April 2025

Expert Insights
PERSPECTIVE ON A TIMELY POLICY ISSUE

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

Key Insights

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

AN FFRDC OPERATED BY RAND UNDER CONTRACT WITH DHS

This research was published in 2025.

Central Bank Digital Currency Design Choices and Effect on Law Enforcement: Key Insights

The Federal Reserve is exploring the creation of a U.S. central bank digital currency (CBDC), a government-backed digital dollar. The law enforcement implications of how such a CBDC is designed—particularly the impact on law enforcement's ability to detect and investigate crime—is unclear.

HSOAC examined—using 27 expert interviews and a scenario-based workshop with 17 participants from private finance and law enforcement—how law enforcement may need to evolve its capabilities for financial investigations to address new challenges from a CBDC. This memo summarizes the top-level findings and policy recommendations that emerged from this research.

Eight CBDC Design Choices are Most Likely to Impact Law Enforcement Investigations

The Office of Science and Technology Policy (OSTP) enumerated 18 CBDC design choices under consideration by policymakers. HSOAC analyzed OSTP's discussion of these 18 design choices, focusing on four criteria we identified through interviews with subject matter experts: privacy, anti-money laundering and countering the financing of terrorism (AML/CFT) compliance, CBDC system security, and consumer protection. Table 1 presents the results of our analysis, summarizing the eight design choices we found most relevant to law enforcement based on their implications for each of the four criteria.

Table 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	

Design Choice	Privacy	AML/CFT Compliance	System Security	Consumer Protection
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 Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, September 2022.

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

While a U.S. CBDC is unlikely to necessitate entirely new law enforcement techniques, law enforcement agencies can anticipate updating how they monitor, analyze, and recover illicit funds if a U.S. CBDC is launched. Table 2 presents a summary of potentially necessary changes to these techniques, as indicated by participants in a workshop HSOAC hosted to assess the need for new law enforcement techniques in the context of a U.S. CBDC.

Table 2. Summary of Potential Changes to Investigative Techniques a U.S. CBDC Might Require

Technique	Example Change(s) Needed
Transaction or activity monitoring	• Higher volumes of Bank Secrecy Act / Anti-Money Laundering, police, and victim reports could necessitate more integrated and automated reporting and monitoring systems to accommodate a U.S. CBDC.
Questioning or 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. • Increased asset recovery needs could prompt adjustments to law enforcement priorities.
Forensics	• No specific changes identified.

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

- 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 digital 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 guarantee individual privacy while allowing for lawful access during investigations.

About This Paper

This work was commissioned by U.S. Department of Homeland Security (DHS) Science and Technology Directorate and was conducted in HSOAC's Infrastructure, Immigration, and Security Operations Program of the RAND Homeland Security Research Division (HSRD), which operates the Homeland Security Operational Analysis Center (HSOAC). This paper reflects the expert opinion of the authors. Comments or questions on this work should be addressed to the project leaders, Jim Mignano (jmignano@rand.org) and Daniel Egel (degel@rand.org).

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/PEA2952-1. The complete research report is available at https://www.rand.org/pubs/research_reports/RRA2952-1.html.