JIM MIGNANO, DANIEL EGEL, PHOEBE ROSE LEVINE, DANIEL CUNNINGHAM, BRIAN A. JACKSON, JOHN S. HOLLYWOOD, LUCY L. THOMSON, DULANI WOODS

Central Bank Digital Currency Design Choices and Effect on Law Enforcement

This publication has completed RAND's research quality-assurance process but was not professionally copyedited.

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

AN FFRDC OPERATED BY RAND UNDER CONTRACT WITH DHS

This research was published in 2025.

Approved for public release; distribution is unlimited.

About This Report

The Federal Reserve is exploring the creation of a U.S. central bank digital currency (CBDC), a government-backed digital dollar. This report explores the potential impact of a U.S. CBDC on law enforcement's investigative capabilities, leveraging insights from interviews and a scenario-based workshop with law enforcement and financial professionals. The design of a U.S. CBDC—particularly decisions over privacy, transaction history, and the role of the private sector—will affect law enforcement's ability to conduct financial investigations. However, as a U.S. CBDC is likely to be only an evolution (rather than a revolution) in digital assets, new law enforcement techniques are unlikely to be necessary though existing techniques may need to evolve.

This research should be of interest to the Technology Centers Division at DHS; federal, state, local, tribal, and territorial law enforcement; and other United States Government agencies with either investigative responsibilities or responsibilities for the future of a U.S. CBDC.

This research was sponsored by the Technology Centers Division at DHS S&T and conducted in the Infrastructure, Immigration, and Security Operations Program of the RAND Homeland Security Research Division (HSRD), which operates the Homeland Security Operational Analysis Center (HSOAC).

About the Homeland Security Operational Analysis Center

The Homeland Security Act of 2002 (Public Law 107-296, § 305, as codified at 6 U.S.C. § 185) authorizes the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. RAND operates the Homeland Security Operational Analysis Center (HSOAC) as an FFRDC for the U.S. Department of Homeland Security (DHS) under contract 70RSAT22D00000001.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. HSOAC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. HSOAC's research is undertaken by mutual consent with DHS and organized as a set of discrete tasks. This report presents the results of research and analysis conducted under 70RSAT23FR0000074, Central Bank Digital Currency Design Choices and Effect on Law Enforcement. The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information on HSRD, see www.rand.org/hsrd. For more information on this publication, see www.rand.org/t/RRA2952-1.

Acknowledgments

We thank the project sponsor, Dr. Anthony Ayodele and team, for their support throughout the course of this study. We also recognize Special Agent Ryan Mahar for his commitment and support. We thank Dr. Danielle Fenimore, Bob Harrison, Erika Darling, Neysha Alvarez, and Steve Rorabaugh, whose insightful feedback and constructive suggestions significantly enhanced the quality of this research paper.

Summary

Key Findings

- U.S. CBDC design could affect law enforcement efforts to trace flows, identify criminals, and freeze and seize assets.
- New law enforcement techniques are likely unnecessary, but existing techniques may need to evolve.
- Given their experience, technical capabilities, and existing partnerships in detecting and investigating crimes involving digital assets, federal law enforcement agencies are likely to play key roles in addressing CBDC-related criminal activities.
- CBDCs present unique interactions between policy, technology, and criminal activity, creating a dynamic threat landscape and potential concerns regarding individual privacy.

Recommendations

- DHS should be prepared to provide financial and technical support to local law enforcement to manage challenges stemming from the introduction of a U.S. CBDC. This support may include centralized analytical and forensic tools, reporting systems, and education.
- Further analysis should be conducted to address the broader implications of a potential U.S. CBDC on illicit activity because a U.S. CBDC could create new opportunities for criminals and hostile actors.
- Federal law enforcement agencies should collaborate to conduct a privacy impact assessment for a U.S. CBDC to understand how to ensure individual privacy while allowing for lawful access during investigations.

Contents

Figure and Tables

Figure

Tables

Chapter 1. Introduction

The Federal Reserve is exploring the creation of a U.S. central bank digital currency (CBDC), a government-backed digital dollar. The intent in developing and deploying a U.S. CBDC is to facilitate "cross-border transactions…, promote financial inclusion and equity…, foster economic growth and stability, protect against cyber and operational risks, safeguard the privacy of sensitive data, and minimize risks of illicit financial transactions."[1]

Executive Order 14067 on "Ensuring Responsible Development of Digital Assets"—issued in March 2022—provided the first official U.S. mandate for a potential U.S. CBDC, though discussions regarding a potential U.S. CBDC have been ongoing since at least 2016.[2] This executive order, which placed "the highest urgency on research and development efforts into the potential design and development options of a United States CBDC,"[3] gave new urgency to the variety of ongoing public and private CBDC efforts in the United States (see Appendix A) and triggered a series of reports by U.S. federal agencies regarding the future of a U.S. CBDC.

This report explores the potential impact of a U.S. CBDC on U.S. law enforcement's ability to conduct financial investigations. Financial investigations play a critical role in the detection, investigation, and prosecution of financial crimes and a range of other criminal activity, including investment fraud, money laundering, cybercrime, and drug trafficking. As such, policymakers need to understand how a CBDC might impact existing investigative techniques and whether new investigative techniques might be needed.

Historical precedent suggests that a U.S. CBDC could—depending on how it is designed—have significant impacts on the ability of U.S. law enforcement to detect and investigate criminal activity. In particular, recent experiences with cryptocurrency demonstrate that two of the design choices currently under discussion for the U.S. CBDC—(1) a digital asset's relationships with the existing banking system ("intermediation") and (2) the degree and type of privacy—can have

[1] White House, "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets."

[2] Digital Currency Initiative, "Project Hamilton - Building a Hypothetical Central Bank Digital Currency."

[3] Executive Order 14067, "Ensuring Responsible Development of Digital Assets." EO 14067 elaborates:

> These efforts should include assessments of possible benefits and risks for consumers, investors, and businesses; financial stability and systemic risk; payment systems; national security; the ability to exercise human rights; financial inclusion and equity; and the actions required to launch a United States CBDC if doing so is deemed to be in the national interest.

significant implications for law enforcement's ability to trace flows, identify criminals, and freeze and seize assets.[4]

This report provides a focused look at how the range of design choices currently being considered for a U.S. CBDC might impact law enforcement's investigative capabilities. It focuses on answering three core research questions:

1. Which U.S. CBDC design choices are most likely to impact U.S. law enforcement?
2. How will law enforcement need to evolve its capabilities for financial investigations to address new challenges from a CBDC?
3. What types of policies should DHS consider to best posture for the advent of a U.S. CBDC?

This research is not intended to provide a comprehensive assessment of the potential effects of a U.S. CBDC on U.S. law enforcement and criminal activity impacting the United States, but rather an understanding of how U.S. CBDC design choices might affect U.S. law enforcement's ability to conduct financial investigations. The research leverages insights from 27 expert interviews with representatives from private financial organizations and local, state, and federal law enforcement and a scenario-based workshop. The workshop included 17 participants from private finance and law enforcement who discussed the implications of CBDC design for tracing flows, identifying criminals, and freezing and seizing assets through a series of vignettes.

While these methods are known for their capacity to assess the implications of new and emerging technologies,[5] their reliance on the perspectives of a select group of experts and the hypothetical nature of the scenarios discussed may not fully capture the breadth of potential CBDC implementations or unforeseen challenges in law enforcement practices. While we aim to improve the generalizability of our findings by analyzing a variety of scenarios and consulting a diverse set of experts, findings may be limited across different contexts or future developments in CBDC technology and policy.[6] Additionally, while we present a concise discussion of potential criminal adaptations to a U.S. CBDC, a comprehensive analysis of these behaviors is beyond the scope of our study.[7]

The rest of this report is divided into five sections. Section 2 characterizes U.S. CBDC efforts by comparing a U.S. CBDC to existing forms of money and digital assets. Sections 3 and 4 present findings concerning the impact of CBDC design choices on investigative techniques.

[4] Jimenez, "Why Some Criminals Love Crypto"; U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*"; Woods et al., *Cryptocurrency and Blockchain Needs for Law Enforcement*.

[5] Popper, "Foresight Methodology."

[6] While specific to the needs of the United States Secret Service and focused on CBDC design (over law enforcement techniques), Flakoll and Redmond, *Digital Dollars and the Future of Money*, pp. 63–71, discusses an additional set of relevant scenarios.

[7] For an extended discussion of how illicit actors might adapt money laundering techniques to a U.S. CBDC, see Fanusie, *Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them*.

Section 5 considers how investigative techniques may need to evolve to accommodate a U.S. CBDC. Section 6 concludes by offering recommendations for how DHS can best posture to prepare for new risks and opportunities presented by the likely design choices of a U.S. CBDC. Appendix A provides a review of ongoing CBDC efforts; Appendix B details methods used in this study; and Appendix C lists additional CBDC design choices.

Chapter 2. Comparison of CBDCs to Existing Money and Cryptocurrency

CBDCs are digital versions of money that are directly tied to and represent claims on a central bank. This direct connection to the central bank distinguishes a CBDC from digital money provided by commercial banks (such as debit and credit cards) and cryptocurrencies (such as Bitcoin).[8] Despite this difference, existing money and digital assets are the closest available analogs to CBDCs, a useful starting point to explore how a U.S. CBDC might function.

Table 2.1 presents an assessment of cash, commercial bank money, cryptocurrencies and stablecoins, and a potential U.S. CBDC along four characteristics: identity privacy, transaction privacy, ledger history, and the role of private sector intermediaries. To construct Table 2.1, we combined insights from the Office of Science and Technology Policy (OSTP) and expert interviews conducted during this study.[9] Plausible characteristics of a U.S. CBDC are based on the Federal Reserve's assessment that a "U.S. CBDC, if one were created, would best serve the needs of the United States by being privacy-protected, intermediated, widely transferable, and identity-verified."[10]

Table 2.1. Comparison of Cash, Commercial Bank Money, and Digital Assets

Characteristic	Cash	Commercial Bank Money	Cryptocurrencies and Stablecoins	U.S. CBDC
Identity privacy: which entities can access identity-related information and under what circumstances	High	Low	Medium	Medium to High
Transaction privacy: which entities can access transaction information and under what circumstances	High	Medium	Low to Medium	Medium to High
Ledger history: if and how transaction histories are maintained	No	Yes	Yes	Yes or No
Role of private sector: role and identity of third parties in storing funds and facilitating transactions	Low	High	Low to Medium	Medium to High

[8] Commercial bank money includes retail deposit products and services (e.g., debit cards, wire transfers), consumer credit instruments (e.g., credit cards), and digital money backed or otherwise funded by retail deposits (e.g., Venmo). Unlike commercial bank deposits, a CBDC does not require mechanisms like deposit insurance to maintain public confidence. And unlike other digital assets that can be highly volatile or dependent on underlying assets, a CBDC's value would be characterized by stability and government backing.

[9] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

[10] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, p. 2

The comparison in Table 2.1 suggests that important characteristics of a U.S. CBDC would not be entirely new but would resemble a mixture of existing money and cryptocurrency.[11] User identity is highly confidential when using cash, is not kept confidential from regulated commercial banks, and may be kept confidential from crypto services. Cash transactions can be conducted confidentially, whereas banks privately collect and monitor transaction information; many cryptocurrencies disclose transaction information on public ledgers. Unlike cash, commercial banks and crypto systems also retain transaction histories through ledgers. While private sector intermediaries such as exchanges exist in the crypto ecosystem, many cryptocurrencies can facilitate direct ("peer-to-peer") transactions between parties. Cash does not require private sector intermediation.

A U.S. CBDC would enter a crowded market of options for criminals to store and move wealth. Criminal organizations commonly use physical cash for anonymity, despite being logistically intensive to transport. They also use vehicles like retail gift cards to move money discreetly, particularly in cyber fraud. Digital assets, including long established Bitcoin and various stablecoins, are already used in online and offline crimes.[12] Criminal use of digital assets and other online modes for money transfer and laundering is widespread,[13] and utilizes a wide variety of transfer and laundering techniques through different types of digital assets.[14] These digital assets, coupled with crowdfunding platforms and other modes of exchange and collection, have enabled a range of criminal activities, including funding non-state violence and terrorism.[15]

Our analysis of the law enforcement investigation implications of a U.S. CBDC derives in significant part from the past experience of law enforcement and private financial actors in dealing with this criminal behavior. As a U.S. CBDC is likely to resemble a mixture of existing money and cryptocurrency, these CBDC antecedents provide a useful historical database on which to draw insights.

[11] We recognize that some design combinations may lead to a CBDC that looks like something entirely new, for example, a cash-like CBDC that supports programmability, but such designs appear unlikely at present.

[12] Chainalysis, *The 2024 Crypto Crime Report*, p. 7.

[13] Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*.

[14] Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders*.

[15] Financial Action Task Force (FATF), *Crowdfunding for Terrorism Financing*.

Chapter 3. Financial Investigations Involving Digital Assets

Financial investigations, or "following the money," can help law enforcement combat a wide range of criminal activities.[16] A financial investigation's overarching purpose is to "identify and document the movement of money during the course of criminal activity."[17] Financial investigations include detecting illicit financial activities and conducting investigations of financial activities connected to criminal activity. Thus, financial investigations can play an important role in both financial and non-financial crimes.

Law Enforcement Techniques Used in Financial Investigations

Financial investigations encompass three major tasks: (1) tracing flows, (2) identifying criminals, and (3) freezing and seizing assets. Tracing flows involves identifying suspicious patterns and following the path of funds. Identifying criminals involves associating funds with the individuals or entities responsible for criminal activity. Freezing and seizing includes correcting fraudulent transactions, suspending accounts, and recovering victims' funds. Each task is important for gathering evidence that can be used in criminal prosecutions. Table 3.1 provides definitions based on international guidelines and includes examples of each task.

Table 3.1. Three Major Tasks of Financial Investigations

Task	Definition	Examples
Tracing flows	Identifying and following the path of money or other assets to link them to criminal activity and to identify them for freezing and/or seizure	• Using Suspicious Activity Reports to investigate a series of rapid, high-value transactions intended to obscure funds' origins. • Following the transfer of funds across multiple accounts or jurisdictions to identify the financial network of a drug trafficking organization.
Identifying criminals	Associating money or other assets to suspects, including identifying the extent of criminal networks and/or the scale of criminality	• Obtaining a subpoena for bank records to link a suspect to the purchase of materials used in a criminal act. • Identifying the owner of a previously anonymous cryptocurrency wallet involved in ransomware payments.
Freezing and seizing assets	Suspending the movement of, and confiscating, assets obtained through criminal activity to recover victims' assets, deny criminal proceeds, and remove the financial incentive of crime	• Requesting a temporary suspension of bank accounts linked to an active fraud scheme. • Obtaining a warrant to seize specific items used in the context of a theft.

[16] We scope our study to investigations only, excluding prosecution and other stages of the criminal justice process. For example, while law enforcement may need to suspend an account or recover funds during an investigation, we do not cover subsequent legal proceedings such as criminal or civil judicial forfeiture.

[17] FATF, *Operational Issues - Financial Investigations Guidance*, p. 3.

Task	Definition	Examples

SOURCE: Features information from FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations*, p. 109; Brun et al., *Asset Recovery Handbook: A Guide for Practitioners, Second Edition*; Basel Institute on Governance, International Centre for Asset Recovery, *Tracing Illegal Assets: A Practitioner's Guide*.

Law enforcement employs a number of techniques to execute these three tasks. Table 3.2 summarizes these techniques, which are each used across the three major tasks of financial investigations. The first column of Table 3.2 lists categories of techniques that investigators can employ during various phases of financial investigations, while the second provides examples of each category. Note that some categories, such as *Financial Data Analysis*, can apply to both digital and non-digital asset-based investigations. Appendix B provides a more detailed discussion of how we developed this taxonomy of techniques.

The type of crime dictates the investigative techniques and expertise required, with crimes involving digital assets necessitating specialized knowledge in blockchain and digital forensics. A common constraint is that some investigative entities, such as local law enforcement, may not have sufficient resources to investigate certain crimes or employ specific techniques or analyses during an investigation.

Table 3.2. Techniques Used in Financial Investigations Involving Digital Assets

Technique	Examples
Transaction/Activity Monitoring: Observing and analyzing financial transactions to identify red flags	Know Your Customer (KYC); Suspicious Activity Reports (SARs); Currency Transaction Reports (CTRs)
Questioning/Interviews: Formal questioning of victims, suspects, witnesses, and experts	Interviewing bank employees regarding possible fraud; questioning suspects about digital asset use or knowledge
Web Research: Systematically gathering and analyzing information from online sources	Observing dark web activities; reviewing chat forums and social media for digital asset wallet addresses
Financial Data Analysis: Utilizing data analytics to answer investigative questions and meet evidentiary needs	Digital asset tracing; blockchain analysis for attribution or suspect identification; forensic accounting
Asset Recovery: Gathering items or freezing assets related to potential criminal activity	Temporary asset suspensions; seizure of accounts, cash, electronics (e.g., hardware wallets, laptops, phones)
Forensics: Identification, recovery, preservation, communication, and analysis of items gathered	Extracting digital asset wallet stored on hardware; analyzing seed phrase (paper wallet) to reconstitute wallet

Transaction/Activity Monitoring reflects techniques used for observing and analyzing financial transactions to identify "red flags," such as suspicious financial activity. Examples include accessing customer identity information collected by regulated entities such as banks and digital asset exchanges through KYC processes and reports made through SARs and CTRs.[18]

[18] Law enforcement's use of reports such as SARs and CTRs, short of applying formal data analytic techniques, further distinguishes transaction/activity monitoring from financial data analysis, which can involve data analytics.

Questioning/Interviews involves direct, often in-person interactions with victims, suspects, witnesses, and experts. Examples include investigators taking formal steps to interview bank staff regarding a crime or questioning suspects about their use and knowledge of cryptocurrencies or specific illicit financial activities.

Web Research consists of gathering information from online sources like the dark web and social media. Web research can help identify important evidence such as digital asset wallet addresses, which are often posted online. Stolen sensitive personal data posted by threat actors can provide essential evidence for investigators. This category does not consist of persistent monitoring of transactions, nor does it require formal data analysis. In fact, many law enforcement agencies do not have the analytic, technical, or legal capabilities to actively monitor, collect, structure, and analyze data obtained online, often limiting them to qualitative analysis of web research.

Financial Data Analysis covers techniques that utilize data to answer investigative questions and meet evidentiary needs. These techniques involve structured data analysis and exploratory statistical analysis, often utilizing specialized software. For example, law enforcement analysts may use commercial-off-the-shelf software to conduct link analysis to visualize and understand a money laundering network. Private firms have developed proprietary software and tools including blockchain analytics to examine digital asset transactions and provide analytical support to law enforcement.

Asset Recovery involves techniques used for gathering tangible or intangible items related to potential criminal activity. Law enforcement, for example, may obtain a criminal's bank account records through a legal process such as obtaining a subpoena, or may informally request that an exchange temporarily suspend activities on a specific account. This category also includes seizing physical items related to digital assets, such as a perpetrator's computer and other electronics used to conduct illicit cryptocurrency transactions.

Forensics reflects techniques that help law enforcement access, identify, recover, and analyze data and materials. In financial investigations involving digital assets, forensics often aims to capture digital evidence, including after seizing data in the cloud or physical evidence such as a computer or cell phone. Examples include using technical means to access a digital wallet on a perpetrator's device or reconstituting a digital wallet from a seed phrase found on paper.[19]

Illicit and Licit Financial Activities

Financial investigations can involve information about both illicit *and* licit financial activities. Cases involving illicit financial activities focus on criminal uses of funds, including: (1) using funds as a means of payment for—or manner of facilitating—criminal activity; (2)

[19] A *seed phrase* is a set of words generated by a digital wallet that gives users access to the funds within the wallet. It can be used to restore a digital asset wallet, providing access to the private keys and addresses in that wallet.

using funds to conceal illicit financial activity; and (3) crimes involving or undermining the money system.[20] Table 3.3 provides examples of illicit financial activities involving digital assets.

Table 3.3. Illicit Financial Activities Involving Digital Assets

Activity	Examples
Using funds to pay for—or facilitate—crime	Buying or selling illegal goods or services, ransomware, extortion, human trafficking, terrorist financing
Using funds to conceal illicit financial activity	Money laundering, tax evasion, sanctions evasion
Crimes involving—or undermining—the money system	Counterfeiting, fraud and theft, heists, "cryptojacking"[a]

SOURCE: Features information from U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, pp. 4–9.
NOTE: [a] *Cryptojacking* is a type of cyberattack in which a hacker uses a victim's computer or other device to mine cryptocurrency without their knowledge or consent.

Information about licit financial activities is often used in financial investigations when law enforcement has already identified a suspect and when such financial information provides valuable context to their investigation. For example, if a suspect is known to have legitimate employment income but is also making large deposits or transfers inconsistent with their reported income, this could indicate illicit financial behaviors.

Interagency and International Collaboration in Financial Investigations

Throughout the investigative process, lead agencies often collaborate with multiple domestic and international entities, including other law enforcement agencies, government bodies, and private sector organizations. This collaboration is important given the multi-jurisdictional nature of many financial investigations, especially those involving digital assets.[21]

Specialized agency offices and interagency task forces may also be involved depending on the type and prevalence of the crime under investigation. For example, the FBI frequently collaborates with the Securities and Exchange Commission, IRS Criminal Investigation, and FinCEN to investigate white-collar and other financial crimes, as well as with DHS's Homeland Security Investigations and U.S. Secret Service, the Drug Enforcement Administration, state, local, tribal, and territorial law enforcement agencies on a variety of crimes that have financial dimensions.[22] The U.S. Secret Service's Global Investigative Operations Center specializes in

[20] Taxonomy of illicit financial activity adapted from U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, pp. 4–9.

[21] For example, blockchain tracing is an important aspect of financial investigations with blockchain-based digital assets. It involves tracking transactions on blockchain networks to identify the movement of digital assets, which requires technical expertise and specialized tools to analyze blockchain data effectively.

[22] Federal Bureau of Investigation, "White-Collar Crime."

analysis of “non-traditional data sources,” including blockchain analytics, to support interagency and international investigations.[23]

Financial investigations with international aspects require coordination across jurisdictions and navigating different legal frameworks. The exchange of information and evidence between countries becomes a critical challenge, especially as some foreign entities do not cooperate fully with U.S. law enforcement agencies. The involvement of offshore entities, cross-border fund transfers, and the use of international financial institutions further exacerbate the challenges. In response, investigative efforts require a high degree of sophistication, involving international partnerships, mutual legal assistance agreements, and sometimes leveraging of specialized international organizations such as INTERPOL.

[23] U.S. Secret Service, “Cyber Investigations.”

Chapter 4. U.S. CBDC Design Choices Most Likely to Impact Law Enforcement Investigations

This section is focused on addressing the first core research question: "Which U.S. CBDC design choices are most likely to impact U.S. law enforcement?" To do this, we focus on the inventory of 18 CBDC design choices policymakers should consider published by OSTP.[24] We used a two-step process to identify which of these design choices are likely to be most salient to law enforcement investigations.

We first evaluated the detailed descriptions of each OSTP-enumerated design choice for whether they discuss law enforcement or adjacent keywords (i.e., privacy, anti-money laundering and countering the financing of terrorism [AML/CFT] compliance, system security, consumer protection). Doing so identified seven design choices with three or more references to these keywords: (1) identity privacy, (2) transaction privacy, (3) intermediation, (4) ledger history, (5) transaction programmability, (6) offline capabilities, and (7) secure hardware. Next, we validated this list through our interviews, asking interviewees to discuss other design choices relevant to financial investigations. This resulted in the inclusion of one additional design choice: cryptography.

Table 4.1 summarizes these eight design choices and our assessment of their relevance to law enforcement. A more detailed discussion of each of these eight design choices is provided below the table and Appendix C describes the excluded design choices.

Our assessment of law enforcement relevance is based on OSTP's discussion of each CBDC design choice. We focus on the four OSTP criteria that our interviews indicated to be of greatest relevance to law enforcement investigations. Other OSTP criteria—such as "financial stability," "systemic risk," and "payment system efficiency"—are important for the overall financial system's health but not relevant to law enforcement. The four criteria that we used can be summarize as follows:

- Privacy: Refers to the protection of personal information from unauthorized access or disclosure, as well as against "arbitrary or unlawful surveillance." Design choices with privacy implications may impact law enforcement's ability to access CBDC data to detect illicit activities and conduct investigations.[25]
- AML/CFT compliance: Involves regulations and procedures that financial institutions and other private sector service providers must follow to help law enforcement detect and investigate money laundering and terrorist financing.[26]

[24] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

[25] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, p. 10.

[26] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, p. 9.

- System security: Refers to the protection of the CBDC infrastructure from cyber threats and unauthorized access. CBDC design can help prevent or mitigate counterfeiting, fraud, hacking, and other cybercrimes.[27]
- Consumer protection: Involves safeguarding the public from unfair, deceptive, or fraudulent practices. Design choices with consumer protection implications may affect the agencies responsible for enforcing these protections and addressing violations.[28]

Table 4.1. CBDC Design Choices Most Relevant to Law Enforcement

Design Choice	Privacy	AML/CFT Compliance	System Security	Consumer Protection
Identity privacy: which entities can access identity-related information and under what circumstances	X	X		
Transaction privacy: which entities can access transaction information and under what circumstances	X	X	X	
Intermediation: role and identity of third parties in facilitating transactions and managing wallets	X	X	X	
Ledger history: if and how CBDC transaction histories are maintained	X	X		X
Transaction programmability: whether third parties can code self-executing rules into the CBDC system	X		X	X
Offline capability: if and how CBDC transactions can occur without connection to the transaction processor	X	X	X	
Secure hardware: if and how the CBDC system prioritizes a hardware-based approach to security	X	X	X	
Cryptography: mathematical techniques used to encode sensitive information	X	X	X	

SOURCE: Features information from OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.
NOTE: Identity privacy is included as the only design choice with direct references to "law enforcement" and "crime" in OSTP (pp. 20–22). Cryptography is included because, according to an expert interviewed for this study, cryptographic design choices are fundamental to CBDC system security.

Identity privacy: The extent to which identity-related information is accessible to the central bank, intermediaries, and law enforcement. Wallet issuance will likely require some collection of personally identifiable information for Know Your Customer (KYC) compliance. Legal procedures for law enforcement to obtain this data will depend on the issuer. To access identity information associated with private sector intermediary issued CBDC wallets, legal procedures could resemble existing processes, but central bank issued wallets would likely require the development of new policies and procedures.

Transaction Privacy: Which entities can view the ledger history and associated information (which could include payment addresses, account balances, user locations, information about

[27] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, p. 8.

[28] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, pp. 7, 51.

goods, and smart contract code) and under what circumstances. As such, transaction privacy intersects with the intermediation, ledger history, cryptography, and programmability design choices, but also incorporates the legal processes which law enforcement authorities must navigate to access the resulting transaction data.

Intermediation: The extent to which third parties are involved in facilitating transfers and managing user accounts.[29] Possible intermediation functionalities include distributing currency, wallet creation and custody, validating and settling transactions, KYC, conducting fraud detection, AML/CFT compliance measures, resolving disputes, customer service, and user interfaces.[30] A less intermediated system would support some peer-to-peer transactions, while a more intermediated system would entail increased involvement from banks or money service businesses. A CBDC could support a spectrum of intermediation, where different transaction types require various levels. The Federal Reserve has indicated that a retail U.S. CBDC would involve private sector intermediation, at least for account opening and management.[31]

Ledger History: The existence and structure of a transaction ledger. Transactions could be recorded on a centralized ledger hosted by the central bank, or a decentralized ledger with trusted intermediaries operating different nodes. Trusted intermediaries could obtain write access to a centralized ledger in an intermediated CBDC system by completing a verification process. Ledger history could be maintained permanently, temporarily to allow for remediation or AML/CFT compliance measures, or not at all.

Transaction Programmability: Whether and under what circumstances third-party smart contracts would be supported. "Smart contracts" are rules coded into the CBDC system that execute when a set of predefined conditions are met. While some smart contracts could automate compliance and enforce transaction-level rules, which may decrease the level of law enforcement effort needed, others might enable new methods of concealing illicit activities. Approved use cases, entity screening for development, quality review processes for deployment, and on-ledger visibility of smart contract execution and data inputs could all vary greatly. Many cryptographic methods under development seek to preserve the privacy of smart contract data inputs.[32]

Offline capability: Whether and under what circumstances CBDC transactions can occur without live connection to the online transaction processor. Offline transactions would be conducted in trusted execution environments, which could be supported by software or hardware solutions. Time spent offline could vary: CBDC could be exchanged offline indefinitely, or

[29] OSTP uses the term "transport layer" to refer to the presence and role of intermediaries in a CBDC system.

[30] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*

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

[32] Bernal Bernabe et al., "Privacy-Preserving Solutions for Blockchain: Review and Challenges."

require users to reconnect to the system at certain transaction intervals or limits. Technical innovations to facilitate secure offline transactions are still under development.[33]

Secure hardware: A CBDC system can prioritize hardware- or software-based approaches for its security. Secure hardware involves using specialized equipment (e.g., hardware wallet, smartphone component) to protect CBDC data and computation. Software may be used as an alternative to—or in conjunction with—secure hardware to protect CBDC data and computation.

Cryptography: Mathematical techniques used to protect data throughout the CBDC system, especially data recorded on the transaction ledger. A common approach to transaction ledger cryptography is public-key cryptography (PKC), in which users have a private key to authorize payments and a public key (derived from the private key) to receive funds.[34] On a more transparent ledger, as with Bitcoin, the sender's wallet address (a hash of the sender's public key),[35] the recipient's wallet address (a hash of the recipient's public key), and the transaction amount are publicly visible. Even though wallet addresses are pseudonymous, it is sometimes possible to connect the address to an identity using transaction data.[36] A CBDC ledger could layer PKC with zero-knowledge proofs (ZKPs) to offer more private transaction options in which users never have to reveal their public address on-ledger or input their private key to the network.[37] ZKPs could also simplify legal aspects of certain investigative processes by allowing investigators to check whether a statement about an account is true without viewing any data associated with the account.[38]

[33] Bank for International Settlements, "Project Polaris: Secure and Resilient CBDC Systems, Offline and Online."

[34] Transactions are authorized using digital signatures cryptographically generated from the sender's private key in conjunction with information unique to the transaction.

[35] A *hash* is a cryptographic function that converts an input (such as a transaction or data) into a fixed-size string of characters, which serves as a unique identifier for that input.

[36] Berentsen, Lenzi, and Nyffenegger, "An Introduction to Zero-Knowledge Proofs in Blockchains and Economics."

[37] Zcash is an example of cryptocurrency that employs ZKPs. Transactions on the Zcash ledger display combined hashes of each address, transaction amount, and a unique transaction serial number alongside a ZKP which verifies that the sender possesses the private key to that set of funds. As a result, the network does not store (or in the case of the private key, even see) any information that could be traced back to an identity.

[38] Bernal Bernabe et al., "Privacy-Preserving Solutions for Blockchain: Review and Challenges."

Chapter 5. New Law Enforcement Techniques Are Likely Unnecessary, But Existing Techniques May Need to Evolve

This section presents the outcomes of a one-day workshop organized to examine the second core research question: "How will law enforcement need to evolve its capabilities for financial investigations to address new challenges from a CBDC?"

Table 5.1 provides a top-level summary of the types of innovation in financial investigative techniques that may be necessitated by a U.S. CBDC, as indicated by workshop participants. As discussed in Section 2, from a law enforcement perspective a U.S. CBDC is likely to resemble a mixture of existing money and cryptocurrency. Consequently, a U.S. CBDC is not likely to necessitate entirely new investigative techniques because it is unlikely to differ substantially from the types of financial assets familiar to law enforcement.[39]

Table 5.1. Summary of Potential Changes to Investigative Techniques a U.S. CBDC Might Require

Technique	Example Change(s) Needed
Transaction/Activity Monitoring	• Higher volumes of Bank Secrecy Act / Anti-Money Laundering (BSA/AML), police, and victim reports could necessitate more integrated and automated reporting and monitoring systems to accommodate a U.S. CBDC.
Questioning/Interviews	• No specific changes identified.
Web Research	• No specific changes identified.
Financial Data Analysis	• Certain ledger history characteristics would necessitate adaptations to analytic tools and approaches. • Programmability could enable new analytic tools and approaches while necessitating more personnel specialized in "smart contract analysis."
Asset Recovery	• The Federal Reserve could play a role in assisting with the expeditious recovery of victims' funds, but new legal and policy frameworks may be needed. • Increasing asset recovery needs could prompt adjustments to law enforcement priorities.
Forensics	• No specific changes identified.

Workshop Approach for Assessing Impact of Design Choices

To explore the potential impact of a U.S. CBDC on law enforcement's ability to detect and investigate criminal activity, we conducted a one-day scenario-based workshop on April 4,

[39] The effect on law enforcement depends on whether malicious actors would choose to use the CBDC for criminal activity over other available financial assets, which is difficult to predict.

2024.[40] The workshop was designed to assess the need for new law enforcement techniques in the context of a U.S. CBDC and involved 17 participants from law enforcement, the U.S. government, commercial organizations, and academia. Workshop participants were recruited based on their diverse viewpoints on digital currencies; their professional qualifications and experience in areas such as financial investigations, digital assets, and blockchain analytics; and included representatives from federal, state, and local law enforcement.

Through three scenario-based discussions, participants engaged in a structured process that included the presentation of scenarios, quantitative impact assessment, and facilitated discussion. The future-oriented scenarios were based on recent cases that highlight different types of crime (i.e., crypto investment scheme, money laundering, and large-scale cyber heist) and different types of funds (i.e., digital assets, cash, and commercial bank money). The cases were selected to (1) assess the impact of CBDC design choices on financial investigations, and (2) determine whether a U.S. CBDC would require new investigative techniques. Appendix B provides further information about each scenario.

The focus of each scenario was an assessment—initially quantitative and then followed by a qualitative discussion—of the level of law enforcement effort needed to investigate the case had it involved a hypothetical U.S. CBDC. Each scenario focused on the same hypothetical U.S. CBDC with eight specific characteristics, each aligned with one of the eight design choices identified in our initial review of OSTP's design choices (see Section 4):

- **High identity privacy** keeps identity information (e.g., payment addresses) confidential.
- **High transaction privacy** limits access to sensitive data for legal reasons only.
- **Not intermediated by regulated financial institutions** allows for peer-to-peer transactions.
- **Ledger history neither created nor maintained** by using a smart card system to store digital currency values (e.g., mobile phone SIM cards) rather than a ledger.
- **Transaction programmability supported**, enabling third-party smart contracts.
- **Full offline compatibility** allows for transactions without connection to the CBDC system.
- **Secure hardware prioritized** (e.g., through hardware wallets).
- **Public-key cryptography with zero-knowledge proofs** used to secure CBDC information.[41]

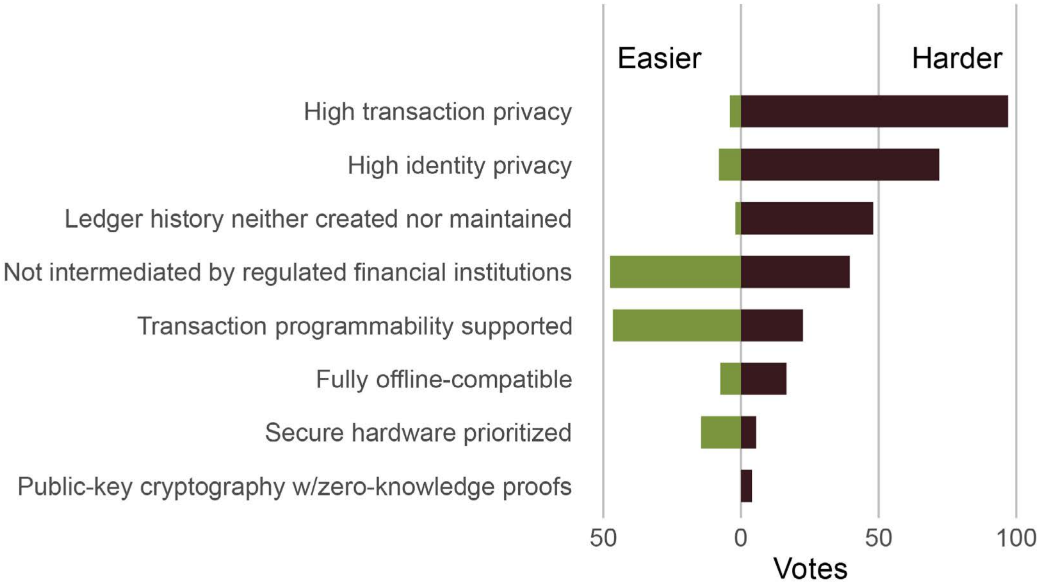
[40] The workshop was held in person at RAND's office in Arlington, Virginia. Two researchers facilitated the workshop, two researchers took notes for later thematic analysis by the research team, and four additional researchers attended as observers. Three members of the project sponsor's team also attended.

[41] The list of design choices presented during the workshop includes two design choices omitted from the final list of design choices most relevant to law enforcement. See Appendix B for details.

Overall Impact of a U.S. CBDC on Financial Investigations

Figure 5.1 summarizes the overall assessment of the relative importance of the eight CBDC design choices that emerged from the scenario-based workshop. The magnitude of the bars is indicative of the relative importance of each of these design choices, as measured by the workshop participants' assessment of whether a design choice would affect the difficulty of conducting law enforcement investigations. Participants were allowed to indicate that a design choice would either increase or decrease the overall difficulty of conducting law enforcement investigations compared to the cases examined during the workshop. This figure reports the total number of "votes" that each option received.

Figure 5.1. Results of Exercise to Estimate the Level of Effect on Law Enforcement



NOTE: This figure presents final assessment votes tabulated for "less effort" (i.e., "Easier") and "more effort" (i.e., "Harder"). Each participant had eight votes to place wherever they preferred (including more than one vote in a single category) per scenario. In addition to the 17 workshop participants, three observers from the sponsor's team voted, resulting in a total of 480 possible votes. Fifty votes for "no change" are not presented here, including 16 votes for high identity privacy, 15 for fully offline-compatible, and eight for high transaction privacy; other design choices had negligible numbers of votes for "no change."

Workshop participants largely assessed the design choices "high transaction privacy," "high identity privacy," and "ledger history neither created nor maintained" as likely to complicate financial investigations. High transaction privacy and high identity privacy inherently limit the visibility of transaction details and the identities of those involved, making it challenging for law enforcement to trace illicit activities or verify the parties in transactions. The nature of ledger history, depending on how it is maintained or not, could further obscure financial trails, hindering efforts to investigate and understand the flow of funds. These features, while enhancing privacy, could pose challenges to investigative techniques, requiring more effort from law enforcement to achieve the necessary level of insight into financial activities.

The design choices "not intermediated by regulated financial institutions" and "transaction programmability supported" were assessed with mixed results. Some workshop participants interpreted the absence of intermediation to mean the Federal Reserve would directly manage the CBDC system, while others interpreted it to mean facilitating peer-to-peer exchange akin to Bitcoin. Either case might simplify transaction monitoring and reporting while complicating the existing legal framework. Workshop participants discussed transaction programmability as potentially working in two directions: it could enable new tools and approaches while necessitating more specialized skills to investigate crimes that exploit programmability in innovative ways.

The remaining design choices concerning offline compatibility, secure hardware, and cryptography were assessed to have limited impact on the level of law enforcement needed. Discussions that ensued during the workshop did not suggest these design choices were unimportant but indicated that they would not materially change the underlying techniques involved in financial investigations or the policy framework within which these techniques operate.

Impact of U.S. CBDC Design Choices on Law Enforcement Tasks

Several workshop participants indicated that a U.S. CBDC could significantly increase the volume of reports related to BSA/AML (e.g., SARs, CTRs), police investigations, and victim complaints. Participants indicated that such a surge in data would necessitate developing more integrated and automated systems for reporting and monitoring financial transactions. Examples identified include user-friendly software enhanced with artificial intelligence to assist local law enforcement report suspicious CBDC activity and monitor results, as well as a CBDC mobile phone app with a simple feature to conveniently report potential crime. Artificial intelligence may facilitate continuously monitoring various data sources for suspicious activities. It could "use machine learning algorithms to examine large datasets, anticipate future crimes, locate crime hotspots, and propose solutions. AI can also compare data to find connections between incidents that may seem unrelated, helping to solve crimes."[42]

The workshop highlighted how stored ledger history could support financial data analysis by providing a comprehensive record of transactions. This capability would allow for enhanced tracing and analysis of financial activities, potentially identifying patterns indicative of criminal behavior. Adapting to these characteristics might require new or upgraded analytic tools and approaches—such as the use of artificial intelligence as described above—to manage, process, and interpret vast amounts of data the ledger would contain.

[42] Lukens, "An Introduction to How AI is Transforming Real Time Crime Centers."

A programmable CBDC would enable "smart contracts" that automatically execute under certain conditions. Malicious actors could exploit vulnerabilities in smart contract code to conduct fraud and theft and could deploy smart contracts to create complex transactions that are difficult to trace, obfuscating illicit financial flows. New analytical tools and professionals skilled in smart contract analysis would be needed to detect and investigate such illicit activities.[43] This analysis would involve both monitoring smart contracts for suspicious transactions and conducting in-depth analysis of the underlying smart contract software code. This dual focus stems from the automated nature of smart contracts, which requires an understanding of both the outcomes they produce and the specific conditions and logic programmed into their code to identify and mitigate potential abuses.

While intermediaries would provide the public interface for a U.S. CBDC, the government might take advantage of new technical tools to ensure the swiftest possible recovery of victims' funds. Workshop participants suggested that the challenge here would be more legal than technical in nature: new legal and policy frameworks would be needed to define the Federal Reserve's authority and procedures for collaborating with law enforcement agencies and intervening in cases of crime. Furthermore, as the adoption of a CBDC could lead to an increase in the need for asset recovery, law enforcement agencies may need to adjust their priorities accordingly. Workshop participants discussed how this adjustment could involve allocating more resources—or shifting them—toward the recovery of stolen or lost CBDC.

Workshop participants did not specify necessary adjustments to questioning/interviews, web research, or forensics. However, if a U.S. CBDC differs substantially from existing money and cryptocurrency, investigators might need to modify their questioning and interviewing techniques to address technical distinctions. Additionally, as threat actors evolve methods to hide illegal activity, investigators may need new technological expertise and tools to effectively locate, document, and gather evidence.

A general agreement among participants was that the unforeseen impacts of CBDC characteristics could necessitate unexpected changes to law enforcement techniques, and participants recommended that CBDC research and development be continuously monitored to prepare for potential adjustments.

[43] A workshop participant identified the importance of legal expertise alongside technical knowledge. Further research may be necessary to understand the legal ramifications of smart contract analysis but is beyond the scope of this study.

Chapter 6. Roles for DHS in Supporting U.S. Law Enforcement for a U.S. CBDC

This final section draws on the findings from this study to explore the third core research question: "What types of polices should DHS consider to best posture for the advent of a U.S. CBDC?" Each of these policy recommendations should be treated as concepts for consideration, as the development and assessment of policy options was a not a central focus of this limited, exploratory study.

Recommendation 1: Prepare to Provide Financial and Technical Support to Local Law Enforcement

Introducing a U.S. CBDC could change the landscape of financial investigations, particularly in terms of the volume and nature of data accessible to law enforcement agencies. If widely adopted, an influx of new data generated by CBDC transactions could overwhelm investigators, especially during early stages of implementation when the learning curve is steep. This challenge is anticipated to be particularly impactful at the state and local levels, both because resources are often limited—particularly access to advanced analytic capability and appropriately trained personnel—and there is potential for significant low-level criminal activity associated with a U.S. CBDC.

DHS should be prepared to help local law enforcement manage these new challenges. This could include expanding modalities for collaboration between federal, state, and local law enforcement in investigations in which digital assets are used, such as services offered by the U.S. Secret Service's Global Investigative Operations Center. In addition, DHS could take steps to improve the capacity and capability of local law enforcement for these types of financial investigations, through focused training, increasing access to analytical and forensic tools for digital asset investigations, and enhancing federal reporting systems to streamline reporting of cross-jurisdictional criminal activities.

Recommendation 2: Conduct Assessment of How a U.S. CBDC May Impact Criminal Activity

The effect on law enforcement of introducing a U.S. CBDC depends on how criminals react to the availability of the new digital currency. It is likely that a U.S. CBDC will create new opportunities for crime. Existing private digital asset systems can be vulnerable to large-scale thefts, and because a U.S. CBDC system would be government-backed, it might also attract attention from other actors (e.g., hostile states).[44] The novelty and ease of using a CBDC could also facilitate an increase in small-scale frauds and thefts, as well as efforts targeting specific populations (e.g., elder fraud).[45]

In addition, a U.S. CBDC may offer an attractive new medium for criminals to store and move wealth. Criminal organizations use a wide array of financial instruments to store and move wealth including physical cash, which offers the greatest anonymity but is logistically intensive to transport; retail gift cards; and a wide array of digital assets. While a U.S. CBDC would enter a crowded market of options for criminals to store and move wealth, it has the potential to increase the number of offramps available to criminals, particularly if there is widespread adoption of the CBDC.[46] A focused assessment of how criminal activity might adapt to a U.S. CBDC could help prepare law enforcement. This assessment could help identify the specific types of capabilities that federal and local law enforcement might require to respond to the new threats and new mechanisms for moving and storing wealth. Such an analysis could also inform the design of a potential U.S. CBDC by helping detail how specific design choices are likely to impact criminal activity and the requirements for the law enforcement community.

Recommendation 3: Conduct Law Enforcement-Focused Privacy Impact Assessment of a U.S. CBDC

The Federal Reserve has committed that a U.S. CBDC would be "privacy-protected" and "identity-verified."[47] Understanding how to ensure privacy while allowing for lawful access during financial investigations was highlighted as a priority during both project interviews and the stakeholder workshop.

One approach for developing such an understanding would be for federal law enforcement agencies to collaborate in conducting a privacy impact assessment (PIA) for a U.S. CBDC. PIAs are important tools to ensure that privacy safeguards align with government policy requirements and public expectations, and can help federal agencies and third party entities identify, assess, and mitigate privacy risks.

Law enforcement could leverage a CBDC-focused PIA process to understand the extent of identity privacy (i.e., confidentiality of identity-related information) and transaction privacy

[44] Egel et al., *Central Bank Digital Currencies and U.S. Strategic Competition with China*.

[45] Cryptocurrency scams targeting those over 60 years of age highlight the issue, with reported losses from such frauds exceeding $1.1 billion in 2023, over 32 percent of total reported losses of $3.4 billion for this age group (Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, *2023 Elder Fraud Report*, pp. 5, 16).

[46] An *offramp* is a means of exchanging digital assets for existing money. A widespread, easily convertible U.S. CBDC could inadvertently provide criminals with more opportunities to launder money and integrate it into the regulated financial system. We thank Erika Darling for this observation.

[47] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, p. 2.

(e.g., confidentiality of information about account balances, user location, smart contract code and inputs), as well as privacy risks with third party access to and use of the personal and financial data (e.g., law enforcement, vendors, financial and business partners such as commercial banks and money service businesses).[48] Such a PIA could also help evaluate if a U.S. CBDC would impose additional BSA/AML compliance burdens on the private sector, along with ways to ease this burden, and set the limits for requirements and technical options to track and monitor CBDC activities.

[48] For information about measures to mitigate privacy risks, see White House, “Privacy” and Office of Management and Budget, Circular No. A-130, “Managing Information as a Strategic Resource,” App. II, Section 5(e). For examples of PIAs for financial systems, see Federal Deposit Insurance Corporation, “Privacy Impact Assessments (PIAs),” Internal Revenue Service, “Privacy Impact Assessments - PIA,” and Financial Crimes Enforcement Network, U.S. Department of the Treasury, “Privacy Impact Assessments.”

Appendix A. Background on CBDC

Central banks around the world are exploring the feasibility of CBDCs. As of March 2024, "134 countries and currency unions, representing 98% of global GDP, are exploring a CBDC," over half of which are in advanced stages of development, including pilot programs and public launches.[49] Interest in CBDCs underscores their potential to support faster, cheaper, more secure, and more accessible payments for the general public and businesses alike.

Central banks, finance ministries, international financial institutions, and industry groups are spearheading CBDC research and development. This encompasses technical design choices as well as policy considerations essential for CBDC implementation. Efforts underway outside the United States provide valuable insights into CBDC design. For example, the European Central Bank's digital euro project has been prolific in publishing policy analyses and experimental results regarding design choices concerning privacy preservation, transaction speeds and scalability, and interoperability with existing financial infrastructure.[50] China's electronic yuan (or e-CNY) pilot is the world's largest active CBDC project, and China has been testing a platform to make its CBDC interoperable with foreign currencies.[51] The Bank for International Settlements—also known as the bank for central banks—has helped coordinate over a dozen technical CBDC experiments, focused on how CBDCs could work across multiple jurisdictions.[52]

U.S. CBDC Research and Development: An Active but Cautious Approach

Federal CBDC research and development reflects an active but cautious approach. Executive Order 14067 "places the highest urgency on research and development efforts into the potential design and development options of a United States CBDC."[53] Executive Order 14067 prompted the 2022 report, *The Future of Money and Payments*, which explores the potential effects of a U.S. CBDC on national economic interests, financial inclusion, its relationship with private digital assets, and a number of foreign policy and national security concerns.[54]

[49] Atlantic Council, "Central Bank Digital Currency Tracker."

[50] European Central Bank, "Technical Documents and Research."

[51] Egel et al., *Central Bank Digital Currencies and U.S. Strategic Competition with China*.

[52] Bank for International Settlements, "BIS Innovation Hub Work on Central Bank Digital Currency (CBDC)."

[53] Executive Order 14067, "Ensuring Responsible Development of Digital Assets."

[54] U.S. Department of the Treasury, *The Future of Money and Payments*.

The Federal Reserve indicates it will not issue a CBDC "without clear support from the executive branch and from Congress, ideally in the form of a specific authorizing law."[55] However, the Fed and its banks have engaged in research to understand the potential implications of a U.S. CBDC. The Fed initiated a public dialogue in 2022 about the benefits and risks of a U.S. CBDC (see "Public Sentiment about a U.S. CBDC…" below).[56]

Motivations for Issuing a U.S. CBDC

Governments worldwide are exploring CBDCs for a range of economic and strategic objectives. A common motivation is to enhance financial inclusion, making it safer and easier for more consumers to access and use central bank money. This is especially true as the use of physical cash declines and where informal or unregulated financial alternatives are on the rise. Another common set of motives is to foster competition, efficiency, and resilience in domestic and cross-border payments. CBDCs also open present opportunities for financial innovation, such as employing programmable money to improve transparency in government payments or introducing new tools to support monetary policy.[57]

U.S. CBDC Projects

One key research initiative is Project Hamilton, led by the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology. Project Hamilton designed an experimental CBDC transaction processor to meet the requirements of a "large retail payment system."[58] The work led to OpenCBDC, an open source project that allows for further experimentation with added functionalities such as programmability.[59]

Another key effort is the Federal Reserve Bank of New York's Project Cedar. Project Cedar began with a prototype CBDC ledger for cross-border payments, evolving into a partnership with the Monetary Authority of Singapore to demonstrate the feasibility of near real-time, secure payments and settlements across multiple ledgers.[60]

By comparison, the private sector in the United States has been more active in CBDC research and development. The nonprofit Digital Dollar Project regularly hosts experiments and

[55] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, p. 3.

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

[57] Atlantic Council, "Central Bank Digital Currency Tracker."

[58] Federal Reserve Bank of Boston, *Project Hamilton Phase 1: Executive Summary*.

[59] Lindsay, "Boston Fed, MIT Complete Research Project into Feasibility of a Central Bank Digital Currency."

[60] Federal Reserve Bank of New York, "Project Cedar: Improving Cross-Border Payments with Distributed Ledger Technology."

working groups to explore the implications of “both private and public digital currency networks,” including CBDCs, stablecoins, and other digital assets.[61] Private sector digital asset efforts can also inform the design and potential applications of a U.S. CBDC, offering examples of proven technology and customer needs. For example, cryptocurrencies such as Bitcoin and Ethereum can provide lessons on the security and scalability necessary for a CBDC, as well as insights into how “smart contracts” could enhance CBDC functionality.[62] Stablecoins such as USD Coin (USDC) and Tether can provide insights into user demand, technology adoption, and potential use cases that can inform the design of CBDCs.

Public Sentiment about a U.S. CBDC Ranges from Enthusiasm to Alarm

The Fed’s *Money and Payments* paper invited public comment regarding the pros and cons of issuing a U.S. CBDC.[63] Supportive comments reinforce the motivations described above. Concerns about a U.S. CBDC include the potential to:

- widen the ‘digital divide,’ particularly for elderly and low-income individuals who may lack reliable internet and phone access,
- shift deposits out of commercial banks, potentially reducing the availability of and raising the cost of credit, and
- exacerbate concerns about privacy and mistrust of government.[64]

A tension related to this third concern is notable for this study. Some commenters “highlighted the potential of a CBDC to promote transparency and reduce illicit activity,” while others “expressed strong concerns about how user data would be protected from unauthorized surveillance.”[65]

Some commenters also identified alternatives to a CBDC they thought would better achieve at least some desired outcomes, such as modernizing the existing payment system and improving the regulatory environment to support private sector innovations like stablecoins. Another theme distinguished retail from wholesale CBDCs, suggesting that a wholesale CBDC “could achieve a

[61] Digital Dollar Project, “Leading the Discussion on Future of the US Dollar.”

[62] *Smart contracts* are self-executing agreements with terms directly written into code, automatically enforcing and executing actions when predefined conditions are met.

[63] The Fed received 2,050 submissions from “financial institutions, technology companies, trade organizations, consumer groups, congressional representatives, and individual private citizens” (Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*, p. 3).

[64] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*, pp. 6–7. This list is for illustrative purposes and is not exhaustive.

[65] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*, p. 9.

narrower set of benefits…without creating broader risks such as disintermediation of the financial sector and risks to individual privacy."[66]

[66] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*, p. 10.

Appendix B. Research Methods

This study employed multiple methods to accomplish three core research tasks. This appendix describes the methods used over the course of this study.

Task 1: Review CBDC Design Choices

We began with a literature scan of 43 U.S. government and international institution reports, academic papers, industry publications, and news articles related to CBDC design and relevant private sectors efforts published since 2020. We compiled these sources starting with government reports issued pursuant to Executive Order 14067 and identified additional references from those reports. We supplemented these sources by a targeted search on Google Scholar using the terms “CBDC” and “law enforcement,” excluding results that did not directly address CBDC design choices and their implications for U.S. law enforcement. This scan aimed to synthesize a broad spectrum of the current state of understanding about CBDC design.[67]

Next, we compared possible CBDC characteristics with cash, commercial bank money, and cryptocurrency. This comparison focused on identifying similarities and differences between each type of existing money and digital asset along the dimensions of CBDC characteristics.

Two-Step Process to Down-Select the Most Relevant Design Choices

Using the OSTP’s descriptions of 18 design choices, we counted mentions of key terms relevant to law enforcement for each design choice (i.e., “law enforcement,” “privacy,” “AML/CFT,” “security,” “consumer protection”). We selected these key terms for analysis because they directly relate to how CBDC design choices impact law enforcement and individual rights. We excluded key terms related to aspects such as financial stability, systemic risk, and payment system efficiency because they pertain more to economic and operational dimensions of CBDCs. While important, these aspects do not directly address the law enforcement implications central to our study. This identified the following seven design choices with the highest counts of these terms: identity privacy, transaction privacy, intermediation, ledger history, transaction programmability, offline capabilities, and secure hardware. This quantitative analysis formed an initial hypothesis regarding their relevance to law enforcement tasks.

[67] We chose to conduct literature scans in Tasks 1 and 2 due to the exploratory nature of this study and the nascent state of literature concerning central bank digital currency and law enforcement. A more thorough examination requires a systematic literature review, following protocols such as those specified by Page et al., “The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews.”

We then assessed this list of seven design choices based on the findings of our interviews with subject matter experts. Doing so resulted in the addition of cryptography, bringing our final total to eight.

Task 2: Assess Impact of CBDC Design Choices on Law Enforcement

Task 2 began with a literature scan of 40 references to describe existing investigative techniques related to digital assets. This literature scan also considered the role of third parties in financial investigations, types of crimes facilitated by digital assets, cases involving a cross-section of U.S. law enforcement agencies investigating crimes involving digital assets, as well as regulatory considerations including the Bank Secrecy Act and FATF guidelines.

We initiated this scan with *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, and identified additional sources from this report.[68] We supplemented these sources with publicly available investigation handbooks or manuals, U.S. Government Accountability Office reports, legal filings, and news articles concerning digital asset investigations conducted or facilitated by relevant government agencies.[69]

Using the findings from the literature, we developed a taxonomy of law enforcement techniques involving digital assets.[70] The concept of "law enforcement technique" encompasses a wide range of practices and strategies as depicted in the literature, varying significantly in scope and application. In the context of investigations involving digital assets, we chose to focus on specific activities such as "transaction/activity monitoring," "web research," and "forensics." This decision was driven by the need to address the unique challenges posed by the digital nature of these assets. Other techniques—such as developing informants and conducting undercover operations—are important but operate at a higher level in law enforcement contexts. By concentrating on these specific activities, our approach aims to provide actionable insights that are directly relevant to the unique aspects of digital asset investigations.

We then compared the findings of Task 1 against the results of our Task 2 literature scan, devoting special attention to various types of criminal activities (e.g., white-collar crime, drug trafficking, child sexual abuse material, petty crime) and investigative techniques. This analysis aimed to identify common trends, challenges, and variations in how CBDC design choices might

[68] U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*.

[69] Including Consumer Financial Protection Bureau, Drug Enforcement Administration, Federal Bureau of Investigation, Federal Trade Commission, FinCEN, Homeland Security Investigations, Internal Revenue Service, Securities and Exchange Commission, and U.S. Secret Service.

[70] We developed this taxonomy following the approach of Nickerson, Varshney, and Muntermann, "A Method for Taxonomy Development and its Application in Information Systems."

impact financial investigations. The result was a map of CBDC implications to law enforcement techniques.

To deepen our analysis and verify the preliminary findings of Task 1 and Task 2, we interviewed 27 subject matter experts between February 2024 and April 2024 (featuring twelve law enforcement professionals, six government experts, six representatives from industry, and three scholars). We identified the first four interview participants through a convenience sample based on existing contacts from members of the research team and the project sponsor's team. Following this initial selection, we used a snowball sampling method to expand our participant pool, starting with contacts identified in the literature and extending through referrals from interviewees.[71] These semi-structured interviews, guided by the questions provided below, focused on how CBDC design choices could affect financial investigations.

[71] We recruited potential participants by email and conducted interviews via Microsoft Teams. Each interview lasted approximately one hour. Interviews were conducted under confidentiality to ensure participants felt comfortable sharing information and insights.

Interview Questions

Section 1: Background

1.1 To begin, please tell us about your current position and experience with digital assets and law enforcement.

Section 2: Detecting Financial Crime and Investigating Criminal Activities

2.1 What U.S. government entities are typically involved in detecting financial crime and investigating criminal activities? What other non-U.S. government entities are typically involved?

2.2 How does law enforcement use information about financial activities in investigations?

2.3 Can you describe the typical investigative process used by law enforcement in crimes involving financial assets? What tools, techniques, and methods are used at each step of the process? What is your impression of the table of techniques we highlight [participant shown table of investigative techniques]?

2.4 Can you describe how this process has been impacted by the evolution of financial instruments—from cash to crypto? Are there specific approaches to tracking conversions between different types of financial assets (e.g., cash, commercial bank money, crypto)?

2.5 How does coordination work when the financial activities of suspected criminals involve multiple jurisdictions? How often do you work through the MLAT process? Are there informal mechanisms you use to obtain information from overseas entities?

Section 3: Privacy

3.1 How have privacy concerns impacted the ability to conduct law enforcement investigations?

3.2 How did it shift under crypto?

3.3 How did it shift with the advent of digital money (e.g., Apple Pay, Venmo)?

3.4 What are the implications for CBDCs?

Section 4: Central Bank Digital Currency

4.1 How might a U.S. CBDC affect criminal activity?

4.2 How might law enforcement techniques need to change under a U.S. CBDC?

4.3 In what other ways might a U.S. CBDC affect law enforcement investigations?

Section 5: Concluding Remarks

5.1 Are there areas you feel we have missed and should consider in our work?

5.2 Is there anyone else you think we should talk to?

Task 3: Identify Possible New Law Enforcement Techniques

On Thursday, April 4, 2024, we conducted a one-day scenario-based workshop to explore law enforcement's ability to detect and investigate criminal activity involving a U.S. CBDC. Its purpose was to assess law enforcement needs for financial investigations involving a U.S. CBDC and to identify new law enforcement techniques that should be considered if a U.S. CBDC is launched.

Over the course of the workshop, participants engaged in three scenario-based discussions facilitated by study team researchers. These discussions were designed to produce both qualitative and quantitative insights into the policy significance of each scenario. The workshop was structured into sequential steps, beginning with the presentation of a scenario, followed by the development of ranking criteria, an initial assessment through voting, a facilitated discussion, a final voting assessment, and concluding with a wrap-up discussion.

To quantify the potential impact of the introduction of a CBDC on law enforcement's ability to trace flows, identify criminals, and freeze and seize funds, we used a voting technique called the Delphi Method.[72] The Delphi method is a technique that typically involves making individual anonymous estimates, followed by examining the distribution of the group's estimates, sharing justifications for the individual estimates, and revising the individual estimates with an eye toward achieving group consensus. In this exercise, we asked participants to quantify the potential impact on law enforcement effort if the scenario were to involve a U.S. CBDC.

We developed the first two scenarios from real-world case examples. Workshop participants developed the third scenario in-session, considering lessons learned and gaps identified through the first two scenarios.[73]

1. U.S. Department of Justice Seizes Nearly $9M of Tether Traced to Cryptocurrency Investment Scheme
2. Homeland Security Investigations Infiltrates Chinese Money Laundering Syndicate
3. U.S. Government Disrupts Nation-State's Attempted CBDC Heist

Table B.1. summarizes the key aspects of cases used to build scenarios discussed during the workshop, which is followed by case descriptions that we provided to participants in advance of the workshop.

[72] RAND, "Delphi Method."

[73] Other types of cases participants offered for consideration include gambling ring, trade-based money laundering, charitable organization money laundering, domestic terrorism/extremism financing, tax evasion, sanctions evasion, and an attack on the CBDC system. Participants selected the CBDC heist case for further discussion by vote.

Table B.1. Key Aspects of Cases Used to Build Workshop Scenarios

Case Dimension	Cryptocurrency Investment Scheme	Chinese Money Laundering	CBDC Heist
Type of fund	Multiple digital assets	Cash, bank accounts	Central bank money
Type of crime	Investment fraud, money laundering	Money laundering	Cybercrime, extortion, wire fraud
Criminal actor	Transnational criminal syndicate	Criminal syndicate	Adversarial nation-state
Lead generation	IC3, Consumer Sentinel Network reports	Cooperating witness (HSI, IRS-CI)	Not discussed
Key investigative techniques	Web Research, Financial Data Analysis, Asset Recovery, Forensics	Questioning/Interviews, Asset Recovery, Forensics	Not discussed

Case 1: DoJ Seizes Nearly $9M of Tether Traced to Cryptocurrency Investment Scheme

OBJECTIVE**:** Explore implications of CBDC for investment fraud and money laundering. In 2023, the DoJ seized nearly $9 million worth of Tether linked to a Southeast Asia-based criminal syndicate's nationwide "pig butchering" scam. Scammers posed as romantic interests, gaining trust and convincing over 70 victims to send funds to a fake crypto platform, which were quickly laundered into various cryptocurrencies. U.S. Secret Service agents, aided by private sector blockchain analytics, followed the victims' money and

> observed that the funds were quickly laundered through dozens of cryptocurrency addresses and exchanged for several different cryptocurrencies, a money laundering technique often referred to as 'chain hopping.' ...The seized funds were linked to numerous victim reports made via the FBI's Internet Crime Complaint Center (IC3) and Federal Trade Commission's (FTC) Consumer Sentinel Network.[74]

Case 2: Homeland Security Investigations Infiltrates Chinese Money Laundering Syndicate

OBJECTIVE: Explore implications of CBDC for money laundering. A federal jury convicted Xianbing Gan in 2020 of laundering drug money for Mexican drug traffickers. Using a technique known as "mirror transactions" to avoid the U.S. financial system, Gan arranged drops of drug money to U.S.-based businesses, who would then make equivalent transfers in China via mobile banking. Agents from Homeland Security Investigations and IRS-Criminal Investigation gathered evidence by infiltrating the syndicate with the help of a cooperating witness, and

[74] U.S. Department of Justice, "Cyber Scam Organization Disrupted Through Seizure of Nearly $9M in Crypto."

obtaining WhatsApp history on Gan's iPhone. Chinese officials declined U.S. informal requests for assistance.[75]

Case 3: Russian Charged for Ransomware Attacks, Bitcoin Tracing Used in Investigation

OBJECTIVE: Explore implications of CBDC for cybercrime, extortion, and wire fraud.[76] In 2023, the DoJ charged a Russian national, Ruslan Astamirov, for cybercrime, extortion, and wire fraud in committing numerous LockBit ransomware attacks worldwide. Stemming from an FBI investigation into LockBit, law enforcement was able to trace an 80 percent "affiliate portion" of a victim's ransom payment to a Bitcoin wallet in Astamirov's control. Law enforcement obtained this information through blockchain analysis and the seizure of Astamirov's iPhone, as well as corroborating evidence through IP location data, email records, and interviewing Astamirov.[77]

[75] Jorgic, "Burner Phones and Banking Apps - Meet the Chinese 'Brokers' Laundering Mexican Drug Money."

[76] This case was omitted during the workshop because participants were given the option to develop their own scenario, which they did.

[77] U.S. Department of Justice, "Russian National Arrested and Charged with Conspiring to Commit LockBit Ransomware Attacks Against U.S. and Foreign Businesses."

Appendix C. Omitted Design Choices

Table C.1 enumerates the ten design choices that we omitted from the final stage of the analysis. Each of these design choices was omitted for reasons described in Appendix B. Although these choices are not directly relevant or impactful to multiple law enforcement tasks, they might influence the outcomes of the other eight choices, and generate impact through them. Cryptography, for example, could be significantly impacted by the data model, fungibility, and signatures design choices. Access tiering could uniquely affect law enforcement needs by producing multiple permutations of the other seventeen design choices that law enforcement would have to approach differently.

Table C.1. Ten Design Choices Omitted from Complete Analysis

Design Choice	Description
Access Tiering	Whether to develop different transaction models based on user details or transaction amounts
Adjustments on Balances	Whether account balances can be adjusted to enable features like interest-bearing accounts or account fees
Adjustments on Transactions	Whether the central bank or intermediaries are allowed to charge fees on CBDC transactions
Data Model	Whether the CBDC system tracks account balances (aggregate amounts of CBDC held in different places) or unspent transaction outputs (specific CBDC units)
Fungibility	Whether CBDC units have unique identifiers (i.e. serial codes)
Holding Limits	Whether there are limits on how much CBDC can be held in a wallet
Interoperability	Whether, and to what extent, the CBDC system can communicate and transact with other domestic and international payment systems
Permissioning	Whether the CBDC system is managed by a set of trusted entities or by a decentralized network of system participants
Remediation	Whether remediation (recovering accounts, voiding transactions, recovering funds, etc.) occurs on- or off- ledger and what is the governance protocol of these actions
Signatures	Whether zero, one, or multiple verifications of identity are required to authorize a CBDC transaction

SOURCE: Features information from OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

Abbreviations

AML/CFT	anti-money laundering and countering the financing of terrorism
BSA/AML	Bank Secrecy Act / Anti-Money Laundering
CBDC	central bank digital currency
CTR	currency transaction report
DHS	Department of Homeland Security
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
Fed, The	Board of Governors of the Federal Reserve System
FinCEN	Financial Crimes Enforcement Network
FTC	Federal Trade Commission
HSI	Homeland Security Investigations
IC3	Internet Crime Complaint Center
IRS-CI	Internal Revenue Service Criminal Investigation
KYC	Know Your Customer
OSTP	Office of Science and Technology Policy
PIA	Privacy Impact Analysis
PKC	public-key cryptography
SAR	suspicious activity report
SEC	Securities and Exchange Commission
ZKP	zero-knowledge proof

Glossary

blockchain: “distributed ledger technologies where data is shared across a network that creates a digital ledger of verified transactions or information among network participants and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value.”[78]

central bank digital currency (CBDC): “a form of digital money or monetary value, denominated in the national unit of account, that is a direct liability of the central bank.”[79] *Retail CBDC* “generally refers to a CBDC that is widely available to the public for day-to-day use in personal and commercial transactions” whereas *wholesale CBDC* “generally refers to a CBDC with a narrower use case, such as one designed primarily for large-value institutional payments and not widely available to the general public.”[80]

cryptocurrency: “a digital asset, which may be a medium of exchange, for which generation or ownership records are supported through a distributed ledger technology that relies on cryptography, such as a blockchain.”[81]

digital assets: “all CBDCs, regardless of the technology used, and to other representations of value, financial assets and instruments, or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology.”[82]

intermediation: the process of involving intermediaries (e.g., banks, money service businesses, non-traditional public or private intermediaries) in CBDC transactions. Potential functions include distributing currency, wallet creation and custody, validating and settling transactions, AML/CFT compliance, conducting fraud detection, resolving disputes, customer service, and managing user interfaces.[83]

[78] Executive Order 14067, “Ensuring Responsible Development of Digital Assets.”

[79] Executive Order 14067, “Ensuring Responsible Development of Digital Assets.”

[80] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*, p. 5.

[81] Executive Order 14067, “Ensuring Responsible Development of Digital Assets.”

[82] Executive Order 14067, “Ensuring Responsible Development of Digital Assets.”

[83] OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

stablecoin: “a category of cryptocurrencies with mechanisms that are aimed at maintaining a stable value, such as by pegging the value of the coin to a specific currency, asset, or pool of assets or by algorithmically controlling supply in response to changes in demand in order to stabilize value.”[84]

[84] Executive Order 14067, “Ensuring Responsible Development of Digital Assets.”

References

Atlantic Council, “Central Bank Digital Currency Tracker,” webpage, March 2024. As of May 1, 2024: https://www.atlanticcouncil.org/cbdctracker/

Bank for International Settlements, “BIS Innovation Hub Work on Central Bank Digital Currency (CBDC),” webpage, undated. As of May 4, 2024: https://www.bis.org/about/bisih/topics/cbdc.htm

Bank for International Settlements, “Project Polaris: Secure and Resilient CBDC Systems, Offline and Online,” webpage, 2023. As of June 26, 2024: https://www.bis.org/about/bisih/topics/cbdc/polaris.htm

Berentsen, Aleksander, Jeremias Lenzi, and Remo Nyffenegger, “An Introduction to Zero-Knowledge Proofs in Blockchains and Economics,” Federal Reserve Bank of St. Louis *Review*, Vol. 105, No. 4, 2023, pp. 280–94. As of May 1, 2024: https://doi.org/10.20955/r.105.280-94

Bernal Bernabe, Jorge, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta, “Privacy-Preserving Solutions for Blockchain: Review and Challenges,” *IEEE Access*, Vol. 7, 2019, pp. 164908–164940. As of May 1, 2024: https://ieeexplore.ieee.org/document/8888155

Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, January 2022. As of April 16, 2024: https://www.federalreserve.gov/publications/money-and-payments-discussion-paper.htm

Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation: Summary of Public Comments*, April 2023. As of May 3, 2024: https://www.federalreserve.gov/publications/money-and-payments-summary-of-public-comment.htm

Brun, Jean-Pierre, Anastasia Sotiropoulou, Larissa Gray, Clive Scott, and Keven M. Stephenson, *Asset Recovery Handbook: A Guide for Practitioners, Second Edition*, International Bank for Reconstruction and Development / The World Bank, 2021. As of May 7, 2024: https://star.worldbank.org/focus-area/financial-investigations

Chainalysis, *The 2024 Crypto Crime Report*, February 2024. As of April 30, 2024: https://go.chainalysis.com/crypto-crime-2024.html

Digital Currency Initiative, “Project Hamilton - Building a Hypothetical Central Bank Digital Currency,” Massachusetts Institute of Technology, webpage, undated. As of May 8, 2024: https://dci.mit.edu/project-hamilton-building-a-hypothetical-cbdc

Digital Dollar Project, "Leading the Discussion on Future of the US Dollar," webpage, undated. As of May 2, 2024: https://digitaldollarproject.org

Egel, Daniel, Jim Mignano, Sale Lilly, James V. Marrone, Max Rangeley, Charles P. Ries, Jessie Wang, and Dulani Woods, *Central Bank Digital Currencies and U.S. Strategic Competition with China,* RAND Corporation, RR-A2911-1, 2024. As of March 22, 2024: https://www.rand.org/pubs/research_reports/RRA2911-1.html

Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders*, 2020. As of April 30, 2024: https://www.elliptic.co/resources/typologies-concise-guide-crypto-leaders

European Central Bank, "Technical Documents and Research," webpage, undated. As of May 1, 2024: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/html/index.en.html

Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, Europol Spotlight Report Series, Publications Office of the European Union, 2021. As of April 30, 2024: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

Executive Order 14067, "Ensuring Responsible Development of Digital Assets," Executive Office of the President, March 9, 2022.

Fanusie, Yaya J., *Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them*, The Lawfare Institute, November 2020. As of May 12, 2024: https://www.lawfaremedia.org/article/central-bank-digital-currencies-threat-money-launderers-and-how-stop-them

FATF, *Crowdfunding for Terrorism Financing*, October 2023. As of April 30, 2024: https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html

FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations*, 2023. As of May 7, 2024: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

FATF, *Operational Issues – Financial Investigations Guidance*, June 2012. As of April 29, 2024: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Operationalissues-financialinvestigationsguidance.html

Federal Bureau of Investigation, "A Brief Description of the Federal Criminal Justice Process," webpage, undated. As of May 5, 2024: https://www.fbi.gov/how-we-can-help-you/victim-services/a-brief-description-of-the-federal-criminal-justice-process

Federal Bureau of Investigation, "White-Collar Crime," webpage, undated. As of April 16, 2024: https://www.fbi.gov/investigate/white-collar-crime

Federal Deposit Insurance Corporation, “Privacy Impact Assessments (PIAs),” webpage, December 13, 2023. As of May 8, 2024: https://www.fdic.gov/policies/privacy/assessments.html

Federal Reserve Bank of Boston, *Project Hamilton Phase 1: Executive Summary*, February 3, 2022. As of May 2, 2024: https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx

Federal Reserve Bank of New York, “Project Cedar: Improving Cross-Border Payments with Distributed Ledger Technology,” webpage, undated. As of May 2, 2024: https://www.newyorkfed.org/aboutthefed/nyic/project-cedar

Federal Trade Commission, “Division of Enforcement,” webpage, undated. As of April 16, 2024: https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-enforcement

Flakoll, Derrick, and Jess Redmond, *Digital Dollars and the Future of Money: Fighting Financial Crime in a World of Central Bank Digital Currencies*, Harvard Kennedy School Policy Analysis Exercise, April 12, 2022. As of May 12, 2024: https://scholar.harvard.edu/files/derrick-flakoll/files/digital_dollars_and_the_future_of_money_pae_-_redmond_and_flakoll.pdf

Financial Crimes Enforcement Network, U.S. Department of the Treasury, “Enforcement Division,” webpage, undated. As of April 16, 2024: https://www.fincen.gov/enforcement-division

Financial Crimes Enforcement Network, U.S. Department of the Treasury, “Privacy Impact Assessments,” webpage, undated. As of May 8, 2024: https://www.fincen.gov/privacy-impact-assessments

Financial Crimes Enforcement Network, U.S. Department of the Treasury, “Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets: Notice of Proposed Rulemaking,” *Federal Register*, Vol. 85, No. 247, December 23, 2020, p. 3. As of May 5, 2024: https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets

Financial Crimes Enforcement Network, U.S. Department of the Treasury, “The Value of FinCEN Data,” webpage, undated. As of May 5, 2024: https://www.fincen.gov/resources/law-enforcement/case-examples

Georghiou, Luke, Jennifer Cassingena Harper, Michael Keenan, Ian Miles, and Rafael Popper, eds., *The Handbook of Technology Foresight: Concepts and Practice*, Edward Elgar, 2008.

Internal Revenue Service, “Criminal Investigation,” webpage, 2023. As of April 16, 2024: https://www.irs.gov/compliance/criminal-investigation

Internal Revenue Service, “Privacy Impact Assessments - PIA,” webpage, July 25, 2023. As of May 8, 2024: https://www.irs.gov/privacy-disclosure/privacy-impact-assessments-pia

Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, *2023 Elder Fraud Report*, 2024. As of May 13, 2024: https://www.ic3.gov/Home/EF

Jimenez, Alison, “Why Some Criminals Love Crypto,” Dynamic Securities Analytics Blog, January 3, 2024. As of May 5, 2024: https://securitiesanalytics.com/why-some-criminals-love-crypto/

Jorgic, Drazen, “Burner Phones and Banking Apps - Meet the Chinese ‘Brokers’ Laundering Mexican Drug Money,” *Reuters*, December 3, 2020. As of April 3, 2024: https://www.reuters.com/article/idUSKBN28D1LP/

Lesavre, Loïc, Priam Varin, and Dylan Yaga, *Blockchain Networks: Token Design and Management Overview*, National Institute of Standards and Technology, NISTIR 8301, February 2021. As of April 16, 2024: https://csrc.nist.gov/pubs/ir/8301/final

Lindsay, Jay, “Boston Fed, MIT Complete Research Project into Feasibility of a Central Bank Digital Currency,” Federal Reserve Bank of Boston, webpage, December 22, 2022. As of May 2, 2024: https://www.bostonfed.org/news-and-events/news/2022/12/project-hamilton-boston-fed-mit-complete-central-bank-digital-currency-cbdc-project.aspx

Lukens, Philip, “An Introduction to How AI is Transforming Real Time Crime Centers,” *Police1*, March 11, 2024. As of June 14, 2024: https://www.police1.com/tech-pulse/an-introduction-to-how-ai-is-transforming-real-time-crime-centers

Nickerson, Robert C., Upkar Varshney, and Jan Muntermann, “A Method for Taxonomy Development and its Application in Information Systems,” *European Journal of Information Systems,* Vol. 22, No. 3, 2013, pp. 336–359. As of April 16, 2024: https://doi.org/10.1057/ejis.2012.26

Office of Management and Budget, Circular No. A-130, “Managing Information as a Strategic Resource,” July 28, 2016. As of May 8, 2024: https://www.cio.gov/policies-and-priorities/circular-a-130/

Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, September 2022. As of April 16, 2024: https://www.whitehouse.gov/ostp/news-updates/2022/09/16/technical-possibilities-for-a-u-s-central-bank-digital-currency/

OSTP—*See* Office of Science and Technology Policy.

Page, Matthew J., Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, Roger Chou, Julie Glanville, Jeremy M. Grimshaw, Asbjørn Hróbjartsson, Manoj M. Lalu, Tianjing Li, Elizabeth W. Loder, Evan Mayo-Wilson, Steve McDonald, Luke A. McGuinness, Lesley A. Stewart, James Thomas, Andrea C. Tricco, Vivian A. Welch, Penny Whiting, and David Moher, "The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews," *BMJ*, Vol. 372, No. 71, 2021. As of June 14, 2024: https://www.bmj.com/content/372/bmj.n71

Popper, Rafael, "Foresight Methodology," in Luke Georghiou, Jennifer Cassingena Harper, Michael Keenan, Ian Miles, and Rafael Popper, eds., *The Handbook of Technology Foresight: Concepts and Practice*, Edward Elgar, 2008, pp. 44–88.

RAND, "Delphi Method," webpage, undated. As of May 8, 2024: https://www.rand.org/topics/delphi-method.html

Science and Technology Directorate, U.S. Department of Homeland Security, "Technology Centers," webpage, March 6, 2024. As of May 11, 2024: https://www.dhs.gov/science-and-technology/Technology-Centers

Tucker, Eric, "US Recovers Most of Ransom Paid after Colonial Pipeline Hack," *AP News*, June 7, 2021. As of April 16, 2024: https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52

Uhlig, Harald, Mike Alonso, and Jon Frost, "Privacy in Digital Payments—Escaping the Panopticon," *Georgetown Journal of International Affairs*, Vol. 24, No. 2, Fall 2023, pp. 177–179. As of April 16, 2024: https://doi.org/10.1353/gia.2023.a913643

U.S. Department of Justice, "Cyber Scam Organization Disrupted Through Seizure of Nearly $9M in Crypto," November 21, 2023. As of April 3, 2024: https://www.justice.gov/opa/pr/cyber-scam-organization-disrupted-through-seizure-nearly-9m-crypto

U.S. Department of Justice, "Russian National Arrested and Charged with Conspiring to Commit LockBit Ransomware Attacks Against U.S. and Foreign Businesses," June 15, 2023. As of April 3, 2024: https://www.justice.gov/opa/pr/russian-national-arrested-and-charged-conspiring-commit-lockbit-ransomware-attacks-against-us

U.S. Department of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, September 2022. As of April 16, 2024: https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network

U.S. Department of the Treasury, *The Future of Money and Payments*, September 2022. As of May 2, 2024: https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf

U.S. Government Accountability Office, *Bank Secrecy Act: Agencies and Financial Institutions Share Information but Metrics and Feedback Not Regularly Provided*, GAO-19-582, August 2019. As of April 16, 2024: https://www.gao.gov/products/gao-19-582

U.S. Government Accountability Office, *U.S. Secret Service: Investigative Operations Confer Benefits, but Additional Actions Are Needed to Prioritize Resources*, GAO-20-239, January 2020. As of April 16, 2024: https://www.gao.gov/products/gao-20-239

U.S. Immigration and Customs Enforcement, "Homeland Security Investigations," webpage, 2024. As of April 16, 2024: https://www.ice.gov/about-ice/homeland-security-investigations

U.S. Secret Service, "Cyber Investigations," webpage, undated. As of June 14, 2024: https://www.secretservice.gov/investigations/cyber

U.S. Secret Service, *Office of Investigations Strategy, FY 2021–2027*, 2021. As of May 5, 2024: https://www.secretservice.gov/sites/default/files/reports/2021-01/inv-strategy-fy21-27.pdf

U.S. Securities and Exchange Commission, *Enforcement Manual*, November 28, 2017. As of April 16, 2024: https://www.sec.gov/enforcement/how-investigations-work

White House, "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets," press release, September 16, 2022. As of May 8, 2024: https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/

White House, "Privacy," webpage, undated. As of May 8, 2024: https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/

Woods, Dulani, John S. Hollywood, Jeremy D. Barnum, Danielle Fenimore, Michael J. D. Vermeer, and Brian A. Jackson, *Cryptocurrency and Blockchain Needs for Law Enforcement*, RAND Corporation, RR-A108-17, 2023. As of April 16, 2024: https://www.rand.org/pubs/research_reports/RRA108-17.html

World Economic Forum, *Digital Currency Governance Consortium White Paper Series – Privacy and Confidentiality Options for CBDC,* November 2021. As of May 7, 2024: https://www.weforum.org/publications/digital-currency-governance-consortium-white-paper-series/privacy-and-confidentiality/