Seton Hall University
eRepository @ Seton Hall

Student Works | Seton Hall Law

2024

Data Privacy and Security Implications of a U.S. Central Bank Digital Currency (CBDC)

Rhianna Ross

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

 Part of the Law Commons

Data Privacy and Security Implications of a U.S. Central Bank Digital Currency (CBDC)

Abstract

A new, digital era of the global financial system has arrived. To keep up with the future of the global financial system, the U.S. government is currently undergoing extensive research into the benefits and risks of a U.S. central bank digital currency ("CBDC"), a digital version of the U.S. dollar. Old fashioned paper and coin could soon become a thing of the past, or, at least, a smaller slice of U.S. currency offerings, but at what expense to data privacy?

While the U.S. and other major world economies are deep into the early research and development stages for future CBDC systems, and as the U.S. has not yet even committed to issuing a digital currency, the purpose of this paper is to explore the critical data privacy questions facing CBDCs and provide some initial design recommendations that could help strengthen the soundness and longevity of a hypothetical U.S. CBDC system. The design recommendations prioritize privacy while simultaneously addressing the risk of scrutiny from international privacy authorities.

Part I of this paper introduces the concept of a CBDC and the status of global research and development efforts into CBDCs. Part II of this paper examines the U.S. government's prioritization of privacy in published research and design discussions. Part III of this paper, first, considers the current federal financial privacy law environment and the delicate balance between personal privacy interests and government financial crime detections efforts. Next, Part III considers state data privacy legislation and data breach requirements applicable to financial institutions in the absence of a comprehensive federal data privacy law. Finally, Part III considers the European Union's ("EU") data privacy regime and introduces challenges

associated with its application to certain CBDCs design choices. Finally, Part IV of this paper, first, provides a high-level overview of technological design choices that could have significant impacts on privacy (e.g., centralized vs. distributed ledger technology), and second, sets forth the following privacy-driven design recommendations for a future U.S. CBDC:

(1) The U.S. CBDC system must be intermediated by private sector financial institutions with robust data privacy compliance programs;
(2) The U.S. government should further investigate whether a U.S. CBDC system can operate via private and permissioned distributed ledger technology ("DLT") while complying with domestic and global data privacy regimes; and
(3) The U.S. CBDC system should be designed to comply with the strictest state data privacy laws and data breach notification requirements.

Part I: Introduction

Over the last four decades, the technology driving the U.S. payment system has evolved considerably. In the private banking sector, digital wallets and third-party peer-to-peer payment services, such as Venmo and Cash App, are now ubiquitous. More recently, retail participation in the digital asset space (e.g., cryptocurrencies, virtual currencies, stable coins, non-fungible tokens, etc.) has grown exponentially following the development of decentralized ledger technology (sometimes referred to as "distributed ledger technology" or "DLT"). According to the Fed, the market capitalization of cryptocurrencies increased "from less than $100 billion five years ago" to around $2 trillion as of February 2022."[1] This new wave of DLT and similar decentralized payment technologies facilitate un-intermediated, peer-to-peer ("P2P") digital asset payments and transfers between account holders.[2]

[1] *See Preparing for the Financial System of the Future*, Governor Lael Brainard, 2022 U.S. Monetary Policy Forum, (Feb. 18. 2022), https://www.federalreserve.gov/newsevents/speech/brainard20220218a.htm.
[2] *See Money and Payments: The U.S. Dollar in the Age of Digital Transformation,* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, at 11, (Jan. 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf; *See also* FedNow℠ SERVICE, BD. OF GOVERNORS FED. RESERVE SYSTEM, https://www.federalreserve.gov/paymentsystems/fednow_about.htm

As for the Federal Reserve Bank System, technological developments have moved at a slower pace. In the 1970s, the Federal Reserve Automated Clearing House (ACH) system emerged to allow real-time interbank payments, and since 2019, the Federal Reserve Board of Governors ("the Fed") has been developing the *FedNow* Service, which would unveil even faster real-time, uninterrupted inter-bank payment services in 2023.[3]

Next up on the docket of advancements to the U.S. payment system (and other payment systems globally) is a brand-new form of currency – a central bank digital currency ("CBDC") – backed by the full faith and credit of the U.S. government, and colloquially referred to as a "digital dollar."[4] This hypothetical U.S. CBDC would carry the same status as a physical dollar, representing "a digital liability of a central bank that is widely available to the general public."[5] In a January 2022 press conference, the Fed Chairman, Jerome Powell, stated that "[the Fed] has been carefully monitoring and adapting to the technological innovations now transforming the world of payments, finance, and banking."[6]

Today, the U.S. remains in the research and development phase as various government agencies are exploring the potential benefits and consequences of a CBDC system. The Fed stated unequivocally that it "does not intend to proceed with issuance of a CBDC without clear support from the Executive Branch and Congress, ideally in the form of a specific authorizing

---

[3] *Id.* at 1.
[4] *See Money and Payments: The U.S. Dollar in the Age of Digital Transformation,* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, at 11, (Jan. 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.
[5] *See Central Bank Digital Currency (CBDC)*, BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, https://www.federalreserve.gov/central-bank-digital-currency.htm, (Nov. 4, 2022).
[6] *See Press Release: Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments landscape,* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, (May. 20, 2021), https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm

law." This statement from the Fed presents an interesting first stop legal question: does the Fed have the authority to unilaterally issue a digital dollar directly to Americans?

The clear answer is no. The powers of the Federal Reserve Banks are enumerated in Section 13 of the Federal Reserve Act of 1913, which does not grant the Fed express authority to issue currency directly to individuals.[7] According to the Fed, if Federal Reserve accounts were offered directly to individuals, "such accounts would represent a significant expansion of the Federal Reserve's role in the financial system and the economy."[8] Despite the Fed's clear intention to refrain from action, U.S. Senator of Texas, Ted Cruz, publicized concern that the Fed could act unilaterally in launching a CBDC. In March 2022, Senator Cruz introduced a bill proposing to amend the Federal Reserve Act to expressly prohibit the Federal Reserve Banks from offering a digital currency "directly to an individual or maintain[ing] an account on behalf of any individual."[9] Nonetheless, the Fed will refrain from taking steps outside of the initial research and development phase without express authorization which could come either in the form of an amendment to the Federal Reserve Act or through entirely new authorizing legislation and is committed to exploring the potential benefits and risks of a CBDCs system in cooperation with other government agencies.

The United States would not be the first to launch a CBDC (or even second or third). According to Atlantic Council's CBDC Tracker as of November 2022, "105 countries,

---

[7] 12 USC 347d. As added by act of Sept. 17, 1978 (92 Stat. 621), BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, https://www.federalreserve.gov/aboutthefed/section13.htm

[8] *See Money and Payments: The U.S. Dollar in the Age of Digital Transformation,* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, at 13, (Jan. 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.

[9] *See* SIL22526, *A bill to amend the Federal Reserve Act to prohibit the Federal reserve banks from offering certain products or services directly to an individual, and for other purposes*, 117th Congress 2d Session, (Mar. 2022), https://www.cruz.senate.gov/imo/media/doc/cbdc.pdf; *See also Press Release: Sen. Cruz Introduces Legislation Prohibiting Unilateral Fed Control of a U.S. Digital Currency*, (Mar. 30, 2022), https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-introduces-legislation-prohibiting-unilateral-fed-control-of-a-us-digital-currency

representing over 95 percent of global GDP, are exploring a CBDC" system.[10] Of those countries exploring CBDCs, 11 CBDCs have launched so far, including in the Bahamas, Jamaica, Nigeria, and eight additional eastern Caribbean countries.[11] Another 17 countries, including Russia and China, are working through pilot phases for CBDC systems.[12]

For example, in February 2022, China launched the digital yuan (referred to throughout as "e-CNY") and the accompanying e-CNY wallet accessible through the digital yuan mobile application.[13] The digital currency backed by the People's Bank of China (PBOC) went live in 11 regions of the country, following extensive research that began as early as 2017 and a small-scale initial pilot phase in 2020.[14] According to Atlantic Council, adoption of the e-currency as of October 2021 rose to 123 million consumer wallets and 9.2 million corporate wallets that have made 142 million individual transactions worth the equivalent of 8.8 billion U.S. dollars.[15]

As of November 2022, another 33 countries exploring CBDCs are navigating the development stages (including the United States) while the remaining majority of 39 countries remain in the research phase.[16] The Fed, various U.S. government agencies, and other government agencies and central bank organizations globally have proceeded with caution while vocalizing particular points of tension in privacy law, among other legal and regulatory issues, that will require additional research and legal analysis. For example, in the Fed's January 2022 first whitepaper on the potential CBDC system, the Fed committed to further research on the

[10] *See Central Bank Digital Currency Tracker*, Atlantic Council, (accessed Nov. 16, 2022), https://www.atlanticcouncil.org/cbdctracker/ (providing a nation-by-nation status updates on applicable CBDC projects).
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

implications of a potential U.S. CBDC on a whole host of U.S law and policy issues, including data privacy and security.[17] While the U.S. and most major European economies wish to remain competitive with the rest of the world that is vigorously exploring projects CBDC research and development projects, progress towards a finished product could be particularly slow due to several legal and regulatory challenges in both domestic and global privacy law, particularly in Europe.[18]

Part II: Prioritizing Privacy for a U.S. CBDC

At the forefront of U.S. government's priority list for a U.S. CBDC system is *privacy*. The Fed is hyper-cognizant that the design choices made raise significant "consumer protection, legal, and privacy considerations."[19] In publicizing the essential pillars of design, the Fed noted that any future CBDC must be: "(1) privacy-protected, (2) intermediated, (3) widely transferable, (4) identity-verified, and (5) resilient to operational and cybersecurity risks."[20] Notably, *privacy* is first on the list.

This comes as no surprise given the common global concentration on the privacy risks associated with newly developing CBDC systems. For example, the European Centra Bank ("ECB") reported that of the 8,221 comments it received as part of a public consultation period

[17] *See Money and Payments: The U.S. Dollar in the Age of Digital Transformation,* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, at 19, (Jan. 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

[18] *See Central Bank Digital Currency Tracker,* ATLANTIC COUNCIL, (accessed Nov. 16, 2022), https://www.atlanticcouncil.org/cbdctracker/ (summarizing Vice Chair of the Fed Lael Brainard's testimony to Congress expressing "concerns that given developments in Europe, the US might fall behind on the technological advantages of CBDCs); *See also Digital Assets and the Future of Finance: Examining the Benefits and Risks of a U.S. Central Bank Digital Currency*, Vice Chair Lael Brainard, Committee on Financial Services, U.S. House of Representatives, (May 26, 2022), https://www.federalreserve.gov/newsevents/testimony/brainard20220526a.htm

[19] *See id.* at 24.

[20] *See id.* at 13.

beginning in October 2020 following the release of its Eurosystem report on a potential digital euro, “41% of all comments addressed "privacy of payments.”[21]

In March 2022, President Biden declared official White House support for dedicated research into the U.S. CBDC system through Executive Order 14067 (“EO 14067”).[22] EO 14067, which primarily addressed the lack of regulatory clarity over cryptocurrencies and other digital assets, mandated that the Secretary of Treasury (in coordination with other government officials including the Secretary of State, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Director of Nation Intelligence, and the heads of other relevant agencies) issue a report analyzing (1) “ the extent to which privacy or consumer protection measures . . . . may be used to protect users of digital assets” and (2) “the potential implications for national security and financial crime.”[23]

Following EO 14067, the White House released Policy Objectives for a U.S. CBDC, stressing the significance of “designing privacy protections for sensitive financial data, mitigating illicit finance risks, and instituting cybersecurity and privacy incident management and contingency plans”[24] At the core of design for a U.S. CBDC and of utmost importance is that “the CBDC system should maintain privacy and protect against arbitrary or unlawful surveillance.”[25]

---

[21] *See Press Release: ECB digital euro consultation ends with record level of public feedback ,* EUROPEAN CENTRAL BANK, Eurosystem,(Jan. 13, 2022), https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html

[22] *See* 87 FR 14143, E.O. 14067, *Ensuring Responsible Development of Digital Assets*, (Mar. 14, 2022), https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

[23] *Id*.

[24] *See Policy Objectives for a U.S. Central Bank Digital Currency System,* THE WHITE HOUSE, (Sep. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Policy-Objectives-US-CBDC-System.pdf.

[25] *Id.*

EO 14067 led to a flurry of CBDC privacy bills from members of Congress. In April 2022, Senator Ted Cruz criticized the idea and sought to expressly ban the Fed from issuing a CBDC altogether, noting that CBDC systems can provide a "central bank control over individual payment and transfer activity (i.e., to be used as a surveillance tool by the US government)."[26] Somewhat dispelling Senator Cruz's concern is the fact that the Fed does not intend to replace physical dollars with digital ones, thus, American citizens whom are warry of any compromise to individual privacy could carry on, business as usual, with their current bank accounts and use of cash or credit cards.

With privacy as a primary concern, U.S. Representative and Chairman of the Task Force on Financial Technology, Stephen Lynch, introduced the Electronic Currency and Secure Hardware (ECASH) Act in April 2022, in support of the development of a U.S. CBDC.[27] The ECASH Act's purpose is to develop a pilot program for a digital dollar that mimics the "privacy-respecting features of physical cash, calling for the incorporation of "key security and functionality safeguards" including: "(1) anonymity, (2) privacy, and (3) minimal generation of data from transactions."[28]

EO 14067 and subsequent policy objectives issued by the Whitehouse eventually trickled down into a series of interagency reports on design implications for a U.S. CBDC, focusing

---

[26] *See* SIL22526, *A bill to amend the Federal Reserve Act to prohibit the Federal reserve banks from offering certain products or services directly to an individual, and for other purposes*, 117th Congress 2d Session, (Mar. 2022), https://www.cruz.senate.gov/imo/media/doc/cbdc.pdf; *See also Press Release: Sen. Cruz Introduces Legislation Prohibiting Unilateral Fed Control of a U.S. Digital Currency*, (Mar. 30, 2022), https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-introduces-legislation-prohibiting-unilateral-fed-control-of-a-us-digital-currency.

[27] *See* H.R. 7231, *Fact Sheet: The Electronic Currency and Secure Hardware (ECASH) Act*, https://lynch.house.gov/_cache/files/5/0/500162f9-7fce-4981-b9b916bf22e10ede/83EE032381B9431A65DE22B213D3A10E.rep.-lynch-ecash-act-fact-sheet.pdf; *See also Pres Release: Rep. Lynch Introduces Legislation to Develop Electronic Version of U.S. Dollar*, (Mar. 28, 2022), https://lynch.house.gov/press-releases?ID=5A0DA9DE-8884-4E06-AC0A-BCA08850F05E.

[28] *Id.*

heavily on *privacy-by-design*. As the name suggests, privacy-by-design is the idea that privacy rights must be factored into the equation of any product or system design from the very beginning stages. For example, the September 2022 Interagency Technical Evaluation produced several privacy-driven implications of CBDC design, including the potential to: (1) "disrupt current balances between individual data privacy and the special needs of law enforcement to surveil financial transactions for illicit activities," (2) "create privacy risks associated with the collection, storage, and transmission of payment information and associated business identifiable and personally identifiable information" and (3) "trigger data breach notification and response compliance requirements" at the state and international level.[29] Additionally, the Department of the Treasury flagged privacy as particular area of concern for U.S. CBDC research, noting that "the development of a U.S. CBDC may warrant the reevaluation of existing privacy standards" altogether, including any further legislative solutions that may address gray areas in U.S. privacy law.[30]

Among the most heavily cited privacy-centered design considerations amongst the publicly available reports were: (1) the choice of whether to leverage intermediaries, (2) the significance of compliance with both Anti-Money Laundering/Know Your Customer ("AML/KYC") laws and regulations while simultaneously adhering to financial privacy laws and regulations, and (3) the nature and extent of privacy protections afforded to individuals through publicly accessible DLTs like blockchain technology (discussed in greater depth in Part IV of this paper).

---

[29] *See Technical Evaluation for a U.S. CBDC System,* OFFICE OF SCIENCE AND TECHNOLOGY POLICY, (Sep. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf.

[30] *See The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14607,* THE DEPARTMENT OF THE TREASURY, (Sep. 2022), https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf

With privacy as the centerpiece, Part III of this paper evaluates the current privacy law landscape applicable to financial institutions in the United States today, while Part IV sets forth recommendations for addressing the critical design questions identified in Table 1 below. The following critical design questions fall into three major design categories – intermediation, identity and transaction privacy, and data breach and incident response – in alignment with the core concerns identified in recent U.S. CBDC published reports.

Table 1: Critical CBDC Design Questions

Intermediation	Should the U.S. CBDC payment system operate with an intermediary between the Fed and individual currency holders? Should the U.S. CBDC operate through a centralized or decentralized ledger model?
Identity & Transaction Privacy	Who should have access to personal identifiable information and transaction data collected and stored in the U.S. CBDC system and under what limited circumstances should it be accessed?
Data Breach & Incident Response	How should the CBDC system respond to data breaches or other data security incidents and comply with data breach reporting requirements (both domestically and globally)?

Part III: The Data Privacy Landscape for U.S. Financial Institutions and Implications for the Proposed U.S. CBDC

Designing a privacy-conscious U.S. CBDC system begins with understanding the legal environment in which it would operate. Unlike the European Union ("EU"), the United States does not have a one-stop-shop federal privacy law that provides a clear set of uniform requirements. Instead, U.S. privacy law is more of a patchwork approach, comprised of various industry-targeted federal privacy laws (e.g., in the healthcare and financial services fields) and associated regulations, in addition to state comprehensive privacy laws.

A. Federal Financial Privacy Law

U.S. financial privacy law was established to maintain an intricate balance between individual privacy interests in securing sensitive financial information while, simultaneously enabling law enforcement to prevent and detect money laundering, terrorist financing, financial crimes, and other illicit financing activities in the U.S. financial system.

Under federal financial privacy law, the first restraint on government access to financial information is through the Right to Financial Privacy Act (RFPA).[31] The RFPA provides a critical safeguard for individuals from unauthorized government requests for information, limiting government access to bank records only where the government has made a legitimate request pursuant to a valid court order.[32] The RFPA allows financial institutions to provide information upon government request if (1) the financial records are reasonably described; (2) the records are relevant to legitimate law enforcement inquiry; (3) the records are properly requested via an administrative subpoena, a search warrant, a judicial subpoena, or a formal written request, and (4) the customer is given notice with respect to the disclosure.[33]

Another consumer privacy-centered, federal financial privacy law is the Graham-Leach-Bliley Act (GBLA) which provides protection for consumers from unauthorized disclosure of nonpublic person information by financial institutions to third parties.[34] The GBLA provides three primary rules, known as, the Disclosure Rule, the Privacy Rule, and the Safeguards Rule.[35]

---

[31] 12 U.S.C. § 3402, et seq, https://www.law.cornell.edu/uscode/text/12/3402; see *also Right to Financial Privacy Act*, Consumer Compliance Handbook, THE BD. OF GOVERNORS OF THE FED. RESERVE; https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf.
[32] *Id.*
[33] *Id.*
[34] *See* 15 U.S.C.§ 6801, et seq, https://www.law.cornell.edu/uscode/text/15/6801.
[35] *See GLBA: The Financial Privacy and Safeguards Rules*, Westlaw: Practical Law Data Privacy & Cybersecurity, (2023).

The disclosure rule requires financial institutions to provide their customers with "privacy notices" that detail the financial institution's privacy policies and practices.[36] The GLBA's Disclosure Rule exempts certain "normal disclosures," for example disclosures made to protect against or prevent actual or potential fraud or to comply with applicable legal requirements, such as the disclosure of information to regulators.[37] The GLBA's Privacy Rule enforces certain information sharing restrictions by requiring financial institutions to give consumers the option to opt-out of their personal information from being shared with non-affiliated third parties.[38]

Lastly, the GLBA's Safeguard Rule imposes upon financial institutions an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[39] While the federal law and implementing regulations do not specify exactly what safeguards would satisfy this affirmative and continuing obligation, it provides that financial institutions must develop policies that promote data security. These polices must be reasonably designed to (1) "ensure the security and confidentiality of customer records and information"; (2) "protect against any anticipated threats or hazards to the security or integrity of such records"; and (3) "protect against unauthorized access to or use that could result in customer injury."

For a U.S. CBDC system to facilitate the RFPA's federal safeguard against unlawful government access to personal bank records, the system must be designed with a layer of protection between the Fed and the individual CBDC account holders. Further, any future U.S. CBDC system would require robust plans and procedures for RFPA and GLBA compliance for

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*

all data sharing practices. For existing private sector banks, these programs have already been set up and running for decades.

B. Federal Anti-Money Laundering (AML) Law and Know Your Customer (KYC) Requirements

In direct conflict with personal data privacy interests is the government's difficult task of identifying and surveilling for money laundering, terrorist financing, organized crimes, financial crimes, tax evasion, and other illicit financing activities. In an effort to afford the U.S. government tools to combat these harmful financial activities and protect the general welfare of the U.S. financial system, Congress passed the Foreign Transactions Act of 1970, commonly referred to as the Bank Secrecy Act ("BSA").[40] The BSA was further amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act") of 2001 and, again, by the Anti-Money Laundering Act ("AMLA") of 2020.[41] Taken together, the BSA imposes upon banks numerous recordkeeping and reporting requirements to help the government identify suspicious movements of money.[42] Financial institutions are required, among many other actions, to (1) report directly to the Secretary of Treasury the payment, receipt, or transfer of currency in excess of $10,000 per day via currency transaction reports (CTR) and (2) file suspicious activity reports (SARs) for any "known or suspected violation of Federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act."[43]

---

[40] *See Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control*, DSC Risk Management Examination Policies, Federal Deposit Insurance Corporation (2021), at 8.1-45, https://www.fdic.gov/regulations/safety/manual/section8-1.pdf.
[41] *Id.*
[42] *Id.*
[43] *Id.*

Whether a SAR must be filed is based on a combination of dollar amount thresholds and circumstantial triggers including: "insider abuse involving any amount; transactions aggregating $5,000 or more where a suspect can be identified; transactions aggregating $25,000 or more regardless of potential suspects; and transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA."[44] However, the FDIC clarified that in "instances of possible terrorism, identity theft, and computer intrusions, the dollar thresholds for filing may not always be met" and that banks are "encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce."[45]

These BSA-mandated reports must include sufficient details to identify the persons and transaction involved including name, street address, social security number or taxpayer identification number, and date of birth, the documentation used to verify the identity of the individual, account number, the amount and kind of transaction that took place, and for foreign currency transactions, the country of origin and US dollar amount of the transaction.

The USA Patriot Act amended the BSA to require all financial institutions to create a customer identification program (CIP). A CIP is a "written, board-approved program that details procedures for (1) verifying the true identity of a financial institution's customer, (2) collecting identifying information from each customer upon account opening, (3) taking appropriate actions such as rejecting the opening of account when a customer's identity cannot be verified, (4)

---

[44] *See* Lori Kohlenberg & Rebecca Williams, *Connecting the Dots…The Importance of Timely and Effective Suspicious Activity Reports,* FEDERAL DEPOSIT INSURANCE CORPORATION, Supervisory Insights, (Dec. 28, 2021), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/article03_connecting.html#:~:text=Dollar%20Amount%20Thresholds%20%E2%80%93%20Banks%20are,and%20transactions%20aggregating%20%245%2C000%20or

[45] *Id.*

maintaining appropriate records during the collection and verification of a customer's identity, and (5) checking the customer's name against terrorist lists".[46]

For the avoidance of doubt, the hypothetical CBDC would constitute currency under the BSA. Under the AMLA amendments to the BSA, passed as part of the National Defense Authorization act of 2021, a new, broader definition of "financial institution" was codified under the BSA to include businesses that "exchange or engage in the transmission of cryptocurrency" and the definition of "monetary instruments" was expanded to include instruments whose "value substitutes for currency."[47] Needless to say, a U.S. CBDC system, while protecting individual privacy interests, must be able to surveil for and report suspicious activities, report daily currency transactions in excess of $10,000, and implement strict customer identification procedures with sufficient detail to satisfy the federal requirements. Complying with the BSA and other implementing regulations points, again, in favor of leveraging the existing infrastructure of private sector banks.

C. State Data Privacy Law and Data Breach Notification Requirements

Given the lack of a single comprehensive federal standard for data privacy practices and data breach procedures, a hypothetical U.S. CBDC system that would serve U.S. citizens across the 50 states would have to take careful account of industry-specific federal requirements, in addition to the nuances in state privacy law.

On the federal side, financial institutions are subject to the GLBA Safeguards rule discussed above, but this rule merely mandates the existence of policies that are aimed to

[46] *Id.*
[47] *See New Challenges: Anti-money Laundering Act 2020*, SIA Partners, (Jul. 22, 2021), https://www.sia-partners.com/en/news-and-publications/from-our-experts/new-challenges-anti-money-laundering-act-2020.

promote data security. Additionally, impacting reporting of cyber incidents and data breach issues, Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in March of 2022, a law that gives the Cybersecurity and Infrastructure Security Agency (CISA) the authority to draft implementing regulations that would mandate cyber incidences and ransomware payments be reported to CISA by covered entities, including financial institutions.[48] However, because no CIRCIA implementing regulations are yet in force, financial institutions are left with varying state data breach and security requirements.

Many state legislatures have taken it upon themselves to fill the gaps existing within the current federal privacy law framework by enacting comprehensive state privacy laws to protect its residents. For example, in passing the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), California legislators took broad measures to create a comprehensive data privacy regime that, in many ways, mirrors the protections offered by the EU's General Data Protection Regulation ("GDPR") discussed below. Similar to the GDPR, California's privacy legislation applies broadly to any entity that "does business in [California] and owns or licenses computerized data that contains [personal information]."[49]

California privacy law contains an expansive definition of personal information (which includes account numbers and passcodes that permit access to an individual's financial account), strict third-party disclosure and notification requirements, a right for data subjects to opt out of disclosure of personal information, a right for data subjects to request the deletion of one's

[48] *See Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/circia.
[49] *Security Breach Notification Chart*, Perkins Coie, (Sept. 2021), https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf.

personal information, and strict data breach notification timing and notice requirements.[50] For example, §1798.82 of the California Civil Code provides that a breach of the security of the system requires disclosure "in the most expedient time possible and without unreasonable delay."[51]

Some states have also imposed legislation aiming to promote desirable data handling practices upon entities doing business in their state. For example, in Virginia, state law requires a "data controller" to "limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer."[52] Virginia law also requires data controllers to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."[53]

Absent a single federal standard, the entities accountable for data related to the U.S. CBDC system must take into account the vast geographical location of its data subjects and ensure that it adheres to local requirements or, in the alternative, adheres to the requirements of the strictest, most consumer-privacy conscious state.

C. International Data Privacy Law

While access to the U.S CBDC system may not be international in scale from the hypothetical date of launch, the government has publicly recognized the value that an integrated, cross-border digital payment system could provide for international transactions down the road.

---

[50] *See California Consumer Privacy Act,* STATE OF CA. DEPT. OF JUSTICE, https://oag.ca.gov/privacy/ccpa.
[51] *See Security Breach Notification Chart*, Perkins Coie, (Sept. 2021), https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf.
[52] *See* § 59.1-578 VA. Code, https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/
[53] *Id*.

In designing a U.S. CBDC system, the U.S. government must contemplate how it will comply with international data privacy regimes if the digital dollar becomes a globally accessible currency.

One of the most demanding and well-known international data privacy regimes is the European Union's (EU) General Data Privacy Protection Regulation (GDPR) enacted in May 2018.[54] This broad European legislation was enacted to "safeguard personal data and uphold the privacy rights" of any individual residing in the EU territory.[55] To accomplish this, the GDPR sets out rules for data storage, retention, and record keeping that apply to any businesses and organizations that perform operations on personal data of individuals living in the EU, no matter where the business processing the data is physically located.[56] These rules include requirements for data processors to disclose the types of information collected, the purposes of collection, and the uses of the data collected; obtain affirmative consent from consumers to any data processing practices; erase personal data upon the consumer's will; and notify consumers of data breaches "without undue delay."[57]

Whether the GDPR's rules apply to a particular entity or organization hinges on whether the organization qualifies as a "data processor" with respect to EU residents. Article 3 of the GDPR provides that the rules apply to organizations that process (i.e., collect, store, transmit, analyze, etc.) the personal data of EU residents by either offering goods or services to people in the EU or monitoring their online behavior."[58] The end-user-facing organization in the U.S.

---

[54] *See EU Data Protection Rules and U.S. Implications*, CONGRESSIONAL RESEARCH SERVICE, at 1, (Jul. 17, 2020), https://sgp.fas.org/crs/row/IF10896.pdf.; *See also The EU General Data Protection Regulation,* IAPP, IAPP Law, https://iapp.org/resources/article/the-eu-general-data-protection-regulation/.
[55] *Id*. at 1-3.
[56] *Id*.
[57] *Id*.
[58] *Id*.

CBDC system would clearly qualify as a data processor subject to the GDPR if EU residents were to participate in the system by virtue of (1) collecting personal identifiable data of EU individuals at the account opening stage and (2) maintaining access to, storing, tracking, and reporting personal identifiable information and transaction data pursuant to U.S. regulatory requirements.

If the U.S. CBDC system is to be accessible by consumers globally, the ability to adhere to the GDPR's stringent requirements must be factored into the CBDC design process from the beginning. For this reason, the use of select global financial institutions as intermediaries to the CBDC system would be ideal for ease of compliance, given many of these institutions have already established GDPR compliant processes and procedures.

However, if the U.S. opens the CBDC system to EU residents, then depending on structural system design choices, there may be significant challenges ahead due to multiple points of tension between the GDPR privacy regime and DLTs.[59] This type of technology and its tensions with the GDPR are further explored in Part IV of this paper.

Part IV: Privacy-driven Design Recommendations for a Hypothetical U.S. CBDC

Before diving into the privacy issues facing a future U.S. CBDC system and potential design solutions, this section will first provide high-level background on existing centralized ledger systems utilized in the U.S. payment system and "decentralized" or "distributed" ledger technologies emerging in the digital asset space globally.

[59] *Id.*

Payments between two individuals and maintenance of the associated transaction data can be accomplished through a centralized ledger or a decentralized ledger. Today, standard electronic cash payments and transfers between accounts are tracked and recorded on a centralized ledgers, operated and maintained by financial institutions as intermediaries that approve the transaction and process the payments.[60] For example, in a centralized payment system, when party A pays or transfers cash to party B, party A must provide payment instructions to a third party (a financial institution). The transaction is then approved by the financial institution and recorded in the bank's centralized ledger.

In contrast, digital asset transactions are conducted in a decentralized manner, which, as its name suggests, is not maintained by any one centralized party. Blockchain technology is one well-known type of DLT utilized today that can be utilized for discussion purposes. A blockchain is "a shared and synchronised digital database" or a shared public ledger.[61] Each participant in a blockchain system is connected to the blockchain network and the blockchain system is "maintained by a consensus algorithm and stored on multiple nodes (or computers that store a local version of the database)." In other words, each participant maintains a node within the blockchain system and data is collected, processed, and stored in a public, decentralized manner that is modifiable by each individual participant (or node) in the system when a transaction is made. This means that each connected participant can transact and modify the public ledger and therefore has control over the data on the blockchain.[62]

---

[60] *See Technical Evaluation for a U.S. CBDC System,* OFFICE OF SCIENCE AND TECHNOLOGY POLICY, (Sep. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf.

[61] *See Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* EUROPEAN PARLIAMENTARY RESEARCH SERVICE, SCIENTIFIC FORESIGHT UNIT, at 1, (Jul. 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[62] *Id*. at I.

In a DLT payment system such as the blockchain technology behind Bitcoin transactions, when party A wants to pay party B in Bitcoin, party A can do so directly through a peer-to-peer ("P2P") transaction involving a series of public and private keys. Party A and Party B each have a public key (i.e., an address or wallet known to the public to which bitcoin can be transmitted), and a private key (or a private password to that public bitcoin address which allows the address owner to access the funds within).[63] Party A will be able to directly transact Bitcoin with Party B so long as Party A knows Party B's public key and Party B can access the Bitcoin with Party B's private key.[64] When Party A and Party B successfully transact bitcoin, a record of the transaction is automatically added to the decentralized ledger without verification by a central party.

DLTs like blockchain provide a plethora of innovative technological benefits to the global payment system, however, some forms of the technology, specifically those that allow for full anonymity, carry an equivalent amount of risk to financial crime detection efforts. Additionally, certain forms of DLT raise unique privacy challenges if selected for the U.S. CBDC design and the digital currency is available across borders.

The following section sets forth design recommendations that address the critical design questions identified in Part II, in light of the privacy law landscape explored in Part III.

Recommendation 1: The U.S. CBDC system must be intermediated by private sector financial institutions with robust data privacy compliance programs

Underpinning each of the critical design questions, is a threshold question: Should the U.S. CBDC system be intermediated or non-intermediated? The clear answer to this question is that the system *must* be intermediated. More specifically, the U.S. government should consider

[63] *See How does Bitcoin work?,* BITCOIN PROJECT, https://bitcoin.org/en/how-it-works; *See also Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf.
[64] *Id.*

selecting a select group of approved private sector banks to serve as the intermediaries between the Fed and the individual currency holders with CBDC accounts. Inserting an intermediary layer between consumers and the Fed will ensure that the delicate balance between aiding the efforts of law enforcement and protecting personal privacy interests is not disturbed.

In addition to preventing an unwarranted tipping of this balance, there are several legal and compliance justifications for intermediating CBDC transactions with selected private sector financial institutions. First, private sector banks have been operating compliance programs for decades under to ensure all requirements under the RFPA, the GLBA, the BSA, state-level data privacy and security requirements, and even international data privacy requirements are fulfilled. For example, global financial institutions typically have robust, top-tier infrastructure in place to verify the identity of each and every account holder pursuant to the BSA's CIP requirements and scan for suspicious transactions pursuant to AML/KYC requirements. If the Federal Reserve Banks, instead were able to offer CBDC accounts directly to the individual or selected some other government entity to centrally operate the CBDC system, it would have to design and build data security programs and financial privacy compliance programs to protect its new account holders from scratch – doing so would be impractical where the Fed could simply leverage the private sector.

Looking to CBDC projects globally, of the eleven launched CBDCs internationally, all eleven countries elected an intermediated structure.[65] Of the fifteen CBDC systems that have entered the pilot phase, only eight have expressly adopted an intermediated structure while the remaining seven countries are still considering the benefits and risks of an intermediated

[65] *See Central Bank Digital Currency Tracker*, Atlantic Council, (Nov. 16, 2022), https://www.atlanticcouncil.org/cbdctracker/ (providing a nation-by-nation status updates on applicable CBDC projects).

structure as opposed to a non-intermediated structure that allows individuals and businesses to open accounts directly with the Central Bank entities.[66] China's piloted CBDC system, referred to as the e-CNY project, is a clear-cut example of an intermediated structure.[67] The power to issue e-CNY belongs to the state of China and the operational system is centered around the People's Bank of China ("PBOC").[68] The PBOC issues e-CNY to "authorized operators," i.e., authorized commercial banks, and manages e-CNY through its entire life-cycle.[69] Once issued, "the authorized operators and other commercial institutions exchange and circulate e-CNY to the public" through the traditional consumer-bank account relationship.[70]

Sweden's "e-krona" pilot project is another example of an intermediated CBDC system design. Sveriges Riksbank ("the Riksbank"), Sweden's central bank body, Sweden's e-krona system is intermediated by two approved participants in the e-krona network .[71] Individuals may set up e-krona accounts, or "e-krona wallets," with one of two approved participants in the e-krona network, Handelsbanken or Tietoevry, which are commercial banks connected to the e-krona network.[72] For testing purposes, the Swedish e-krona system was constructed in a manner where "Tietoevry's and the Riksbank's nodes were implemented in [Riskbank's IT environment], while Handelsbanken's node were implemented in [Handelsbanken's] own IT environment."

---

[66] *Id*.
[67] *See Privacy and Confidentiality Options for Central Bank Digital Currency,* WORLD ECONOMIC FORUM, Digital Currency Governance Consortium White Paper Series, at 3, (Nov. 2021), https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.
[68] *See Progress of Research & Development of E-CNY in China,* THE PEOPLE'S BANK OF CHINA, Working Group On E-CNY Research And Development Of The People's Bank Of China, at 3, (Jul. 2021), http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.
[69] *Id.*
[70] *Id.*
[71] *See E-krona Report: E-Krona Pilot Phase 2*, SVERIGES RIKSBANK, (Dec. 16, 2022), https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf.
[72] *Id*. at 14.

Despite the differing IT environments used by each participant, customers of both banks were "able to communicate and carry out transactions on a common e-krona network."[73]

The U.S. CBDC System should be designed similarly to the intermediated e-krona system, but with one key difference – the selected intermediary financial institutions should connect to the greater CBDC network o*nly* through its own IT infrastructure. In other words, unlike Swedish e-krona system, the intermediary financial institutions should be physically barricaded from connecting to the CBDC system via the Fed's IT infrastructure.

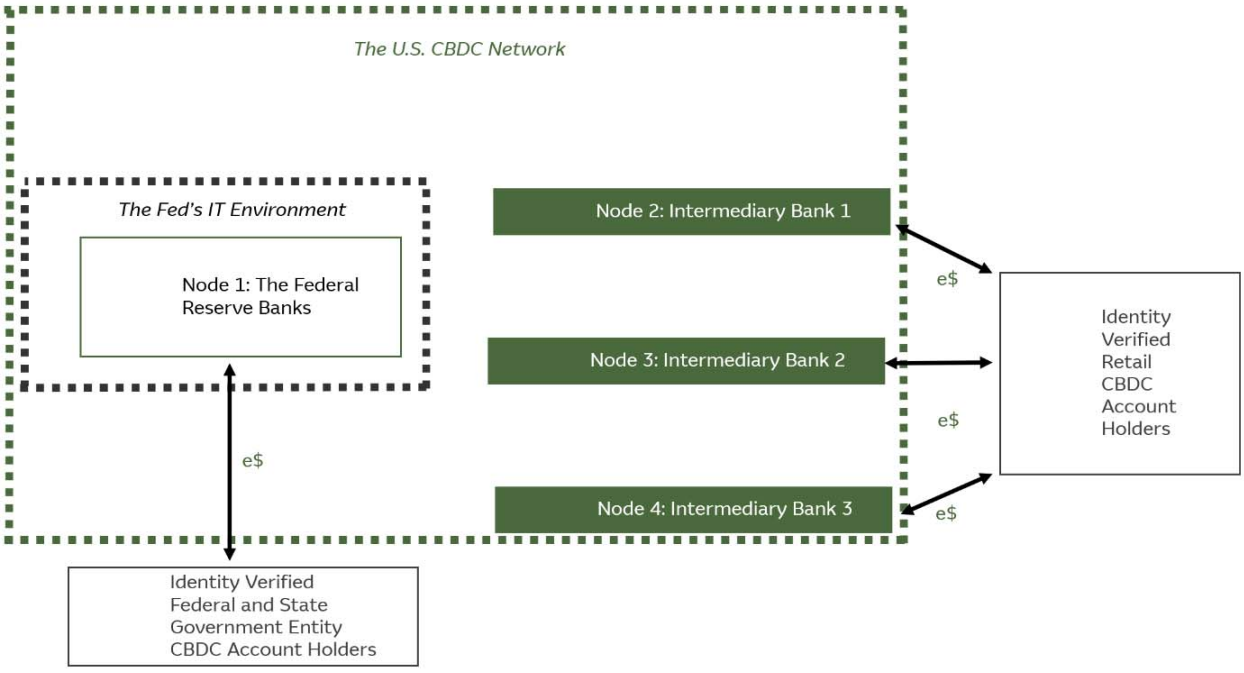
This paper proposes the below structure for the future CBDC system set forth in Figure 1. In this proposed design, the Department of the Treasury or the Fed, pending allocation of authority, would be solely responsible for issuing the digital currency into circulation and the selected intermediary banks would distribute the digital currency to account holders (with the exception of federal and state government entities who may establish accounts directly with the Federal Reserve Banks under the existing U.S. monetary system).[74]

---

[73] *See id.*; *See also Privacy and Confidentiality Options for Central Bank Digital Currency,* WORLD ECONOMIC FORUM, Digital Currency Governance Consortium White Paper Series, at 4, (Nov. 2021), https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf. 4 (graphically depicting the e-krona project design).

[74] *See FAQ: Does the Federal Reserve maintain accounts for individuals? Can individuals use such accounts to pay bills and get money,* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM, https://www.federalreserve.gov/faqs/does-the-federal-reserve-maintain-accounts-for-individuals-can-individuals-use-such-accounts-to-pay-bills-and-get-money.htm#:~:text=The%20Federal%20Reserve%20Banks%20provide, accounts%20at%20the%20Federal%20Reserve.

Figure 1: Proposed Design for an Intermediated U.S. CBDC System[75]



This intermediated design will (1) establish maximum individual privacy rights for US bank customers under existing federal financial privacy law by eliminating the possibility of unwarranted information sharing and (2) protect the Fed's infrastructure from added risk of targeted cyber-attacks. Private-public separation is critical for a U.S. CBDC system to move forward under the U.S. privacy law environment.

[75] *Figure 1: Proposed Design for an Intermediated U.S. CBDC System:* Figure 1 is a graphical depiction of an intermediated CBDC System with three selected intermediary banks. The large green dashed box represents the U.S. CBDC Network on which the system operates. The smaller black dashed box represents the Fed's IT environment in which the selected intermediary banks may not connect to the CBDC network through. Each individual green box represents a node or connection to the CBDC Network outside of the Fed's IT environment. Outside of the CBDC Network are two categories of account holders which must set up CBDC accounts (account relationships between end-users and intermediaries are denoted by black arrows): (1) Identity verified federal and state government entity CBDC account holders which may set up CBDC accounts directly with the Federal Reserve Banks and (2) Identity verified retail CBDC account holders (e.g., individuals and businesses) which must set up a CBDC account with one of the three selected intermediary banks.

Recommendation 2: The U.S. government should further investigate whether a U.S. CBDC system can operate via private and permissioned distributed ledger technology ("DLT") while complying with domestic and global data privacy regimes.

Having established that intermediation is not only preferred, but a necessity, for legal and compliance purposes, the next question is: who should have access to identity data and transaction data and under what circumstances? As discussed in Part III, a U.S. CBDC System must be considerate of the RFPA and GBLA's rules concerning disclosure of personal and financial data to third parties (including the U.S. government), in addition to the recordkeeping and reporting rules set forth under the BSA.

First, the U.S. government cannot lawfully maintain unlimited access to identity and transaction data generated by the CBDC system under the present U.S. financial privacy law environment. This information may lawfully be transferred to the government's hands, without violating individual privacy interests, if the information is requested in manner that is compliant with the RFPA's disclosure rules or the information is reported pursuant to the BSA's transaction reporting rules. Therefore, any CBDC future design choice must not inadvertently expand the powers of the U.S. government to collect personal information on U.S. citizens, in violation of individual privacy rights.

Further every individual maintains a right against unlawful disclosure of personal and financial information to third parties. The GBLA, state data privacy laws, and other data privacy regimes globally have established the rules under which personal and financial information may be disclosed by financial institutions to third parties unaffiliated with the disclosing party. Any future CBDC design choice must also consider how access to information is managed to protect

individual participants in the CBDC system from (1) unlawful disclosures of their own personal and financial information or (2) unintended legal responsibility associated with access to data.

A critical privacy law hurdle that the Fed will face in designing the U.S. CBDC system that lies at the center of identity and transaction privacy concerns is whether the system should operate by recording and tracking transactions on (1) a centralized ledger operated by a single body or (2) a decentralized ledger operated and modifiable by all participants connected to the CBDC network. If a decentralized model is chosen, a sub-issue that the Fed will face is whether access to the ledger and ledger history is (1) public or private, or (2) permissioned or permissionless.[76] A public ledger would mean that all information on the transaction ledger would be publicly available to all participants that are active in the CBDC network (including end-users) and a private ledger would mean that only a subset of private entities would maintain access to the ledger. Separately, "a CBDC system could either be managed by a set of trusted entities ("permissioned") or by a network of system participants ("permissionless").”[77]

Turning, again, to global CBDC projects, China’s e-CNY project provides a clear example of a centralized ledger operating model where all e-CNY transactions are conducted and recorded on a centralized ledger operated by the PBOC. China’s e-CNY system utilizes a model referred to as “controlled anonymity” where transactions are completely anonymous to all parties involved in the system, except for the PBOC. Therefore, the PBOC alone has complete visibility and “can trace DC/EP [Digital Currency Electronic Payment] movements.”[78] Under China’s e-CNY model, not only can the PBOC trace individual transactions, but it can also map the

[76] *See Technical Evaluation for a U.S. CBDC System*, OFFICE OF SCIENCE AND TECHNOLOGY POLICY, (Sep. 2022), 14 at Footnote 18, https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf.
[77] *See id.* at 11.
[78] *See Privacy and Confidentiality Options for Central Bank Digital Currency,* WORLD ECONOMIC FORUM, Digital Currency Governance Consortium White Paper Series, 5, (Nov. 2021), https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.

individual transaction addresses back to the user's true identity.[79] However, the PBOC explained that it takes additional measures to protects against unlawful government surveillance by utilizing firewalls for any e-CNY-related information, designating "special personnel to manage [e-CNY] information," and prohibiting all "arbitrary information requests".[80]

In contrast to China's e-CNY model, the Swedish Riksbank's e-krona pilot project was constructed via *Corda*, a Swedish, open-source DLT or blockchain platform which is currently used for the transferring digital assets.[81] Operating through a DLT model, e-krona "transactions are not recorded in a central database, but in the nodes of the participants directly involved in the transaction."[82] This means all e-krona wallet holders that initiate transactions maintain visibility into the public, e-krona digital ledger, and have modifying capabilities with respect to the ledger.

How the Swedish e-krona system operates in practice raises concerns about identity and transaction data privacy. In the pilot project, each individual end-user sets up an e-krona wallet with one of the participant banks connected to the e-krona network. Through an alias service, each end-user's e-krona wallet address is assigned a unique alias.[83] All alias and associated wallet address information is housed in a centralized alias database within the Riksbank's IT environment operated by a third-party alias service provider with sole access to the alias mappings.[84] When an end-user enters an alias that it wishes to transfer e-krona, "it is done via the participant's [i.e., the bank's] e-krona engine, which calls the [e-krona] network's central alias

[79] *Id.*
[80] *Id.* at 7.
[81] *Id.* at 3.
[82] *Id.*
[83] *See E-krona Report: E-Krona Pilot Phase 2*, SVERIGES RIKSBANK, (Dec. 16, 2022), 14, https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf.
[84] *Id.*

service that stores the specified alias together with the associated wallet ID" before completing the transaction.[85]

The Riksbank, as a central bank organization of an EU member country, is concerned about the e-krona pilot project, as currently designed, and its ability to comply with the EU's GDPR. In the Riksbank's e-krona pilot project phase two report, the Riksbank notably recognized that "one cannot rule out the possibility that data in the network is processed in a way that is not compliant with the legislation on financial secrecy and data protection."[86] The Riksbank further warned that consultation with Swedish and European Union data protection authorities about how blockchain technology relates to data protection regulations, may be required for the piloted e-krona system to fully comply with data protection legislation.[87]

What exactly is the privacy issue that Riksbank is concerned with? It essentially boils down to a question of accountability. Stated differently, the question raised by DLTs under the GDPR is: who is accountable for the sensitive data as a data processor within a CBDC system (and for complying with the GDPR's requirements) operating via DLT (where all participants in the system could be "processing" or "controlling" data per the regulation's definitions).

The interplay between blockchain technology and the European Union's GDPR creates a complex and murky environment to build a compliant CBDC system. Riksbank has heavily disclaimed that the piloted e-krona system, noting that the system will likely be subject to legal and information security changes in the future, pending further legal analysis. Specifically,

[85] *Id.*
[86] *Id*. at 5.
[87] *Id*. at 29.

Riksbank believes it "is likely that the data accompanying a transaction in the transaction history will be considered personal data and subject to financial secrecy."[88]

The European Parliament's Research Service addressed these issues in 2019 by raising three critical tensions between DLT and the GDPR: (1) the GDPR holds "at least one natural or legal person" accountable whom EU resident data subjects can address to enforce their rights, however, DLT replaces a single accountable actor with several contributing actors which, in turn, "hampers the allocation of responsibility and accountability," (2) the GDPR requires data to be "modified or erased where necessary to comply with Articles 16 and 17, however, DLT by design typically does not give any one participant the right of modification or erasure, and (3) the data minimization principles behind the GDPR are frustrated by DLT which typically stores information publicly and across multiple nodes in the system.[89]

What does this mean for a U.S. CBDC system as the Fed contemplates global access to the digital dollar? Can a hypothetical U.S. CBDC system be designed to take advantage of the innovative benefits of DLT, while simultaneously complying with domestic and global privacy laws and regulations?

What makes digital assets so attractive to the general public as a form of payment is the ability to transact directly and instantaneously between peers in a cash-like, anonymous manner, and the ability to trace and verify the validity of all transactions through an anonymized public ledger. At the same time, completely anonymizing all CBDC transactions and the use of DLT could potentially hinder the purpose and spirit of the BSA and its related implementing

---

[88] *Id.*

[89] *See Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* EUROPEAN PARLIAMENTARY RESEARCH SERVICE, SCIENTIFIC FORESIGHT UNIT, at II, (Jul. 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

regulations that seek to identify and prevent money-laundering, fraud, and other harmful financial crimes.

As discussed in Part III, BSA reporting requirements apply to daily aggregate cash transaction levels, and in some cases, certain cash transactions that are deemed suspicious, but that do not rise to certain minimum dollar-amount thresholds. The requirement for financial institutions to *say something* when they *see something* makes designing a U.S. CBDC system running on a decentralized, public and permissionless ledger with complete identity anonymity an impossibility.

Moving to some potential privacy-conscious solutions, first, the U.S. CBDC system could operate on a centralized ledger model, in the same way the U.S. payment system functions today, thus, avoiding DLT-associated legal challenges altogether. Under this centralized model, only the selected participant banks would have access to ledger transactions and ledger history. A centralized model would ensure that only the banks maintain authority over transaction details and identity details for the purposes of compliance with BSA/AML/CIP requirements while ensuring all personal and transaction data is protected by and confined to the hands of the selected financial institutions that have the infrastructure to protect privacy. A centralized model would eliminate any potential disharmony with the GDPR if the system were to be accessible by EU residents or compatible with EU CBDC systems down the road. It is no secret that a centralized model would be the path of least resistance.

Alternatively, the Fed could consider operating the CBDC system via a private and permissioned DLT platform where non-traceable, non-identifying details of CBDC transactions are visible to the permissioned intermediary financial institutions in the network on the private ledger. However, identifying details of CBDC transactions would need to be accessible to the

select intermediary financial institutions (e.g., through a highly secure form of cryptographic technology) for the purposes of maintaining compliance with BSA compliance programs. For example, the permissioned intermediary financial institutions, after conducting all CIP procedures at the account opening stages, could assign a randomly generated alias to each end-user account to appear on the private ledger for a specified period of time (e.g., a single day alias). The permissioned intermediary banks could, therefore, see transaction amounts associated with randomly generated daily account identifiers (similar to the e-krona alias concept) which are not, by themselves, traceable to specific end-users. The financial institutions would, therefore, be able to conduct and apply existing surveillance tools to the CBDC system's partially anonymized private ledger to fulfill its responsibility to surveil for and report suspicious activities or activities over certain nominal reporting thresholds.

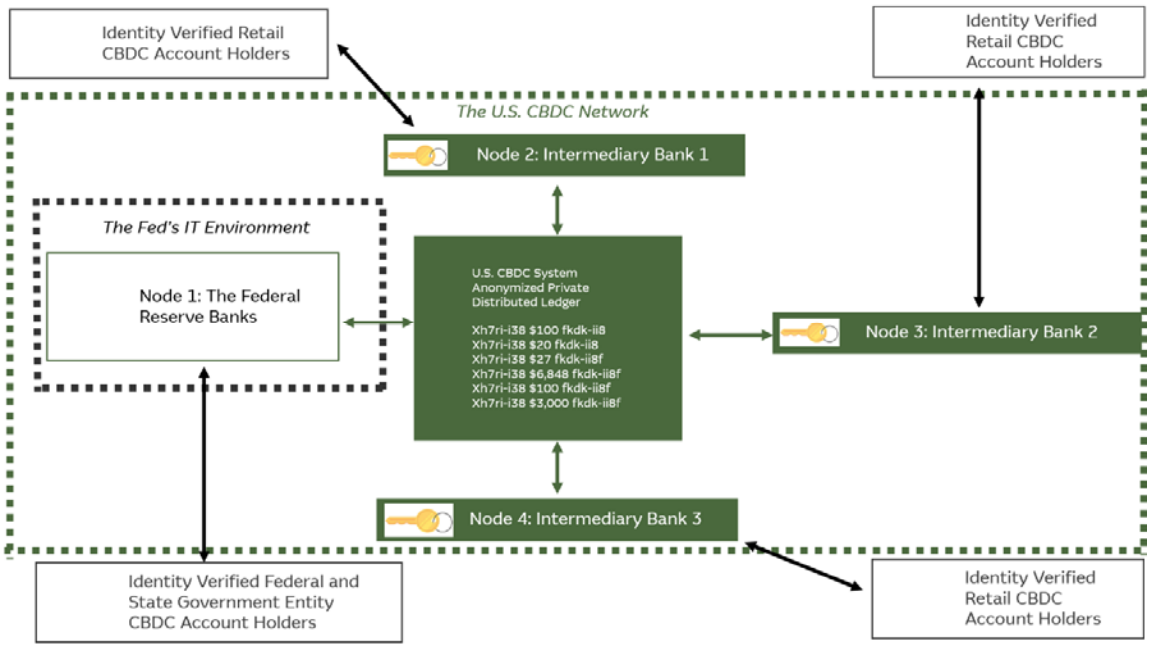
If the financial institutions suspect any criminal or otherwise suspicious financial activity on the ledger associated with the assigned aliases, the financial institutions must be able to map the anonymous alias information to a particular account owner when required for BSA reporting purposes. The Fed could consider an array of technological solutions for securely locking down alias identities while allowing for targeted identity mapping capabilities. For example, the World Economic Forum has released a series of Digital Currency Governance whitepapers delving into potential "privacy enhancing techniques for financial institutions" including various types of "cryptography" that can securely lock and unlock identity and transaction details.[90] These

[90] See Privacy and Confidentiality Options for Central Bank Digital Currency, WORLD ECONOMIC FORUM, Digital Currency Governance Consortium White Paper Series, at 8, (Nov. 2021), https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.

cryptographic techniques include zero-knowledge proofs, symmetric-key and asymmetric key cryptography, differential privacy, and homomorphic encryption.[91]

Figure 2 below reflects a hypothetical design for an anonymized, private, and permissioned DLT system that the U.S. government could consider for the U.S. CBDC system, building upon the foundation of Figure 1.

Figure 2: Hypothetical U.S. CBDC System Anonymized Semi-Public Distributed Ledger[92]



In summary, the privacy issues raised by DLT are relatively new and highly complex. When compared against other data privacy regimes globally, such as the GDPR, these privacy concerns will only escalate in complexity as technologies evolve. Because of this area of

[91] *Id*. at 8-11 (explaining various types of cryptography tools utilized across the global financial system).
[92] *Figure 2: Hypothetical U.S. CBDC System Anonymized Semi-Public Distributed Ledger:* Each individual account holder would open a CBDC account or wallet with one of the selected intermediary banks, subject to identify verification procedures (account relationships between end-users and the intermediary banks are indicated by the black arrows). Each verified CBDC wallet is assigned a randomly generated, single-day alias that would appear on the private ledger (accessibility to the private ledger is indicated by the green arrows). Each participating intermediary bank would be able to map the randomly generated single-day aliases to its individual account holders using cryptographic technology in order to satisfy BSA transaction reporting and other compliance purposes.

uncertainty, it is prudent that the Fed, in conjunction with other contributing government agencies to the U.S. CBDC research and development project, participate in international dialogue and cooperative research efforts when designing a privacy-conscious system. Designing a system that, for example, fails to adhere to the requirements of the GDPR, will stifle its longevity and viability in the global payment system.

Recommendation 3: The U.S. CBDC system should be designed to comply with the strictest state data privacy laws and data breach notification requirements.

Another critical benefit of leveraging select private sector financial institutions as intermediaries to the U.S. CBDC system is the reality that most large-scale financial institutions serve customers across the 50 states and, therefore, have dedicated compliance staff (or even entire regulatory compliance teams or departments) that ensure state level privacy requirements are monitored for and adhered to.

In order to reduce the possibility for error on whether a particular state data breach notification requirement is triggered and to ensure the CBDC upholds the strongest data security practices for U.S. domiciled data subject possible, the U.S. CBDC system and its associated data breach response policies and procedures should be designed to comply with the strictest of state privacy laws, in addition to international data privacy regimes. Further, when the U.S. government initiates its process for selecting trusted intermediary financial institutions, those which do not currently meet the strictest state level data privacy requirements (or which cannot reasonably comply with the strictest state laws ahead of the chosen launch date) should not be selected to operate within the CBDC system.

As an example, various states have set timeframes for notification to individuals with respect to data breaches. Among the 50 states, Colorado currently maintains the strictest

notification timeline requirement which provides that individuals of a data breach or incident must be notified "as expeditiously as possible and without unreasonable delay, [but] no more than 30 days."[93]

Outside of the data breach context, the U.S. CBDC system should adhere to disclosure, and data security requirements set by comprehensive state privacy laws for all end-users of the system, regardless of their state of residence. For example, Colorado's privacy legislation requires affirmative consent to data processing, providing that "a controller shall not process a consumer's sensitive data without first obtaining the consumer's consent."[94] Colorado further imposes a minimum duty of care on data controllers to "take reasonable measures to secure personal data during both storage and use from unauthorized acquisition," that are "appropriate to the volume, scope, and nature of the personal data processed and the nature of the business."[95] Further, Colorado law imposes a duty for all data controllers to strive for data minimization, meaning "collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed."[96]

While this paper references Colorado's comprehensive data privacy requirements as a starting point for analysis, there are several other states that have enacted comprehensive privacy laws, including, for example, California, Virginia, and Utah.[97] It is critical that the U.S. CBDC

---

[93] *See* Colo. Rev. Stat. § 6-1-716, https://casetext.com/statute/colorado-revised-statutes/title-6-consumer-and-commercial-affairs/fair-trade-and-restraint-of-trade/article-1-colorado-consumer-protection-act/part-13-effective-712023-colorado-privacy-act/section-6-1-1308-effective-712023-duties-of-controllers; *See also State Data Breach Notification Chart*, IAPP, (Mar. 2021), https://iapp.org/resources/article/state-data-breach-notification-chart/

[94] *Id*.

[95] *Id*.

[96] *Id*.

[97] *See State Data Breach Notification Chart*, IAPP, (Mar. 2021), https://iapp.org/resources/article/state-data-breach-notification-chart/; *See e.g.* Cal. Civ. Code § 1798.100(e), https://cpra.gtlaw.com/general-duties-of-businesses-that-collect-consumers-personal-information/; *See e.g* VA. Code. § 59.1-578.3, https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-578/; *See e.g* Utah Code § 13-61-302(b)(2), https://le.utah.gov/xcode/Title13/Chapter61/13-61-S302.html?v=C13-61-S302_2022050420231231.

system's selected intermediary financial institutions take utmost care to review state data privacy laws and secure the personal identifiable information and transaction data obtained while operating the CBDC system with highly protective and compliant measures. For example, all personal identifiable information and CBDC transaction information collected and stored should be limited only to the types of data that may be required for BSA/AML purposes and all other data should be securely erased. Further, all data collected for BSA/AML purposes must be stored in a secure location using encryption tools or other similarly protective measures. Additionally, transaction or personal data transmitted to the government for legitimate BSA/AML purposes or other legitimate law enforcement purposes must, similarly, be transmitted with encryption tools or by other protective measures.

Finally, any state-imposed duty to uphold minimum data security practices should also be extended to all third-party service providers that are onboarded by the participating CBDC intermediary financial institutions to facilitate any data-related functions for the U.S. CBDC system. It is imperative that there are adequate policies and procedures mandating third-party compliance with state-level third-party service provider privacy and security requirements.

Part V: Conclusion

To remain on track with global financial system advancements, the U.S. can almost certainly expect a CBDC system in the future. As explored in this paper, how this future system is designed can have critical privacy implications on the current balance between individual privacy interests and the needs of law enforcement under U.S. privacy law. Further, a CBDC system accessible to end-users globally will face friction from international data privacy authorities. The goal of this paper and the privacy-by-design recommendations within is to assist

in planning for the longevity of the future U.S. CBDC system by prioritizing individual privacy protections and proactively anticipating scrutiny from international data privacy authorities.

To help strike the appropriate balance under existing U.S. privacy law while dealing head-on with uncertainties in state-level and international privacy regimes, the U.S. CBDC system should be: (1) intermediated by selected private sector financial institutions with robust data privacy compliance programs, (2) operated either on a centralized ledger or, pending further legal analysis and international cooperation, operated on a GDPR-compliant, private and permissioned decentralized ledger and (3) designed to comply with the strictest state data privacy and data breach notification requirements.