefore incorporating counterfeit-deterrent technologies in digital dollars, the Department and its offices and bureaus (e.g., the Bureau of Engraving and Printing) should ensure the acquisition of necessary expertise, resources, and personnel to "mint" secure digital dollar tokens.

2) Third format of currency

Under the DDP Champion Model, a tokenized digital dollar would be a third form of legal tender with the same legal status as cash and reserves, backed by the full faith and credit of the U.S. government. Banks, policymakers, and standards-setting organizations will need to be clear on recordkeeping and valuation approaches.[21] Banks would need to ensure that a digital dollar is interoperable with existing forms of currency, including foreign CBDCs and commercial bank money.

Recordkeeping and Reporting

Introducing a digital dollar as a third form of legal tender may pose a risk to banks that need clarity on rules and guidance for recordkeeping and regulatory reporting requirements. Bank recordkeeping functions will require updates to integrate with token-based systems, though they may still encounter operational risks like conversion errors or process breakdowns if guidance is not codified.[22] Provided a potential digital dollar will be a liability of the central bank, there would likely be some new reporting requirements for banks, including ensuring that banks are adhering to any applicable holding limits.

Banks would benefit from regulatory reporting guidance from policymakers to align with the Federal Reserve's oversight of CBDC issuance and redemption. Assuming regulatory reporting of digital dollars will be required, banks will need to enhance their data governance, quality, and integration capabilities to accommodate various custodial arrangements, including those involving third-party wallet providers.

Convertibility

The convertibility of a digital dollar is a key factor in achieving the easy flow of funds to and from other payment systems. Below are three scenarios to spark discussion surrounding digital dollar convertibility with other assets and potential risk mitigation controls.

---

[21] Board of Governors of the Federal Reserve System "Money and Payments: The U.S. Dollar in the Age of Digital Transformation"

[22] See generally, FASB Proposed Accounting Standards Update (ASU), Intangibles — Goodwill and Other — Crypto Assets (Subtopic 350-60): Accounting for and Disclosure of Crypto Assets.

Scenario #1: Digital Dollar vs. foreign CBDCs

Introducing a digital dollar could change currency exchange activities, both bilaterally and via Continuous Linked Settlement (CLS), introducing currency and intraday credit risk. These changes include settlement methods and speeds and variations for trading pairs (trading against currencies without digital representation). There are also strategic business model risks (see discussion on FX bank in Towards the Holy Grail of Cross-Border Payments).[23] With the inclusion of interoperability measures to address various foreign CBDC designs, banks can mitigate risk by integrating real-time FX quotes, bulk order rate methods, or a hybrid of both.

Scenario #2: Digital Dollar vs. privately-issued stablecoins

Banks may face credit and liquidity risks when holding, redeeming, or exchanging privately-issued stablecoins against a digital dollar. Risks vary based on issuer creditworthiness and treasury compliance standards, which banks are well-positioned to establish. Banks should ensure stablecoin issuers have robust compliance functions, underlying issuer banking capabilities, and audit functions. Banks may need to mitigate liquidity risks by monitoring network and off-network activities and updating their treasury functions. Risk controls may include market manipulation controls and governance checks to confirm reserves via Merkle Root Testing.[24]

Scenario #3: Digital Dollar custody vs. traditional deposit account balances

Expanding public access to financial services is a core benefit of a retail digital dollar. However, to bolster financial inclusion, CBDCs should not displace the existing banking system's processes for managing deposits. Because banks will likely custody digital dollars for consumers, they should consider ensuring that any new custody systems integrate with traditional custody methods. Potential convertibility and settlement (payout) failures caused by system downtime or disruption increase the risk of losing customer funds. These matters are further discussed in the OSTP paper Technical Evaluation for a U.S. Central Bank Digital Currency System.

Policy Considerations

- Federal recordkeeping requirements will require updates to account for the deployment of a tokenized digital dollar. Policymakers should evaluate the Bank Secrecy Act, the Truth in Lending Act, OFAC regulations, and related policies for continued relevance in a future with tokenized digital currencies. Private sector intermediaries like banks would benefit from clear guidance to ensure compliance with updated recordkeeping rules. A well-designed digital dollar should efficiently interoperate with foreign CBDC systems, commercial bank money, and physical currency.
- Given the importance of transferability and convertibility between asset classes, banks would benefit from U.S. government leadership on international technical standards for CBDCs. Some key standard-setting bodies include Financial Accounting Standards Board (FASB), the Financial Stability Board (FSB), the FATF, the Comprehensive Capital Analysis and Review (CCAR), the Committee on Payments and Market Infrastructure (CPMI), International Organization for Standardization (ISO), and others. Similarly, Central Banks and Payment System Operators would need to collaborate on convertibility and transferability across asset types and payment systems, including but not limited to system rules.

---

[23] European Central Bank. "Towards the Holy Grail of Cross-Border Payments"

[24] A Merkle Tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

3) Maintenance of a two-tiered banking system

In the existing two-tiered banking system, the Federal Reserve issues bank notes for the public and creates reserves within the banking system. The DDP Champion Models envisions a retail and wholesale digital dollar to maintain the existing two-tiered distribution architecture where commercial banks and other regulated intermediaries exchange reserves and banknotes for digital dollars. Digital dollars would then be distributed to retail and corporate end-users by commercial banks and other regulated intermediaries. This section addresses risk areas specific to the impacts of a potential digital dollar within the context of the existing two-tiered distribution model.

Erroneous and Misdirected Transactions

Instant settlement is a CBDC feature that could accentuate the risk of customer disputes related to failing to recover misdirected payments caused by errors or malicious activity. For example, if a digital dollar is a bearer instrument that carries settlement finality, a simple case of a customer mistakenly sending $100 to the wrong recipient would be more complicated. The customer's bank may need to be positioned to remediate this misdirected and settled transaction.

Lessons may be drawn from the credit card industry's model for risk-shifting, which offers clear rules for distributing risk across banks, acquirers, merchants, and cardholders and enjoys widespread adoption.[25] Banks should explore similar models to allocate risks across network actors. For example, providing customers with the ability to flag transactions and the bank with the ability to reverse transactions to bolster trust in a digital dollar system. Residual risks of irrevocable transactions may persist and must be considered for bank regulatory obligations like Regulation E, which is designed to protect users when they use electronic fund and remittance transfers (e.g., ATMs, overdrafts, direct deposit, international payments).

Digital Financial Literacy

Another risk area for banks is the potential need for digital financial literacy among customers. Digital currency, such as a digital dollar, offers new and innovative ways to manage and store value. However, customers may not fully understand its core features, such as acting as a bearer instrument that carries settlement finality and managing private keys. Unlike traditional financial products, disputes may not be possible in a token-based system where value and messages transfer instantaneously, making transaction reversal difficult. As a result, customers may lose funds, and banks may suffer reputational damage due to this lack of education. Banks could mitigate this risk by investing in customer education and intuitive user experiences to help them manage digital dollars effectively.

Bank customers would benefit from education on CBDCs on how to deposit, transfer, and spend digital currencies. Focus areas for customer education include but are not limited to custody, private key management, counterfeit detection, identifying known addresses, scams, and funds recovery. While empowering customers to make safe choices using CBDCs could reduce risk, residual risks related to human error and unexpected system outages may persist.

[25] The credit card industry has successfully developed and maintained a liability-shifting framework to account for risks across multiple parties involved in a payment—issuer, merchant, acquirer, and cardholder. Liability for risks, such as fraud or credit risk, is allocated based on which party is incentivized to identify and mitigate the risk.

Policy Considerations

- Policymakers should evaluate whether a Federal Reserve regulation that outlines rules and procedures for electronic funds transfers (Regulation E) properly addresses the CBDC ecosystem for domestic and cross-border payments and whether it will need to be updated to address risks related to instant settlement.[26]
- Policymakers should evaluate whether transaction-level remediation in a potential digital dollar system could be retroactively ordered and, if so, who can authorize remediation and what technical and legal features would enable such a process.
- Tokenized digital dollars operating within a digital dollar system could enable instant settlement finality. Given the immediate settlement finality, policymakers should consider whether new oversight for misdirected or flawed transactions is needed.
- Federal financial regulators should provide clear guidance to banks on how to handle the reversal of a transaction should the transaction be deemed illegitimate post-settlement. Regulators and banks should also determine the appropriate remediation approaches and consider developing or enhancing relevant disclosure documentation specific to CBDCs as needed.
- The public and private sectors have roles in conducting educational outreach to bolster consumer digital financial literacy. The private sector has led many financial literacy initiatives that may serve as useful examples for future efforts. Banks and bank-related associations have historically played a role in educating consumers about the risk of fraud. The American Bankers Association, for example, ran a "Banks Never Ask That" campaign to educate people about avoiding scams. Additionally, the U.S. government should partner with community banks and credit unions already serving as trusted institutions, particularly for underserved communities. As an example of public sector educational outreach, the Consumer Financial Protection Bureau offers a range of educational consumer resources that should be updated if the United States deploys a digital dollar. [27]

4) Privacy

This paper does not discuss the potential risks of undue surveillance and the related implications for privacy. However, the DDP recognizes the importance of privacy and has established a privacy-focused working group. This working group is guided by the Digital Dollar Project's Privacy Principles, which were published in October 2021. To explore this topic further, the Digital Dollar Project has organized a series of privacy roundtables and released initial high-level insights. These insights will contribute to the DDP's upcoming publication around proposed privacy requirements for a potential digital dollar.

5) Monetary policy neutral

This paper does not discuss the risks associated with monetary policy. The implementation of a digital dollar should have no bearing on monetary policy.

---

[26] See generally, 12 CFR §205 Electronic Fund Transfers

[27] Consumer Financial Protection Bureau. "Consumer Resources"

6) Technology decisions and design choices driven by functional needs

A core feature of a potential digital dollar system is the custody of CBDCs by consumers, businesses, banks, and other potential custodians, depending on the selected model. Because digital dollars would exist in a digital location (i.e., a shared ledger), the designated custodian will safeguard those funds from attack or compromise. Given banks' current roles as holders of customer deposits, digital custody of CBDCs will likely be a key requirement for banks. This requires examining digital wallets and custodial models to secure private keys and prevent wallet takeovers.

Custodial Key Management

CBDC experimental patterns to date have adopted the custodial model whereby an intermediary holds private keys, and therefore funds, on behalf of a customer; this promotes usability by shifting custodial key management responsibility to an institution with the knowledge, systems, and controls for such oversight. The private sector has also explored the self-custody model, where customers own private keys and funds. Both models offer risks and trade-offs that should be understood when considering the design of a digital dollar system.

Under the custodial model, customers do not have independent and direct access to their private keys associated with the wallet and, therefore, do not fully control their funds. This exposes banks to the risk of losing keys and associated customer funds in the event of a breach. In August 2022, thousands of Solana wallets were drained following a suspected "widespread private key compromise" because of inadequate third-party key management. This compromise resulted in an estimated $8 million loss for customers.[28] A digital dollar network should have standards and controls that codify clear lines of liability to prevent incidents like this, and banks should institute measures to store keys securely.

The MIT Media Lab reported that to support financial inclusion, CBDC system designers should consider preserving the benefits of self-custody, which is currently not possible for U.S.-issued currency in the digital realm. Underbanked and unbanked individuals who may not trust financial intermediaries may elect to take custody of their digital dollars, as this offers a similar degree of access and control of cash in its physical form.[29] With self-custodial wallets, customers risk mishandling, misplacing, or disclosing their private keys. Customers can be victims of phishing scams, which are growing in prevalence, or may misplace sensitive information, such as passphrases. Self-custodial wallets may also introduce risks to banks as users may circumvent the onboarding processes of a designated entity, such as a licensed bank. Unscreened self-custodial wallet users may then transact with bank-onboarded customers using custodial wallets. Therefore, in its initial deployment, a digital dollar system will likely follow the custodial model, where approved intermediaries are responsible for managing customers private keys and funds.

[28] TechCrunch. "Thousands of Solana wallets drained in multimillion-dollar exploit."
[29] MIT Media Lab. "Expanding Financial Inclusion or Deepening the Divide?"

Emerging wallet innovations should be explored to limit the risks customers and banks take under either model. Multi-signature is a technical control that requires multiple authorizations from trusted individuals to execute certain transactions. Banks and the Federal Reserve should ensure that customers are educated about responsibilities and are aware of common threats like phishing. Physical controls like business continuity plans, physical access management, and offsite storage facilities can also mitigate the risk of compromised custody keys.

Wallet Takeovers

The shift of some funds from physical banknotes and traditional deposit accounts to a digital dollar system based on custody may introduce novel risks associated with unauthorized access to funds or digital wallet compromises. Should a customer's private keys be disclosed, bad actors could gain unauthorized access to their CBDC tokens. This will likely result in financial losses, poor customer experience, and reputational harm. Similarly, validator nodes like licensed banks could encounter remediation challenges or disputes in the event of an account takeover and unauthorized transactions.

Customers accessing their retail CBDC wallets can benefit from fraud prevention technologies like multi-party computation (MPC) and multi-factor authentication (MFA), which are increasingly becoming industry-standard tools to mitigate account takeovers and fraudulent transactions. MPC is a cryptographic technique for securing private keys by distributing responsibility amongst multiple parties (e.g., bank and customer). Coinbase announced MPC support for their wallet-as-a-service offering, and the technology is growing in popularity because of an improved customer experience.[30] In addition, suspicious behavior controls like fraud risk scoring and behavior monitoring at the wallet- and transaction-level could help safeguard customer funds and detect unauthorized access.

Banks may still need help with unauthorized access to customer wallets despite properly managing custodial keys. To address this risk, banks should explore secure methods for sharing sensitive information with required counterparties for account opening and other data-sharing activities. Privacy incident management and robust contingency plans may alleviate risks associated with a breach.

Banks should evolve their risk management processes to safeguard customer information for the digital dollar system design. For example, Coinbase, Fidelity, Kraken, and others are addressing these concerns through TRUST (Travel Rule Universal Solution Technology), a global, secure, and industry-driven solution designed to protect customers.[31] TRUST does not store personal data in a centralized manner; it instead offers proof of ownership on the network to enable secure and trustless transactions. Banks should explore security capabilities like TRUST to reduce the risk of mishandling customer data in a digital dollar system.

---

[30] Coinbase. "Coinbase announces Wallet as a Service."

[31] See generally, Jennifer Lee, TRUST: A solution to crypto's Travel Rule dilemma, Compliance Week (February 22, 2022)

- Federal financial regulators should evaluate the benefits and costs of allowing users to self-custody digital dollars and provide clarity on the legal status of self-custody. Allowing users to self-custody their funds could bolster public trust and enhance financial inclusion [32] – key policy goals for a U.S. CBDC system – but may introduce user risks, including loss of funds without redress and cyber risks. Policymakers should examine these risks and their potential downstream implications on banks when evaluating the merits of digital dollar self-custody.
- When possible, cybersecurity best practices and guidelines, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which offers a flexible risk management approach and should be updated and utilized. [33] Similarly, the FDIC set up a "Banker Resource Center, Information Technology (IT) and Cybersecurity," which can serve as a resource if updated to ensure continued relevance. Both approaches serve as models for cybersecurity frameworks for a digital dollar system. The FDIC also has IT and Cybersecurity resources in its Banker Resource Center.[34]
- Policymakers should consider private sector best practices for custody key security as new guidance, frameworks, and laws are evaluated to address the cybersecurity risks of a digital dollar.

7) Future proofing the architecture through flexibility

As a new form of money, CBDCs should co-exist alongside and complement systems like Fedwire and FedNow to bolster payment resiliency. Moreover, the architecture of a digital dollar system could improve flexibility and agility to benefit the private sector. However, consistent standards and infrastructure are important success factors, and regulatory clarity is necessary for adequate offline payment security and operation.

Secure Infrastructure

All technical infrastructures have some degree of technical risk. A digital dollar system may introduce cybersecurity-related risks associated with nodes, protocols, consensus mechanisms, devices, access points, and ledgers for online and offline transactions. The inherent risks related to a CBDC infrastructure and cybersecurity include but are not limited to a network interface or encryption compromises, malware, distributed denial-of-service (DDoS) attacks, hardware breaches, consensus protocol exploitation (51% attack), and malicious validators.

Banks should evaluate traditional risk frameworks, such as ISO 27001, NIST RMF, and CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), to implement controls for the network infrastructures and interfaces. These frameworks, complemented with a bank-led coordinated and automated risk assessment, will promote early detection of infrastructure-related cyber incidents. Potential factors subject to assessment include users, transactions, disputes, and access points like hardware. Additionally, device security for CBDCs is further explored in the OSTP's September 2022 Technical Evaluation of a U.S. CBDC paper. [35]

---

[32] MIT Digital Currency Initiative, MIT Media Lab, Maiden. "CBDC: Expanding Financial Inclusion or Deepening the Divide? Exploring Design Choices that Could Make a Difference."

[33] National Institute of Standards and Technology. "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to Cybersecurity Framework."

[34] FDIC, Banking Resource Center

[35] See Secure Hardware (pg. 26) in OSTP September 2022 paper

Cybersecurity information-sharing forums (e.g., Financial and Banking Information Infrastructure Committee) may become more important as banks will be expected to facilitate transactions across a wide range of actors. Money transmitters and other non-banks will likely be required to adopt risk management capabilities to interoperate with regulated intermediaries—that is, they will likely be held to bank-like standards when participating in the distribution and transfer of a potential digital dollar because they could be deemed to be acting on behalf of banks or even the central bank.

If the digital dollar system is built on blockchain, nodes can be set up to support infrastructure security. A consensus mechanism built to declare transactions valid could prevent malicious actors from engaging in collusion by blocking invalid transactions to prevent denial-of-service (DOS) attacks. Albeit rare, a 51% attack whereby malicious actors gain control of over 50% of a blockchain's hashing—or processing—power is possible.[36] In parallel, continuous network resiliency testing can serve as a useful mitigant to conduct ongoing monitoring of risks. A digital dollar system should prevent such attacks so that valid transactions from banks and their customers do not become susceptible to reversal or rejection.

Offline Payments

A core benefit of a digital dollar could be supporting financial inclusion by enabling payments to occur when needed. The Bank of Canada reported that offline CBDC payments could improve financial inclusion by offering payment availability regardless of location, system outages, or internet connectivity.[37] Further, the Bank for International Settlements (BIS) recently conducted a survey where 49% of central banks surveyed consider offline payments with retail CBDCs vital, while another 49% considered it advantageous. The study described three modes of offline payments: fully offline, intermittently offline, and staged offline. For details on each model, see the BIS' A handbook for offline payments with CBDC. [38]

While important for improving financial inclusion, offline transactions may introduce new risks, including "flaws in a trusted execution environment" due to a lack of connectedness to the network.[39] Offline digital dollar payments may also be prone to counterfeiting given the lack of connection to a shared ledger and accompanying security control features, fraud detection, and real-time transaction monitoring, which may all challenge banks' ability to conduct transaction investigations.[40] Moreover, offline payments increase the risk that a transaction occurs without the necessary AML/CFT measures.[41]

Offline transactions will likely be needed, and banks should prepare to deter bad actors from exploiting them. Banks should introduce infrastructure controls to protect customers from risky offline transactions. This can include enhancing security controls for phone applications (a possible medium for offline transactions) by requiring MFA. Banks should explore public key cryptography and secure hardware technologies to allow customers to make secure digital payments offline. Likewise, security-enhanced digital wallets should be explored, such as tamper-resistant, trusted hardware chips that facilitate immediate offline settlement.

---

[36] CoinDesk. "What Is a 51% Attack?"
[37] Bank of Canada. A central bank digital currency for offline payments.
[38] Bank of International Settlements. Project Polaris. A handbook for offline payments with CBDC.
[39] The White House. "Technical Possibilities for a U.S. Central Bank Digital Currency."
[40] Erin English, Visa Economic Empowerment Institute, "Finding a secure solution for offline use of central bank digital currencies "
[41] The White House Office of Science and Technology Policy (OSTP), Technical Evaluation for a U.S. Central Bank Digital Currency System

Policy Considerations

- EO 14067 on "Ensuring Responsible Development of Digital Assets" cites the potential of a digital dollar to "support efficient and low-cost transactions" as a primary reason to explore a digital dollar. A tokenized digital dollar could enable instant transaction settlement; however, the irreversibility of transactions caused by instant settlement could pose novel risks for offline transactions.
- Under current law, cash transactions for trade and business over $10,000 must be reported to the IRS. A similar threshold-based framework at various quantitative levels could be considered for a digital dollar for offline transactions.
- The U.S. government should continue engaging with international standard-setting bodies, including the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the Financial Stability Board, the International Monetary Fund, and the Organization for Economic Cooperation and Development (OECD) to explore technical standards related to cross-border interoperability, including the impact of cross-border interoperability on banks' abilities to monitor and detect illicit activity across domestic and foreign bank accounts.
- The Federal Reserve should clarify the controls banks can adopt to ensure safe and secure offline payments.
- Policymakers will need to explore how the design of a digital dollar would allow banks and customers to detect illicit activities committed offline.

8) Continued private sector innovation

A potential digital dollar system should provide a conducive environment for the private sector to innovate and spur economic activity. As such, integrating third parties, including, but not limited to, wallet providers, custodians, and FX providers, comes with several risks that should be understood.[42]

Third-Party Risk Management

Given public sector support for digital dollar interoperability (see 4a, White House Policy Objectives for a U.S. CBDC System), third-party vendors will likely operate across borders to facilitate transactions with other systems and currencies.[43] This regional diversity may challenge the consistency of standards applied to third-party vendors across jurisdictions. Banks should co-develop interoperability standards in public and private forums, such as NIST and ISO, to form a model for engaging with third parties. These standards may include convertibility requirements (discussed above) and system interaction models for on- and off-network protocols. An example of cross-organizational efforts to address technological issues is the Metaverse Standards Forum, a platform for companies to develop interoperability standards for an inclusive and open metaverse.[44] The banking sector should evaluate these efforts and coordinate a cross-organizational approach to coordinating third-party business and technical standards.

---

[42] BIS Project Icebreaker explores the potential role of FX providers in a CBDC system. "Project Icebreaker"

[43] The White House. "Policy Objectives for a U.S. CBDC System."

[44] The Metaverse Standards Forum

Introducing third parties to the network may also invite risks associated with inconsistent third-party risk management practices. This operational risk calls for examining best practices and related guidance for banks to understand and advocate while a digital dollar system is being explored. This presumption of third-party involvement warrants an examination of existing risk management frameworks. One example is the proposed Interagency model by the FDIC, Office of the Comptroller of the Currency (OCC), and the Board of Governors of the Federal Reserve System, which offers six areas for consideration: planning, due diligence, third-party selection, contract negotiation, oversight and accountability, ongoing monitoring, and termination.[45] The potential risks in each area are explored below.

Planning

Bank contingency planning for critical activities outsourced to third parties may be pronounced under a CBDC model. Such planning should manage the transfer of critical activities to another third party or bring them in-house if necessary. Banks should identify substitutable providers to support contingency planning and prepare the secure transition of accounts or assets. Planning should also involve setting third-party data standards and retention requirements. Also, banks can segment partners based on the nature of the services provided and, where applicable, the jurisdictions being served, allowing for managing risk at scale through adjustable controls.

Due Diligence

The novel nature of a CBDC may challenge the performance of due diligence on, and monitoring of highly risk-rated activities provided by third parties. Bank procurement teams, relationship managers, vendor onboarding teams, and others should be educated on the implications of CBDCs on their operations. They may form consortiums for oversight to facilitate open dialogue and optimize group efforts through shared resources like audit results that verify a third party's fulfillment of standards.

Third-Party Selection

As part of the consortiums discussed above, banks may rely on other digital dollar ecosystem participants and their due diligence findings as part of the selection process. Banks can classify third parties into tiers following their selection to form the basis of a due diligence review, as it helps to identify the applicable risk control requirements. Tiering can be based on the third party's risk profile and the degree of their responsibility and criticality. For example, third parties designated the ability to handle customer information, and funds warrant a higher risk profile as funds are at stake.

Contract Negotiation

The distributed nature of a CBDC network may introduce risks related to contracting. For example, a vendor may be onboarded by Bank A, while Bank B may be unsatisfied with the vendor's services. Legal teams can construct agreements to accurately reflect these roles and responsibilities for risk functions to codify risk assessment, monitoring, and mitigation.

---

[45] FDIC. "Proposed Interagency Guidance on Third-Party Relationships: Risk Management."

Oversight & Accountability

Banks have started to enhance third-party risk management teams focused on managing stakeholders, tool distribution, policies, templates, and overseeing program health and reporting. There is a growing focus on defining clear roles and responsibilities and a collaboration model to avoid fragmentation and enhance accountability across the three lines of defense. This oversight and accountability will be more important due to the assumption that a CBDC system will rely on various third-party relationships across products to keep the system running effectively and to incorporate leading-edge technologies.

On-going Monitoring

Banks can manage third-party risk by monitoring using on- and off-network audits and using metrics to evaluate performance against enterprise and industry benchmarks. Banks should audit compliance requirements, including business continuity, disaster recovery, and KYC/AML regulatory obligations, by reviewing policies, procedures, and internal test results of the vendor's activities.

Termination

If a bank has determined to relinquish a vendor's services, third-party termination in a CBDC construct may operate as it does traditionally. Banks will monitor and evaluate issue handling (raised during business-as-usual processes or audits) performance and may off-board third parties when selecting another vendor or bringing processes in-house. Termination may result in the operational risk of system disruptions and can be addressed through testing/troubleshooting for new operating processes.

Policy Considerations

- A digital dollar system may require an increased need for service providers such as custodians, wallet providers, and FX providers. This potential increase in third-party management for banks warrants a re-examination of risk management frameworks, such as the proposed interagency model by the FDIC, OCC, and the Federal Reserve Board. Policymakers should evaluate what elements of existing and emerging third-party risk management frameworks may be applied to a digital dollar.
- Policymakers should consider setting up consortia to periodically assess and share results of industry audits on third-party vendors that can help inform future rules and guidance.

Conclusion

The potential deployment of a digital dollar could offer significant economic and societal benefits. To fully realize these benefits, the private sector must understand and prepare to mitigate new and enhanced risks related to this innovation, with clear guidance from U.S. regulators.

Additionally, the private sector must be engaged by government entities in the research and potential development of a safe, sound, and well-designed digital dollar. Public participation can include public comment, research partnerships, and public-private development, amongst other public engagement tools. With proper mitigation measures in place, banks can address operational and compliance risks and play a key role in ensuring that the benefits of a digital dollar outweigh the risks—however it is more difficult for banks to do so if they are not part of identifying the risks and opportunities from the beginning of discussion.

Amongst other topics out-of-scope for this initial work, future research is needed to fully understand a digital dollar's impacts on fractionalized lending and risks to non-bank institutions such as money transfer operators, payment networks, and non-financial industries.

In the near term, the DDP will share this working paper with policymakers, business leaders, trade associations, and other interested parties. The DDP invites public and private sector leaders to share feedback on this work to promote collaboration in its development. Comments and questions can be sent to info@digitaldollarproject.org.

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 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. For more information on The Digital Dollar Project, please visit https://digitaldollarproject.org.

Acknowledgments

Risk Working Group

The Digital Dollar Project would like to acknowledge the contributions to this work through the expert knowledge and immensely valuable participation of its RWG members.

Accenture

The Digital Dollar Project thanks Accenture for its contributions to conducting research and managing the development of this working paper:

- Duane Block, Accenture Managing Director
- David DeLeon, Accenture Managing Director
- Cameron Nili, Accenture Senior Manager
- Ryan Aykroid, Accenture Manager

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most recent developments. The Digital Dollar Project disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. The Digital Dollar Project does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

For more information on The Digital Dollar Project, please visit https://digitaldollarproject.org.