Digital Dollar: Privacy and Transparency Dilemma

Jiaying Jiang
University of Florida Levin College of Law, jiang@law.ufl.edu

Follow this and additional works at: https://scholarship.law.ufl.edu/facultypub

Part of the Banking and Finance Law Commons

Recommended Citation
U.C. L.J. (forthcoming 2024)
Digital Dollar: Privacy and Transparency Dilemma

Jiaying Jiang*

Abstract

Many have voiced concerns that a digital dollar, a digital form of central bank money, will facilitate government surveillance, thus depriving users of privacy. Contrary to popular belief, this Article investigates critical technical designs proposed by leading think tanks, central banks, and scholars from interdisciplinary fields, it reaches a surprising conclusion: a digital dollar can offer better privacy protection than existing digital payment systems. The Article argues that those expressing concerns have made two flawed assumptions: (1) that the digital dollar data is fully transparent regarding personal information and transaction details, and (2) that the government or the Federal Reserve has unlimited access to this fully transparent data and the potential for their misuse. In reality, the designs directly oppose these assumptions by allowing for a certain degree of anonymity, whether it be payer anonymity, transaction anonymity, or a combination of both, and by preventing government access to identity data and transaction details. The real issue is that if the digital dollar adopts these privacy-preserving designs, it will directly conflict with existing anti-money laundering and countering the financing of terrorism (AML/CFT) regulations that require transparent data to combat financial crimes. Accordingly, this Article proposes changes to financial institutions’ record-keeping and reporting practices. It also suggests modernizing AML/CFT requirements to allow a certain degree of anonymity to protect privacy while still fulfilling public interest objectives such as combating money laundering and terrorist financing.

* Assistant Professor of Law, University of Florida Levin College of Law. The author is grateful for the invitation to present this piece at the CBDC conference hosted by the Bank for International Settlements (BIS), attended by general counsels from 63 central banks, whose feedback was invaluable. Special thanks also go to industry experts Mike Alonso and Robert Oleschak from the BIS and Luca Barbatti from KPMG for their insightful discussions. The author also owes a debt of gratitude to numerous academics who shared their perspectives or reviewed and commented on this piece, including Amy Stein, Peter Molk, Saul Omarova, Tsang Cheng-yun, Yulia Guseva, Heng Wang, Chris Hampson, Matthew Kim, Kathy Hwang, Ben Johnson, and participants at the UF junior scholars’ workshop. Additionally, the hard work and support of research assistants Christopher Radcliffe, Seth Frye, and Daniel Pinkus are deeply appreciated.
Table of Contents

Introduction ............................................................................................................................................. 3

I. Central Bank Digital Currencies and the Digital Dollar .......................................................................... 8
   A. International Movement .................................................................................................................... 8
   B. Domestic Development .................................................................................................................. 11

II. Unjustified Concern: Surveillance ........................................................................................................ 15
   A. Assumptions .................................................................................................................................. 16
   B. Reality ........................................................................................................................................... 20

III. Real Challenge: Misalignment with AML/CFT Laws ......................................................................... 24
   A. AML/CFT Framework .................................................................................................................... 24
   B. Payer Anonymity Design .............................................................................................................. 27
   C. Incompatibility ............................................................................................................................. 33

IV. Modernization of AML/CFT Practices and Laws ............................................................................... 35
   A. Change practices .......................................................................................................................... 36
   B. Change laws ................................................................................................................................. 38
   C. Benefits and challenges ............................................................................................................... 40

Conclusion .................................................................................................................................................. 42

Electronic copy available at: https://ssrn.com/abstract=4774186
Introduction

In an era where digital footprints shadow every aspect of our lives, the concept of financial privacy often seems like a relic of the past. Reflect for a moment: when was the last time the notion of cash's anonymity sparked your curiosity? Or when did you last exchange physical currency for goods or services? In cash transactions, the exchange remains a private affair, known only to the parties involved. Contrast this with the digital payments landscape, where every swipe of your card or click of a button is monitored, recorded, and analyzed by an array of financial institutions. The convenience of digital transactions comes at the cost of our privacy, a price many of us have reluctantly accepted. However, as we navigate through this digital era, an intriguing question emerges: what if the government constantly monitors every aspect of our financial transactions? This concern is at the heart of the debate surrounding central bank digital currencies (CBDCs).

CBDC is a new form of central bank money.¹ Instead of printing money (i.e., banknotes and coins) in physical forms, the central bank issues money in digital form backed by the full faith and credit of the government.² One hundred and thirty countries, representing 98% of global GDP, are actively exploring CBDCs, and 11 countries have successfully issued their CBDCs.³ The movement toward digital currency is gaining unprecedented momentum. In the United States, the exploration into a CBDC, commonly referred to as the “digital dollar,”⁴ involves an in-depth examination of its feasibility and the design choices crucial for determining how Americans would engage with it. The digital dollar stands at a crossroads, with the potential to either enhance the American values of freedom and liberty or to serve as a mechanism for extensive surveillance and control over the personal financial activities of its citizens.

Introducing a digital dollar would raise multifaceted legal issues under various domains including central bank law, monetary law, financial regulation, tax law, contract law, privacy and data protection law, insolvency law, property law, and private international law.⁵ At the core of these multifaceted legal issues lies what can be termed the “privacy and transparency dilemma.”

¹ Central Bank Digital Currency Tracker, Atlantic Council, https://www.atlanticcouncil.org/cbdctracker/ (last visited Dec. 28, 2023); See also Jiaying Jiang, Privacy Implications of Central Bank Digital Currencies, 54 SETON HALL L. REV. 69, 71 (2023) (“The Federal Reserve Bank defines a CBDC as ‘a digital liability of a central bank that is widely available to the general public.’ The International Monetary Fund defines a CBDC as ‘a new form of money, issued digitally by the central bank and intended to serve as legal tender.’ The Bank for International Settlements considers a CBDC ‘a digital form of central bank money that is different from balances in traditional reserve or settlement accounts and that works as ‘a digital payment instrument, denominated in the national unit of account, [which] is a direct liability of the central bank’... Broadly speaking, CBDCs can be defined as a new form of money—a digital liability issued and guaranteed by a central bank.”)
² Id.
³ Central Bank Digital Currency Tracker, supra note 1.
In an ideal scenario, individuals expect privacy and financial transactions to remain inaccessible to unrelated parties, particularly the government. However, the government must retain the ability to access transaction details and monitor financial activities due to existing anti-money laundering and countering the financing of terrorism (AML/CFT) regulations, a set of laws requiring financial institutions to assist the government in combating financial crimes. This situation creates a substantial tension between the desire for privacy and the regulatory obligations that require transparency in financial data.

The literature on the legal aspects of CBDCs is notably scarce, with even fewer sources addressing the specific legal issues of the digital dollar. Even rarer is the discussion on privacy and transparency within the U.S. context. Arguably, the first substantial exploration of the legal aspects of CBDCs was presented in an International Monetary Fund (IMF) working paper, which offered a detailed framework for analyzing the legal foundations and treatments of CBDCs under central bank law and monetary law. However, this paper does not address critical issues related to privacy and transparency or mention the specifics of the digital dollar.

Among the limited articles that do address the legal issues of the digital dollar, the discussion on the balance between privacy and transparency is insufficient, with none offering practical solutions. For instance, Ricks et al. discuss the potential benefits of a digital dollar and advocate for a FedAccount, allowing the public to hold accounts directly with the central bank to use government-issued digital money. They raise the question of whether having anonymous payments that protect the privacy of citizens should be a policy goal for the Federal Reserve at all. Schwarcz argues that Article 4A of the Uniform Commercial Code (UCC) could serve as the foundation for a regulatory framework governing the digital dollar. He proposes amendments to the UCC to address AML concerns specific to the digital dollar, such as preventing fraudulent payment orders and safeguarding customer privacy and security. However, he does not address privacy needs and the inherent tension between privacy and AML/CFT requirements. Yadav et al. examine the regulatory complexities within the U.S. payment system, especially the interplay between state and federal jurisdictions in overseeing payment service providers, yet they do not explore the intersection of privacy with AML/CFT laws.

With scarce literature touching upon the tension between privacy and transparency, three significant gaps stand out: (1) a lack of focus on the digital dollar; (2) a general lack of exploration into whether privacy and transparency can coexist, with most literature assuming

---

6 World Econ., Privacy and Confidentiality Options for Central Bank Digital Currency 1, 13 (2021)
8 As of December 2023, approximately 400 articles on CBDCs were available on SSRN. Among these, about 50-60 articles broadly tackled legal issues, predominantly from international viewpoints, with fewer than 10 articles specifically focusing on the US context.
9 Bossu, supra note 5, at 5.
11 Id.
13 Id. at 1059–60.
they are mutually exclusive; and (3) almost no belief in the feasibility of achieving anonymity within a CBDC. Nonetheless, at least there is an agreement on the existence of an inherent tension between privacy needs and transparency requirements.

More specifically, the Deutsche Bundesbank has explored the AML/CFT legal frameworks concerning CBDC designs yet maintains that anonymity is unfeasible.15 Tsang et al. delve into the privacy concerns surrounding CBDCs from Taiwanese and international perspectives.16 They advocate for a robust disciplinary mechanism to mitigate privacy concerns but consider the anonymization of CBDC data to be impractical.17 Pocher provides a broad analysis of legal issues and the potential for anonymity in CBDCs based on their structural design.18 However, Pocher does not suggest detailed design strategies for ensuring anonymity in the digital dollar. Among central banks, the Bank of Canada has offered the most thorough analysis, discussing how a CBDC system could respect privacy while adhering to AML/CFT regulations within the Canadian framework.19 It outlines several design options yet indicates anonymity is not desired.20 The European Central Bank and the Digital Pound Foundation have discussed design choices and the possibility of anonymity and compliance with AML/CFT laws, but they are focused on European law.21

This Article fills the gap by systematically investigating the privacy and AML/CFT tension surrounding the digital dollar within the U.S. context. It challenges the notion that privacy and transparency must be sacrificed for one another, arguing for a feasible equilibrium. It further bridges the gap by arguing that a certain degree of anonymity is feasible in a digital dollar system and, most importantly, provides a path to strike a balance between privacy and transparency in the digital dollar system.

Methodologically, this Article begins by investigating the technical designs available for the digital dollar. It examines various technical proposals from leading central banks, think tanks, technical experts, and scholars. It reaches a surprising conclusion: these technical designs can enhance privacy protections more effectively than existing digital payment systems. A recurring theme from the designs is their ability to allow for certain degrees of anonymity—be it payer anonymity, transaction anonymity, or a combination of both—while ensuring that government

15 David Ballasch & Jan Paulick, The public, the private and the secret: Thoughts on privacy in central bank digital currencies, Deutche Bundesbank (2021). See also Francesco Mazzetti, The Legal Obstacles on the Road to Central Bank Digital Currency (CBDC) and the Digital Euro Case, 32 (2022) (stating that anonymity in payments is not going to happen and supporting the general consensus among many scholars that it is impossible to preserve anonymity if a CBDC is issued).

16 Cheng-Yun Tsang, Yueh-Ping Yang, & Ping-Kuei Chen, Disciplining CBDCs: Achieving the Balance Between Privacy Protection and Central Bank Independence 43 Northwestern J. of Int’l L. and Bus. 235 (2023) (While it does briefly touch upon design choices, it fails to provide specific design choices that would ensure privacy and anonymity within a CBDC).

17 Id.

18 Pocher, supra note 5 at 3-5.

19 Sriram Darbha & Rakesh Arora, Privacy in CBDC technology, Bank of Canada (June 2020) https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/ (discussing the tradeoffs and risks of higher levels of privacy within a CBDC system, but is in the Canadian context and does not discuss the United States’ regulatory requirements or policy objectives).

20 Id. at 269-270.

entities cannot access identity data and transaction details. Those who express surveillance concerns or fear of losing privacy are operating under incorrect assumptions about the nature of data being fully transparent and government entities having unlimited access to this data, with the potential for abuse.

The Article then addresses a real challenge: introducing privacy-preserving designs for the digital dollar may lead to conflicts with existing AML/CFT regulations. Utilizing Project Tourbillon—a proposal advocating for payer anonymity within transactions—as a case study, it delves into the potential clashes between payer anonymity and the stringent record-keeping and reporting mandates mandated by AML/CFT regulations. This exploration exposes intricate dynamics between the desire for privacy in transactions and the increasingly rising trend towards greater transparency demand by law enforcement agencies in recent years.

In mitigating this crucial conflict, the Article calls for a thoughtful modernization of AML/CFT laws. The objective is twofold: to safeguard user privacy by allowing for certain levels of anonymity and not sacrificing the effectiveness of identifying and mitigating the risks of money laundering and terrorist financing. It recommends modifications to the compliance practices of financial institutions, particularly concerning their data collection and management strategies within the digital dollar system. It also proposes specific amendments to the record-keeping and reporting requirements under AML/CFT regulations. The proposed changes not only reconcile the need for privacy with the transparency mandates but also pave the way for a more balanced and efficient financial ecosystem.

This Article makes significant contributions at both theoretical and practical levels. Theoretically, it addresses a critical gap in the existing literature, which predominantly focuses on macroeconomic issues, monetary policy, financial inclusion, international relations,

22 Jorge Abad et al., "CBDC and the Operational Framework of Monetary Policy" 2 (Bank for Int’l Settlements, Working Paper No. 1126, 2023); see also Schwarcz, supra note 12, at 1051–52; see also Saule Omarova, *The People’s Ledger: How to Democratize Money and Finance the Economy*, 74 VAND. L. REV. 1231, 1288 (2021) (hereinafter Omarova, *The People’s Ledger*) (finding that if the Fed issued a CBDC, it would have a ripple effect that reduced the overbearing effects of certain actors in the current finance field, such as too big to fail banks or “shadow banking” entities such as money market mutual funds); Saule Omarova et al., *Hidden Fallacies in Corporate Law and Financial Regulation: Reframing the Mainstream Narratives*, 23–27 CORNELL LEGAL STUD. RESCH. PAPER SERIES 1, 14–15 (forthcoming 2024) (hereinafter, Omarova, *Hidden Fallacies*) (finding that there is a common misconception in understanding financial innovations in the context of individual market transactions and not the context of the macroeconomic landscape). See also Shen Wei & Heng Wang, *Global Stablecoins and China’s CBDC: New Moneys with New Impacts on the Financial System?*, 41 REV. OF BANKING & FIN. L. 258, 283–84 (2021).

23 Abad supra note 22; See also Omarova, *The People’s Ledger*, supra note 22, at 1259 (discussing the possibility of credits and debits to FedAccounts as a method to control the money supply); Omarova, *Hidden Fallacies*, supra note 22, at 27–29 (finding that a CBDC and the roles of existing bank deposits can coexist, but that the public nature of a CBDC would place it at the top of the financial hierarchy); Michael Kumhof, *Central Bank Money: Liability, Asset, or Equity of the Nation?*, 20–46 CORNELL LEGAL STUD. RESCH. PAPER SERIES 1, 38 (2020) (finding that central bank money, like retail CBDC, is best managed not through inflation like cash, but instead through adjustments in balance sheet assets and liabilities and interest rates on retail CBDC). See also Marco Dell’Erba, *Stablecoins in Cryptoeconomics: From Initial Coin Offerings to Central Bank Digital Currencies*, 22 N.Y.U. J. OF LEGIS. AND PUB. POL’Y 1, 37–38 (2019).


technical designs,\textsuperscript{26} and institutional designs.\textsuperscript{27} Diverging from this trend, this Article uniquely concentrates on the legal challenges and solutions associated with the digital dollar. This unique perspective broadens the scope of the CBDC conversation and pioneers an exploration into the legal intricacies within the U.S. context. By delving into how a digital dollar would navigate the complex landscape of privacy demands and transparency mandates, this work illuminates the underexplored nuances of the AML/CFT legal framework, offering a fresh viewpoint on the digital dollar's potential misalignment within this system.

At the practical level, this Article serves as an invaluable resource for policymakers, guiding them through the complex legal challenges. This Article is timely, given the ongoing debate in the U.S. about whether to issue a digital dollar.\textsuperscript{28} Despite criticisms of the U.S. lagging behind in researching and adopting this new technological innovation—compared to other countries, where 19 of the G20 nations are now in the advanced stage of CBDC development, and 11 countries have fully launched their CBDCs—this Article helps policymakers make better-informed decisions through a legal lens. Although this Article remains neutral on whether the U.S. should issue a digital dollar, it offers crucial insights into the design, deployment, and legal framework considerations, responding to urgent inquiries outlined in President Biden’s executive order.

In addition to contributions to policymakers, another practical contribution of this Article is its role in addressing and dispelling the unjustified concerns that both the general public and scholars may have regarding the purposes of a digital dollar. It provides an objective analysis that empowers the public to form informed conclusions rather than being swayed by political rhetoric. By debunking common misconceptions, this Article encourages scholars to delve into the technicalities and collaborate with technologists to form a more nuanced understanding of the digital dollar, rather than jumping to hasty conclusions about its use.

To clarify, this Article does not argue that a digital dollar, or CBDCs in other countries, cannot be used for government surveillance. It certainly can be and would be an effective tool if governments intend to use it as such and can achieve it through institutional and technical designs. However, this Article recognizes that government surveillance through finance is certainly not what most citizens desire. Through investigations into existing technical designs by leading institutions and experts, it concludes that current efforts largely reflect citizens’ desires.


\textsuperscript{27} Auer, supra note 26, at 85. See also Omarova, The People’s Ledger, supra note 22, at 1261–62 (positing that a potential design for FedAccounts could be a two-tiered system, with a “reserve sub-account” that would be subject to de-issuance should the need ever arise); Omarova, Hidden Fallacies, supra note 22, at 24 (finding that financial innovations, such as CBDC can originate from both private and public actors); Kumhof, supra note 23, at 13 (finding that the notion of over-issuance of retail CBDC relies on the assumption of a fixed interest rate, which it posits could be an alternative solution to over-issuance). See also Tsang, supra note 16, at 258–60. See also Dell’Erba, supra note 23, at 14–15.

\textsuperscript{28} Saule Omarova, Financial Innovation: Three Fallacies in the Debate, 23–27 CORNELL LEGAL STUD. RsCH. PAPER SERIES 1, 3 (forthcoming 2024).

\textsuperscript{29} Id. at 3–4.

\textsuperscript{30} Atlantic council, supra note 1.
for privacy. These efforts demonstrate a commitment to preventing the use of CBDCs as tools of surveillance. This insight is particularly vital, highlighting the Article's contribution toward demystifying the functionalities of a digital dollar and fostering an environment where public and academic discourse is informed by facts and thorough, objective analysis rather than fear or speculation.

This Article is structured as follows: Section I describes the fundamentals of CBDCs, the popular debates surrounding them, international efforts on CBDCs, and domestic advancements in developing the digital dollar. Section II addresses a prevalent but unfounded concern: the fear that the digital dollar might serve as an instrument for governmental surveillance, thereby eroding user privacy. Section III delves into the real problem in the U.S. context: privacy preserving designs of a digital dollar could clash with existing AML/CFT regulations. Section IV advocates for changes to financial institutions’ record keeping and reporting practices and the modernization of AML/CFT laws to permit certain degrees of anonymity, thereby balancing the need for privacy protection and the pursuit of public interest objectives.

I. Central Bank Digital Currencies and the Digital Dollar

The international movement on CBDCs is rapidly gaining momentum as countries around the globe explore and pilot their own digital currencies. Nations such as China with its digital yuan, the U.K. and Japan with their prototypes, the Bahamas with the sand dollar, and the European Central Bank with its ongoing exploration of a digital euro are leading the charge. These efforts highlight a growing recognition of the potential for CBDCs to enhance financial efficiency, bolster economic inclusion, and secure national financial sovereignty in the digital age.

Domestically, the United States is cautiously advancing its exploration of the digital dollar, recognizing the need to balance innovation with security and privacy. The Federal Reserve has been engaging in research and development efforts, highlighted by the release of discussion papers and the solicitation of public and expert opinions on the potential benefits and risks of a digital dollar. However, stakeholders have expressed a broad spectrum of concerns and hold divergent opinions. These differences have notably slowed the pace of research and development efforts related to the digital dollar, highlighting the challenges associated with rolling out a digital dollar in the United States.

A. International Movement

CBDCs can be categorized into two types: wholesale and retail. Wholesale CBDCs are specifically designed for financial institutions holding reserve deposits with a central bank. They are not available to the general public. Given that many central banks reserve accounts have already transitioned to digital formats, wholesale CBDCs in a technical sense, are already a part of the modern financial infrastructure. On the other hand, retail CBDCs are designed for widespread use by the general public and businesses. This Article focuses exclusively on retail CBDCs.

31 Mazzetti supra note 15, at 11; See also Bossu, supra note 5, at 9; See also Annea Kosse & Ilaria Mattei, Making Headway – Results of the 2022 BIS Survey on Central Bank Digital Currencies and Crypto, Bank for Int’l Settlements 2 (July 2023) https://www.bis.org/publ/bppdf/bispap136.pdf.
32 Wouter supra note 11, at 9; See also Mazzetti supra note 15, at 8; See also Kosse supra note 31, at 2.
33 Schwarcz, supra note 12, at 1051.
34 Kosse supra note 31, at 2.
Designing a CBDC entails considerable nuances, including choosing between a one-tier or two-tier system.\textsuperscript{35} In a one-tier system, the central bank issues a CBDC directly to the general public.\textsuperscript{36} In a two-tier system, the central bank issues a CBDC to financial institutions, such as commercial banks, which then distribute the CBDCs to the public.\textsuperscript{37} Another critical decision is choosing between an account-based CBDC and a token-based CBDC.\textsuperscript{38} In an account-based model, the ownership of the digital currency is tied to an individual's identity, similar to how bank accounts operate.\textsuperscript{39} The claims are represented in a database that records the value along with a reference to the identity of the account holder.\textsuperscript{40} In a token-based model, ownership and transfer of CBDCs are authenticated by cryptographic tokens rather than being tied to an individual's identity.\textsuperscript{41} This Article only addresses two-tier and account-based CBDCs.

Common motivations to explore and potentially issue CBDCs across the globe include promoting financial inclusion by providing easy and safer access to money for unbanked and underbanked populations;\textsuperscript{42} introducing competition and resilience in the domestic payments market, which might need incentives to provide cheaper and better access to money;\textsuperscript{43} increasing efficiency in payments and lowering transaction costs;\textsuperscript{44} creating programmable money and improving transparency in money flows;\textsuperscript{45} and providing for the seamless and easy flow of monetary and fiscal policy.\textsuperscript{46} Each of these motivations has been extensively debated. It is crucial to recognize that while these are the goals central banks aim to achieve with CBDCs, the actual outcomes remain to be seen.\textsuperscript{47}

A popular debate on the need for a CBDC often stems from the belief that money is already digital, as seen in online banking and various digital payment tools.\textsuperscript{48} This perspective, however, misunderstands the nature of a CBDC. A CBDC is not simply another payment technology.\textsuperscript{49} As a direct liability of the sovereign government, a CBDC’s place is at the very top of the money hierarchy.\textsuperscript{50} It can be a uniquely potent level of structural change, the core element of a qualitatively new—more efficient, stable, and democratic—financial ecosystem.\textsuperscript{51} Realizing

\textsuperscript{35} Auer, \textit{supra} note 26, at 88-89. In addition to the design options highlighted here, there are numerous other considerations in the design of a CBDC, such as whether it should bear interest, be subject to quantitative limits, and the methods for its conversion into cash or bank deposits, among others. Each of these design choices carries distinct functionalities, involves specific trade-offs, and has varying implications for different stakeholders.

\textsuperscript{36} Id.

\textsuperscript{37} Id.

\textsuperscript{38} Id. at 93.

\textsuperscript{39} Id.

\textsuperscript{40} Id.

\textsuperscript{41} Id. at 93-94.

\textsuperscript{42} Exec. Order No. 14,067, 87 Fed. Reg. 14,143, 14,143 (Mar. 14, 2022); \textit{See also} Yesha Yadav, \textit{supra} note 14, at 64-68; \textit{See also} Kosse \textit{supra} note 31, at 6-7.

\textsuperscript{43} Kosse \textit{supra} note 31, at 9.

\textsuperscript{44} Id. at 6-7; \textit{See also} Yadav \textit{supra} note 14, at 25–27; \textit{See also} Morgan Ricks, \textit{Money as Infrastructure}, 2018 Colum. Bus. L. Rev. 756, 830-31.


\textsuperscript{46} Central Bank Digital Currency Tracker, \textit{supra} note 1; \textit{See also} Kosse \textit{supra} note 31, at 6-7.

\textsuperscript{47} Jiang, \textit{supra} note 1 at 85–91.


\textsuperscript{49} Omarova, \textit{supra} note 29, at 29.

\textsuperscript{50} Id.

\textsuperscript{51} Id.
this potential requires policymakers to think beyond the basic payment frame.\textsuperscript{52} Policymakers must acknowledge the implications of changing the nature and composition of central banks’ primary liabilities.\textsuperscript{53} Currently, central banks’ primary liabilities to the general public are in physical form, such as federal reserve notes and coins in the United States. Moving from physical to digital form “can change the entire relational dynamics between the central bank, private finance and the broader economy.”\textsuperscript{54}

This perspective also misunderstands the key distinction between central bank money and commercial bank money. Commercial bank money refers to the type of money created through commercial banks’ fractional reserve banking system when they provide loans or credit to businesses or individuals.\textsuperscript{55} This money is a promise by the bank to pay the deposit holder a certain amount.\textsuperscript{56} Commercial bank money is not physical cash but rather exists as digital or ledger entries on a bank’s balance sheet. When individuals check their balance, what they see is commercial bank money, digits that represent a bank’s promise to pay. The promise is reflected in their ability to withdraw or transfer funds as needed.\textsuperscript{57} Unlike central bank money, commercial bank money is not a liability of the government or the central bank. It is the liability of the individual bank that issues it.\textsuperscript{58}

This difference is significant for risk: central bank money carries no credit risk, while commercial bank money does carry the risk of bank default. Depositors might lose their money if a commercial bank becomes insolvent, while central banks, which can keep issuing money and serve as lenders of last resort, are unlikely to fail the same way commercial banks do.\textsuperscript{59} Therefore, central bank-issued money is often considered safer than that from commercial banks.\textsuperscript{60} Nevertheless, the advantage of CBDCs in this sense may be small for consumers in countries like the United States, which has robust regulations and government backstops that ensure people do not lose funds if their financial institutions fail.\textsuperscript{61} However, in countries without credible accountholder protections, CBDCs may offer useful security benefits.\textsuperscript{62}

Recent developments in CBDCs have been notable. According to data from the Atlantic Council, out of 131 tracked countries, 11 have launched CBDC initiatives, 21 have implemented pilot programs, 33 are developing CBDCs, 46 are researching CBDCs, 16 are inactive, and two have canceled CBDC projects.\textsuperscript{63} Nearly 60\% of central banks have cited the continued rise of

\begin{itemize}
  \item \textsuperscript{52} Id.
  \item \textsuperscript{53} Id.
  \item \textsuperscript{54} Id.; See also Omarova, \textit{The People’s Ledger}, supra note 22, at 1253.
  \item \textsuperscript{55} Tsang, \textit{supra} note 16, at 247–48.
  \item \textsuperscript{56} Id.
  \item \textsuperscript{58} Tsang, \textit{supra} note 16, at 247–48.
  \item \textsuperscript{60} Id. See also e.g., Sverige Riskbank, \textit{Payments & Cash: E-krona}, \url{https://www.riksbank.se/en-gb/payments-cash/e-krona}.
  \item \textsuperscript{61} Id. In the United States, the Federal Deposit Insurance Corporation (FDIC) provides insurance up to $250,000 per account, offering some degrees of protection to depositors. However, such safeguards may not be available in other jurisdictions.
  \item \textsuperscript{62} Id.
  \item \textsuperscript{63} Central Bank Digital Currency Tracker, \textit{supra} note 1; See also Kosse \textit{supra} note 31, at 4-6 (noting that 93\% of central banks have engaged in some form of CBDC research, and more than half of central banks are engaging in concrete experiments or pilots).
\end{itemize}
cryptoassets and stablecoins as catalysts to accelerate their work on CBDCs. Notably, the European Central Bank (ECB) has transitioned to the preparation phase of its digital euro initiative and cites the need to make public money available for digital payments and to strengthen the monetary sovereignty of the euro area for its continued development. The Bank of England and the Bank of Japan are developing CBDC prototypes and consulting the public and private sectors on privacy and financial stability issues. China started research in 2014 and has been piloting a digital yuan program since 2020. The pilot program has reached 260 million people in 25 cities, and the digital yuan is being tested in over 200 scenarios, some of which include public transit, stimulus payments, and e-commerce. Some government employees have even begun receiving the digital yuan for their salaries.

B. Domestic Development
These international developments have urged the United States to evaluate the feasibility of a digital dollar more intensely. In this context, recent updates include President Biden's executive order on ensuring responsible development of digital assets, where he recommended safe research and development of a US CBDC, particularly in data and financial security and accessibility.

The executive order outlined three major categories of risk that need navigating in the continued development of the digital dollar. These three categories are financial risk, systemic risk, and national security risks. Within financial risk there are concerns about money laundering, terrorist and proliferation financing, fraud and theft schemes, and corruption. The biggest solution to these worries will be the design and implementation of the digital dollar in the scope of the financial system at large. Systemic risk is mostly concerned with navigating macroeconomic risks to financial stability. Here, concerns look like potential bank runs, low confidence in the digital dollar, or a worry about over or under-inflation. Finally, National

64 Kosse supra note 31, at 1-2; See also Fed Rsrv., supra note 4, at 14-16 (citing improvements to private-sector innovation, cross-border payments, the international value of the US dollar, financial inclusion, and public access to safe and stable central bank money.; See also Kosse supra note 31, at 13-15.
66 Central Bank Digital Currency Tracker, supra note 1.
68 Central Bank Digital Currency Tracker, supra note 1.
71 Id.
72 Id.
73 Id.
74 OFFICE OF SCI. AND TECH. POL’Y, TECHNICAL DESIGN CHOICES FOR A U.S. CENTRAL BANK DIGITAL CURRENCY SYSTEM (Sep. 2022).
security risks are concerned with cybersecurity, data privacy and security, protecting human rights, combating and preventing crime, and international sanctions. These risks range in scale from individual concerns, such as individual accounts being hacked, or data being leaked, to large-scale problems such as sanctions or human rights enforcement.

The benefits to researching, developing, and implementing the digital dollar mostly mirror the potential risks of unwisely or inadequately researching, developing, or implementing the digital dollar. First, a digital dollar could increase financial inclusion and equity. A digital dollar could reach individuals who are unbanked or underbanked, and by encouraging the creation of an account with the federal reserve, or an authorized distributing bank of the digital dollar. Next, continued research and development into technologies that will facilitate a digital dollar could assist with technological innovations, such as quantum computing. In a similar vein, working with ledger technologies, including their research and development for a digital dollar, could lead to cybersecurity innovations that could improve cybersecurity techniques going forward. Next, unrelated processes and technologies, such as energy demands or climate change, could have novel technologies or strategies applied to them, based on the development of the digital dollar, such as new machine learning techniques. Finally, a digital dollar could represent a massive improvement in financial stability and economic strength, such that the United States could change and expand its foreign policy to exercise, support, and enforce human rights globally.

The executive order, in acknowledging these potential risks and benefits called for several risk assessments in the wake of this executive order, including: the National Money Laundering Risk Assessment, the National Terrorist Financing Risk Assessment, the National Proliferation Financing Risk Assessment, and the updated National Strategy for Combating Terrorist and Other Illicit Financing. After these risk assessments are completed, the United States will seek to mitigate these risks through regulation, supervision, public-private engagement, oversight, and law enforcement. Following the executive order, the Office of Science and Technology has published a report on the technical feasibility of a digital dollar.

The Federal Reserve Bank of Boston and MIT have tested the underlying technology since 2020 and published two reports titled “Project Hamilton.” Project Hamilton suggested decoupling transaction validation from execution, ensuring that the transaction format and protocol are secure and providing flexibility for potential functionality, such as self-custody,

---

78 Nir Kshetri & Elena Loukoianova, Data Privacy Considerations for Central Bank Digital Currencies in Asia-Pacific Countries, 55 COMPUT. 95, 97–98 (Mar. 2022).
80 Yadav, supra note 14, at 64–68.
85 Id.
programmability, and efficiency. Project Hamilton emphasizes that policy and design are interconnected, and that a successful implementation will require novel solutions to balance these to achieve the end-goals, such as financial stability or financial inclusion.

The most important finding of Project Hamilton is that the design choices of the digital dollar are much more granular than previously thought, which has wide ranging ramifications on several key aspects of a digital dollar. First, rather than simply making a choice between a “token-based” or “account-based” digital dollar, design choices must be made regarding the trust and threat models of the digital dollar, the transaction format, and the fault-tolerance scaling strategies underlying the implementation of the digital dollar. Second, existing technologies and financial strategies such as distributed systems and blockchain technologies can be combined in unique ways to improve scalability, privacy, intermediation strategies, and auditability, however, these goals must be realized in order to research the underlying technology. Finally, it finds a trade-off between user-to-user privacy and making transactions visible to track whether a transaction has occurred. Specifically, unlike current public cryptocurrencies, where all transactions are available to be seen publicly, but the lack of other identifying information prevents user’s identities from being compromised, a different solution must be chosen for a digital dollar. This is because Project Hamilton recommends that the central bank limit its data storage to account information and transaction information for pending transactions.

In terms of design choices, Project Hamilton also made two design recommendations regarding scalability and data storage. It found that in order to maximize the throughput of transactions and lower latency, scalability is best achieved through vertical scalability. Regarding data storage, the central bank should only retain the information pertinent to unspent funds. Unspent funds are the most important to track server-side because the bank must prevent these funds from being double-spent. In this design, the central bank would merely provide parties with receipts for past transactions, called preimages, which would also be used by parties to facilitate the original payment.

In the Office of Science and Technology Policy’s report on the technical feasibility of the digital dollar follows the recommendation of Project Hamilton to establish goals to guide the technical design of the digital dollar. The office establishes the policy objectives of the digital dollar to expand equitable access to the financial system, preserve the role of physical cash, only collect strictly necessary data, be sustainable, and be functional. The report analyzes eighteen major design choices and lists their pros and cons, but only makes one major recommendation. It recommends that the digital dollar could technically be permissionless, but points out that

---

89 Id. at 3.
90 Id. at 31.
91 Id. at 30.
92 Id.
93 Id.
94 Id. at 31.
95 Id.
96 Id. at 24–25.
98 Id. at 28.
99 Id. at 24–25.
100 Id. at 31.
102 Nelson, supra note 87.
being permissionless does not make sense for a system that has a trusted entity, such as the Federal Reserve.\textsuperscript{104}

Regarding the necessity of issuing a digital dollar, opinions vary. Governor Christopher J Waller, a Federal Reserve Board of Governors member, described it as "a solution in search of a problem."\textsuperscript{105} Governor Waller rejects the notion that foreign CBDCs, most notably China’s E-CNY, will undermine the primacy of the U.S. dollar because he claims that non-Chinese firms will not see enough benefit from the switch to outweigh the surveillance concerns of the Chinese government through E-CNY.\textsuperscript{106} Even if this was a concern, Governor Waller claims that distributing a digital dollar would not solve these concerns about U.S. dollar primacy by making it available to American households to “pay their electric bills via a Federal Reserve [digital dollar] account instead of a commercial bank account.”\textsuperscript{107} Additionally, Governor Waller claims that its threat to privacy far outweighs any potential benefit derived from the digital dollar. These privacy concerns include federal surveillance on the financial activities of its citizens, foreign terrorist financing, or illicit financial transactions like money laundering.\textsuperscript{108} Finally, Governor Waller claims that any concern to the stability of the U.S. dollar can be solved adequately by private sector financial innovations, such as cryptocurrencies that are tied to the value of the U.S. dollar.\textsuperscript{109}

Meanwhile, Jerome Powell, the Federal Reserve Chairman, has stated that there is no urgency to issue a digital dollar, and the Federal Reserve will not issue a digital dollar without congressional approval.\textsuperscript{110} Because of the executive order by President Biden, Chairman Powell feels that there is currently a mixed message surrounding the development of a digital dollar, and is resistant to develop one without explicit permission from all angles for fear of backlash.\textsuperscript{111} This approach that American leadership needs to be a united front before the development of the digital dollar can occur is very unique. In comparison to Governor Waller’s position that a digital dollar should never be researched, developed, or issued, Chairman Powell’s position is that without complete approval, the development of a digital dollar should not begin, however, with approval, the development could begin.

Conversely, Treasury Department reports under Treasury Secretary Yellen have been interpreted as positive towards the development and potential of a digital dollar.\textsuperscript{112} Secretary Yellen recognizes that there may be some benefits to digital currency, such as increased financial

\textsuperscript{104} Id. 6.
\textsuperscript{106} Waller, supra note 71.
\textsuperscript{107} Id.
\textsuperscript{108} Id.
\textsuperscript{109} Id.
\textsuperscript{111} Id.
\textsuperscript{112} Fatima Hussein, Treasury Recommends Exploring Creation of a Digital Dollar, A.P. NEWS (Sep. 16, 2022, 12:29 PM), https://apnews.com/article/cryptocurrency-biden-technology-united-states-ae9e8d1d16deeb2fab48edbb2e49f0e.
stability or financial inclusion, however, it is impossible to do much beyond speculate as to these benefits without doing the underlying research and development. Specifically, Secretary Yellen acknowledges that some aspects of the existing financial system are too slow and too expensive, but without researching CBDCs, determining if one could fix these issues is not possible. Further, Secretary Yellen believes that knowing the underlying design policies, strengths and weaknesses, and concepts will help equip the United States to better deal with contemporary monetary policy abroad, even if it chooses not to develop and issue a digital dollar because other countries will issue a CBDC. For all of these reasons, Secretary Yellen believes that researching, and potentially developing, CBDCs are in the United States’ best interests, even if it never winds up issuing the digital dollar. This outlook is markedly more positive towards CBDCs than Governor Wallen, and potentially Chairman Powell, although he chooses not to speak on the merits of a CBDC at all.

A few scholars advocate for introducing the digital dollar. Yadav et al. critique the current U.S. payment system as being outdated and inefficient. A digital dollar could be one of the innovations to modernize the U.S. payment system. Omarova sees advantages in issuing a digital dollar, including the potential to diminish the roles of traditional financial institutions, such as too-big-to-fail banks or “shadow banking” institutions like money market mutual funds. Ricks and his colleagues argue that the most appealing strategy for implementing a digital dollar is broadening access to the Federal Reserve’s accounts, which are currently limited to a small, favored set of clients (i.e., banks and government entities). They recommend making these accounts, termed “FedAccounts,” accessible to the general public, including individuals, businesses, and other institutions.

II. Unjustified Concern: Surveillance

The CBDCs and the United States' digital dollar have undeniably captured significant attention and momentum, attracting a wide array of stakeholders whose views diverge considerably. These perspectives range from those grounded in evidence-based analysis to others that are more speculative in nature. This section addresses a common but unfounded concern that CBDCs serve as a tool for financial surveillance, depriving citizens of privacy. This fear is based on incorrect assumptions that CBDC data is fully transparent, and that the governments or central banks have unfettered access to personally identifiable information and transaction details. However, an investigation into the latest technical designs reveals that they actually bolster privacy protections by allowing for certain degrees of anonymity, whether it be payer anonymity, transaction anonymity, or a combination of both. Contrary to these concerns, governments or central banks will not have unlimited access to personally identifiable information and transaction details.

113 Id.
114 Id.
115 Yadav, supra note 14, at 3 (explaining the inefficiencies of the United States’ financial system, including its routine financial exclusion and outdated architecture).
116 Id.
117 Omarova, The People’s Ledger, supra note 22, at 1253.
118 Ricks, supra note 44, at 840.
119 Id.
A. Assumptions
Many politicians have voiced concerns that the digital dollar could become a tool for surveillance. In the United States, republican representatives like Tom Emmer and French Hill have expressed apprehension about the digital dollar leading to increased government surveillance. Hill, in particular, has highlighted the potential for more significant data collection and privacy issues associated with a government-backed digital dollar. Similarly, Florida’s Governor Ron DeSantis and officials from a few other states such as North Carolina, Utah, South Carolina, South Dakota, and Tennessee, have indicated a desire to ban the digital dollar. These states argue that a digital dollar could infringe on citizens’ financial privacy and autonomy, reflecting a growing skepticism towards digital currencies under government control.

The sentiment is not limited to politicians but is echoed by the general public. A survey conducted by the European Union indicated that a majority of the respondents believed privacy should be the most important feature of any digital currency. Additionally, in a series of town hall meetings in the United States, citizens frequently raised concerns about financial privacy in

---

120 Governor Ron DeSantis Signs First-in-the-Nation Legislation to Protect Against Government Surveillance of Personal Finances, FL Gov. (May 12, 2023) https://www.flgov.com/2023/05/12/governor-ron-desantis-signs-first-in-the-nation-legislation-to-protect-against-government-surveillance-of-personal-finances/ (Press release that highlights a law, SB 7054, passed by Governor Ron Desantis that expressly prohibits the use of a federally adopted CBDC by excluding it from the definition of money within Florida’s Uniform Commercial Code. Florida has passed this law in order to prevent perceived unprecedented government overreach that would jeopardize privacy rights and increase government control through the issuance of a CBDC. This clearly indicates a fear and concern about potential privacy violations that could be inherent in a CBDC if it is designed incorrectly).

121 Sandali Handagama, North Carolina House Unanimously Votes to Ban Digital Dollar Payments to the State, CoinDesk (May 4, 2023) https://www.coindesk.com/policy/2023/05/04/north-carolina-house-unanimously-votes-to-ban-digital-dollar-payments-to-the-state/ (Stating that North Carolina’s House of Representatives unanimously passed a bill prohibiting the state’s agencies and institutions from accepting payments in central bank digital currencies including a Federal Reserve issued digital dollar. The bill also bans states from participating in any pilot tests for CBDCs).

122 David Pokima, United States Lawmakers Introduce Bills to Exclude CBDCs from the Definition of Money, Cryptonews (Jan. 17, 2024) https://cryptonews.com/news/united-states-lawmakers-introduce-bills-to-exclude-cbdc-from-the-definition-of-money.htm (Describing proposed bills in South Carolina, South Dakota, Tennessee, and Utah that are seeking to prevent CBDCs from being considered legal tender in the states by simply stating that CBDCs are not legal tender or that money as a medium of exchange does not include CBDCs)

123 Id.

124 Id.

125 Id.

126 Amaka Nwaokocha, Multiple US Senate bills object to CBDC’s definition of ‘money’, Coin Telegraph (Jan. 17, 2024) https://cointelegraph.com/news/us-senate-bills-exclude-cbdc-money-definition and https://www.cryptopolitan.com/u-s-states-inclusion-of-cbdc-legal-tender/ (Re-iterating that multiple states are introducing bills or have passed bills to prevent or limit the use of CBDCs within their states by defining money as not including CBDCs within their definitions).

127 Peter Goettler, CBDCs Threaten Privacy, CATO Institute (June 26, 2023), https://www.cato.org/commentary/cbdc-threaten-privacy (Arguing that the issuance of a CBDC would endanger financial privacy even more than it has in recent years and would serve as a capstone for expanding financial surveillance by making every financial transaction available to the government by default).

128 Euro. Cent. Bank, Eurosystem report on the public consultation on a digital euro, 10 (2021) (Stating that 43% of respondents to this survey stated that privacy was the most important feature that they wanted to see in a CBDC).
the context of the digital dollar. Similarly, a report from a think tank in Asia highlighted the privacy concerns of the general public as a battleground for the power struggle between political leaders and central banks as many central banks do not require the user data of a CBDC to achieve their mandates but other government agencies may find the information to be very useful. Canadian citizens are also immensely concerned with financial privacy, yet do not trust the institutions responsible for handling data privacy and protection. Canadian sentiments for a Canadian CBDC are extremely low with 86% of respondents to a survey expressing strong criticisms against a Canadian CBDC and 52% of respondents considering it a bad idea that they have no intention of using.

See Public Comments Received on Money and Payments: The U.S. Dollar in the Age of Digital Transformation, Board of Governors of the Federal Reserve System (June 24, 2022), https://www.federalreserve.gov/cbdc-public-comments.htm (Detailing nine large pdf documents that contain the many public comments that were received by the Federal Reserve after publishing their paper about a potential U.S. CBDC. Regularly echoed throughout the various public comments is the concern that a digital dollar will be abused by the central government or will result in privacy violations. A general distrust of the government and the way that they may manage a digital dollar appears very pervasive throughout the many public comments on this issue).

Digital Canadian Dollar Public Consultation Report, FORUM Research 40 (Nov. 2023) (Providing the statistics mentioned above as well as several comments that participants in the survey shared after the survey. Below are several statements indicating public sentiment toward a Canadian CBDC.

1. “A digital dollar sounded great until we saw the Federal government freeze private bank accounts of its own citizens for supporting a political movement it disagreed with. I have no faith at all in the system anymore.”
2. “As I have already stated, I do not see the reason or benefit of a digital dollar. Cash is accessible to everyone. Cash is private, cash is senior friendly, cash is disability friendly, cash is as secure as the individual makes it, cash is there and readily available, and cash is already legal tender.”
3. “I am deeply concerned about privacy and freedom. Already, most of our transactions are linked to our personal information and are traced by many entities, which I find disconcerting. Additionally, a digital Canadian dollar would mean that the government would, in theory (and very likely in practice) control access to money for its citizens. This will surely lead to tyranny, and I do not wish to live in such a state. Control over money is a potent instrument for oppression and forced obedience. I cannot imagine a CBDC being compatible with our values of liberty and privacy.”
4. “I think it is a horrible idea and just one more way the government can control and track us. Cash is easy and it is anonymous, and it has been the way for thousands and thousands of years. Nobody can hack into cash. Cash is foolproof. Kids can use cash. What happens to the homeless? They can't afford a phone or computer to access this digital money. They rely on cash. The world [relies] on cash. When I go to another country I take out [cash] as every country has their own currency. What happens when the bank gets hacked or the bank goes bankrupt? All of our money is gone. With cash we can take it out and it's physically with us. It's a safety net. I am very against this digital dollar.”
5. “Digital dollars will be tracked by all banks, all federal agencies and the [government]. They will be programmed to control what people buy, how much accessed at a single time, carbon footprint, political party affiliations, religion, and every other possible aspect of your personal life.”
6. “Initially when something is launched we are promised no fees are attached to this. But as time passes there are always fees attached. Regardless of this survey, the BOC is going to do this no matter what. Make it for the people and not the banks and their greed.”
7. “Think of how quickly this has the potential to go wrong with the wrong people in power.”
Scholars have also scrutinized CBDCs, raising privacy concerns. Academics argue that the digital nature of CBDCs inherently increases the potential for surveillance from the central bank or other government agencies that may find private financial data useful. Many point out that, unlike physical cash, digital transactions leave a digital trail that can be easily monitored and analyzed. This capability could lead to unprecedented levels of government oversight and control over individual financial transactions, fundamentally altering the relationship between the state and its citizens in terms of financial privacy and autonomy. Scholars ultimately recognize that all means of payment provide varying degrees of privacy or anonymity, ranging from requiring the bank to monitor transaction and identity data, to anonymous transactions in cash, and CBDCs must incorporate privacy into its design to satisfy the concerns of the general public.

But what does privacy mean in this context? Defining privacy has been challenging. There are six conceptions of privacy but each of them is either overly broad or unduly narrow. They all fail to effectively capture the dynamics of CBDCs. In my prior work, I argued privacy must be understood contextually. Privacy should not be viewed as a separate, abstract concept but rather “a dimension of certain practices and aspects of life.” In the context of CBDCs, it is crucial to identify the actors involved in CBDC payments, understand the nature of the information shared, and determine which aspects of this payment practice should be kept private and from whom. Thus, when we state that we are “protecting privacy,” we are essentially

8. “Canadians do not need a digital dollar, there is already one in place. It is your debit card.”

9. “It’s the beginning of the end of freedom.”

10. Id. at 104 (critiquing six categories of conceptions of privacy and explaining why each conception is either too broad or too narrow). See also World Econ. F., supra note 6, at 17; Ruth Gavison, Privacy and the Limits of Law, 89 Yale L.J. 421, 422 (1980) (lamenting the lack of a useful, distinct and coherent concept of privacy).
committing to safeguard specific practices from unauthorized disruptions. What should be considered private is a normative argument and may vary across jurisdictions, cultures, and times. When conducting normative analysis, it is necessary to balance the value of privacy and other conflicting values.

Unfortunately, numerous assumptions regarding the privacy implications of CBDCs have been made. This Article argues that the prevailing narrative, which suggests that CBDCs inherently compromise privacy and facilitate surveillance, is based on wrong assumptions.

The first assumption is that all data within the CBDC system will be fully transparent and unencrypted, suggesting that anyone with access to this data could gain detailed insights into an individual’s spending habits, financial status, and personal preferences. This sensitive data typically encompasses personal identity information and specific transaction details. The second assumption concerns the governance of data, particularly regarding access privileges. There is a prevalent assumption that within a CBDC system, the government or central bank would have unfettered access to financial data, potentially using this information for surveillance purposes or against its users. Specifically, there is concern that the central bank, as the issuing authority, would find it easier to monitor and track citizens’ CBDC activities. This possibility raises alarms about financial censorship and the potential for exerting political control through financial oversight.

However, these assumptions overlook a crucial factor: the design of CBDCs can significantly shift the privacy dynamic. Regarding the first assumption of fully transparent data, if specific identity information or transaction details are anonymized or encrypted, it could severely limit the ability to glean insights into an individual's spending habits, financial status, and personal preferences. Concerning the second assumption of data governance and the use of CBDC data, if the design restricts central banks or governments’ access to CBDC data, the prospects of surveillance could be significantly curtailed. Therefore, the intrinsic digital nature of CBDCs does not automatically result in diminished privacy or increased surveillance; the actual impact hinges on the specific design and deployment of the CBDC.

Of course, if a government or central bank intends to use the CBDC system for surveillance purposes, they certainly possess the capability to design it accordingly. Such a design could enable the monitoring of users and the collection of massive amounts of data, leading to significant privacy breaches. This could be achieved through various means, such as requiring the disclosure of personal information whenever a central bank issues a CBDC, tracking the ownership and expenditure of each CBDC, and continuously monitoring subsequent transactions. The point is, a CBDC can be a tool for surveillance only when it is designed to do so. It is wrong to blindly assume that CBDCs will automatically and directly diminish privacy and enable surveillance. It all depends on the design.

The question then arises: do the entities involved in issuing and designing CBDCs, as well as their prospective users, actually desire a system geared towards surveillance? The following section will argue that this is not the case, through examining various technical designs.

143 Id. at 96. For instance, should payer’s identity information remain private from an irrelevant third party? If the answer is yes, then the action of payer’s bank sharing payer’s identity information with an irrelevant advertisement company would violate privacy. See also Solove, supra note 138, at 1129.
144 Id. at 103.
145 Id. at 104.
B. Reality

Contrary to those wrong assumptions, leading central banks, think tanks, and scholars from interdisciplinary fields have proposed CBDC designs that are specifically aimed at protecting privacy. Below are several creative designs that are currently under exploration and experimentation.

The European System of Central Banks (ESCB) has established a proof of concept focused on anonymity in transactions. The goal is to provide users with degrees of privacy for lower-value transactions while monitoring higher-value transactions. The system is designed to protect a user’s identity and transaction history from the central bank and any intermediaries except those specifically chosen by the user. ESCB accomplishes this by building its proof of concept around intermediaries with a dedicated “AML” authority that is responsible for performing AML/CFT checks. ESCB built their proof of concept using distributed ledger technology with four entities (two intermediaries, once central bank, and one AML authority). The CBDC tokens in this proof of concept contain information on the past and current owners and cryptographic proof of validity. Intermediaries are responsible for ensuring that the tokens are valid when accepted by a payee and can be redeemed with the central bank on demand. Each user is on-boarded by an intermediary which provides the user with pseudonymous identities that are used as network addresses for CBDC payments.

The ESCB system uses “anonymity vouchers” that are spent at a ratio of each unit of CBDC that is transferred. These anonymity vouchers allow the CBDC to be spent anonymously until they are used up, and then any additional payments over that amount are no longer anonymous. These vouchers are issued free of charge, are not transferrable, and are simply the technical tool to limit the amount of CBDC that an individual can spend anonymously. Each wallet has a set cap on the amount of CBDC that can be held to prevent limiting the supply of CBDC in a way that could lead to excess demand from its users. CBDC transfers occur without the involvement of the central bank because users transfer the CBDC tokens among the intermediaries. Additionally, the AML authority does not need to be involved with the transaction as long as the user has sufficient anonymity vouchers in their wallet. With this proof-of-concept, ESCB has shown that it is possible to have a degree of privacy for lower-value transactions.

---

146 Herve Tourpe, Ashley Lannquist, and Gabriel Soderberg, A Guide to Central Bank Digital Currency Product Development: 5P Methodology and Research and Development 1, 15 (Sep. 2023) (providing a proof of concept is a realization of a certain method or idea in order to demonstrate its feasibility, or a demonstration in principle with the aim of verifying that some concept or theory has practical potential. In the context of CBDCs, a proof of concept is the second step in exploring CBDCs).
148 Id. at 2
149 Id.
150 Id.
151 Id.
152 Id.
153 Id.
154 Id.
155 Id.
156 Id.
157 Id.
158 Id.
159 Id.
transactions, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks.  

The Bank of Canada has recognized that the public overwhelmingly values privacy and anonymity and believe that the central bank should not collect or have access to Canadians’ personal and spending information. 161 Canadians desire a digital dollar that performs the function of a banknote without the need to share personal information. 162 To meet this demand from its citizens, Canada has proposed a credential issuance and verification scheme that complies with KYC requirements and allows authorized issuers to authenticate users and then issue those users pseudonymous credentials that can then be used to pseudonymously register with financial service providers. 163 Once the pseudonymous credentials are used to engage in transactions, a constant-time, interactive, zero-knowledge proof relying on a one-way function and asymmetric encryption are used to verify that payments are accurate and comply with any relevant regulations. 164 Using this, Canada may be able to comply with their legal obligations while simultaneously providing anonymous payments to its citizens.

The Bank of Canada has also discussed the trade-off between privacy and anonymity. 165 It defines privacy as the extent to which holdings and transaction data are concealed from participating entities in the CBDC system. 166 Participating entities include banks, money services businesses, government institutions, payment providers, and the general public. 167 A system may be more private with respect to one entity and less so for another. Adopting a “privacy by design” approach enables system designers to ensure they cover all entities and safeguard privacy to the extent necessary. 168 The Bank of Canada addresses the trade-offs between privacy and anonymity by recognizing that lower privacy levels are easier to achieve because less information needs to be secured. 169 Still, higher privacy requires the system to encapsulate data in reliable controls, which adds complexity and raises operational costs and computational overhead. 170 The Bank of Canada has discussed using group signatures, secret sharing, zero-knowledge proofs, homomorphic encryption, multi-party computation, and differential privacy in the CBDC design. 171 So far, its approach is largely theoretical, and a one-size-fits-all solution is unfeasible for privacy in CBDCs due to the diverse perceptions and legal systems across different countries.172

---

160 Id.
162 Id.
164 Id.
165 Darbha, supra note 19.
166 Id.
167 Id.
168 Id.
169 Id.
170 Id.
171 Id.
172 Kshetri, supra note 78, at 97–98.
The People’s Bank of China (PBOC) shares a similar principle of anonymity for lower-value transactions and traceability for higher-value transactions.173 The digital yuan has four wallet types, each allowing for progressively higher transaction limits.174 Users only need a mobile phone number to obtain the anonymous wallet.175 The anonymous wallet has limits of 500 yuan (about $77) per payment, 1,000 yuan (approximately $154) daily, and 10,000 yuan ($1,536) monthly.176 To obtain the other three wallet types, users are subject to varying degrees of regulations, with the requirements increasing for higher transaction limits.177

To further balance privacy and transparency requirements, the People’s Bank of China distributes the digital yuan to authorized operators like commercial banks, which then provide exchange and circulation services to the public.178 These authorized operators collect and store the personal information generated by the digital yuan wallet.179 ID anonymization technology ensures that personal data exchanged between wallets remains anonymous to counterparties and other commercial entities.180 For legitimate transactions, none of the entities above can obtain complete transaction information to protect consumers’ privacy.181 Only when suspicious transactions arise can the authorized operators apply to obtain relevant data for further analysis.182 The People’s Bank of China does not hold personal information and simply processes “inter-institutional transaction information.”183 When relevant authorities require access to users’ personal data, they must obtain legal warrants.184

Many scholars from various fields have proposed creative designs to protect user privacy. Prior to even the idea of a CBDC being discussed, David Chaum proposed a type of system that could protect the anonymity of a user called a “group signature.”185 A group signature is a generalization of credential mechanisms where a member of a group can convince a verifier of

175 Id.
176 Id.
177 Id. Based on the data in 2020, wallet type 4, the anonymous wallet, allows for transactions up to 500 yuan (about $77) per payment. Moving up, wallet types 3 and 2 permit transactions of 2,000 yuan (about $307) and 5,000 yuan (approximately $768), respectively. At the higher end, wallet type 1 allows for transactions up to 50,000 yuan ($7,681). See data: China's digital yuan wallet trial goes public, then withdrawn, Ledger Insights (Aug. 31, 2020), https://www.ledgerinsights.com/china-digital-yuan-trial-goes-public-withdrawn/.
179 Id.
180 Id.
181 Id.
182 Id.
183 Id.
184 Id. at 2–3. See also People’s Bank of China, supra note 173, at 7 (stating “The e-CNY system collects less transaction information than traditional electronic payment and does not provide information to third parties or other government agencies unless stipulated otherwise in laws and regulations. Internally, the PBOC sets up a firewall for e-CNY-related information, and strictly implements information security and privacy protocols, such as designating special personnel to manage information, separating e-CNY from other businesses, applying a tiered authorization system, putting in place checks and balances, and conducting internal audits. Any arbitrary information requests or use are prohibited”).
information that he belongs to the group without revealing his identity. These group signatures are generally anonymous, but when a manager sees a potential issue with the signatures or what they are being used for, they can open the signature to view the individual that signed it. This is similar to current projects that are generally anonymous, but if they trigger an AML/CFT report they can be opened to check for any potential violations. These signatures and this research are the basis of many of the anonymity projects and experiments that many central banks are working on when developing their CBDCs.

Katrin Tinn and Christophe Dubach propose a hybrid form of the CBDC model, deliberately designed with asymmetric features for sending and receiving money. This system aims to separate the link between individuals and their purchases to ensure near-complete anonymity for payers. In this proposal, they argued that outgoing flows of money should bear no information on the payer’s identity, but that incoming money does not require full privacy because incoming money is subject to taxation and at least some institutions in the economy are entitled to information on incoming money flows. Incoming flows can be linked to individual identities to facilitate the prevention of fraud, money laundering, or tax evasion. Accomplishing this hybrid anonymity approach can be done through a “ZeroCash” approach that leverages zero-knowledge proofs to achieve this objective of offering privacy for the payer and simultaneously identifying the receiver.

Christian Grothoff and Thomas Moser focus on identifying payers while keeping the transaction data private through a token-based and software-only CBDC. The CBDC token is issued and distributed just like banknotes. These tokens are referred to as coins and customers can withdraw coins by withdrawing money from their bank account and exchanging them for these coins. The coins would be stored locally on the computer or smartphone and would not involve an account or ledger. The coins would also have no record linking the coins to the owner. They offer privacy through blind signatures, where a blinding operation is performed on the user’s device to hide the numeric value of the coin from the central bank before requesting the signature. Because users carry out these blind signatures, they do not have to trust the central bank or the commercial bank to safeguard their private spending history. This system would not use distributed ledger technology, would not use zero-knowledge proofs because of the computational demand, and would prevent double-spending by only allowing the coins to be

---

186 Id. at 257–258.
187 Id.
189 Id.
190 Id.
191 Id.
192 Id.
193 CHRISTIAN GROTHOFF & THOMAS MOSER, HOW TO ISSUE A PRIVACY-PRESERVING CENTRAL BANK DIGITAL CURRENCY, 2–3 (2021). This approach diverges from typical cryptocurrencies, which have been considered account-based systems where users’ accounts are credited and debited based on what payments they make with the currency, and then those transactions are verified by a distributed ledger technology.
194 Id. at 1.
195 Id. at 3.
196 Id.
197 Id.
198 Id.
spent once and providing a list to the central bank of coins that have been spent. If a payee receives a coin that has already been spent, the payee can reject the transaction as invalid. These proposals indicate that CBDCs can be crafted to significantly enhance user privacy. Such designs can provide various levels of anonymity, covering the identity of the payer, the specifics of transactions, or both. Consequently, no single entity would be able to access a fully transparent data trail, thereby obtaining comprehensive insights into an individual’s spending habits, financial status, or personal preferences. In most of these designs, access by central banks or government bodies to identity data or transaction details is restricted, alleviating concerns related to surveillance.

Another intriguing conclusion is that these CBDC designs could offer better privacy protections compared to current payment systems. In today's digital payment landscape, commercial banks routinely collect consumer financial data, with user information and transaction history fully accessible to them. Additionally, law enforcement agencies can obtain detailed identity and transaction data based on reports from these banks. More concerning is the practice of financial institutions selling user data to third parties or utilizing this data in loan origination. These practices starkly contrast with the above CBDC designs. The enhanced privacy features incorporated into CBDC systems may well be a direct response to public concerns about the erosion of privacy and government surveillance. Such concerns could have led to an overcorrection in the design of CBDC, leading to a strong emphasis on anonymity beyond what is observed in existing payment systems.

III. Real Challenge: Misalignment with AML/CFT Laws

The previous section argues that the prevailing privacy and surveillance concerns associated with CBDCs are rooted in incorrect assumptions and concludes that CBDCs can be designed to provide better privacy protection to mitigate such concerns. This section points out that the real issue is the potential conflict between privacy-preserving designs and AML/CFT laws. Focusing on the digital dollar within the U.S. context, it begins by outlining the AML/CFT framework. Next, it employs Project Tourbillion as a case study to illustrate how designs aimed at ensuring payer anonymity may fail to meet the record-keeping and reporting requirements under AML/CFT laws.

A. AML/CFT Framework

The AML/CFT laws include the Bank Secrecy Act (BSA) of 1970 and its subsequent amendments, notably the Uniting and Strengthening America by Providing Appropriate Tools

\[199\] Id. at 3–4.
\[200\] Id. at 4.
\[201\] See generally Id.
\[202\] Id.
\[203\] Why do Banks Share your Financial Information and Are They Allowed To?, U.S. Government Accountability Office (2020) https://www.gao.gov/blog/why-do-banks-share-your-financial-information-and-are-they-allowed (explaining that banks are permitted to share personal consumer information if they comply with the Gramm-Leach-Bliley Act of 1999. Banks regularly collect and share consumer financial information with third-parties such as (1) financial companies like mortgage bankers, securities broker-dealers, and insurance agents, (2) retailers that are looking for data to sell a product to specific customers, (3) companies that deliver services on behalf of the lender, and (4) government agencies and nonprofits).

The BSA stands as a cornerstone in U.S. anti-money laundering legislation. Passed in 1970 to prevent banks from engaging in tax evasion, it also provided tools in fighting organized crime by mandating financial institutions to assist U.S. government agencies in detecting and preventing money laundering, primarily through record keeping and report making.\(^{204}\)

Key requirements regarding making reports include: (1) Reporting transactions (including deposit, withdrawal, exchange or other payment or transfer) over $10,000 through a Currency Transaction Report (CTR),\(^{205}\) (2) keeping various records regarding numerous funds transfers, cash purchases of negotiable instruments such as money orders, cashier’s checks, traveler’s checks, etc., under different circumstances,\(^{206}\) and (3) filing reports of suspicious activity that might signify money laundering, tax evasion, or other criminal activities.\(^{207}\) Additionally, records kept in compliance with the BSA generally are required to be held for five years, either after the record was made or after the closure of the account\(^{208}\), and kept in an easily accessible form such as paper or microfilm.\(^{209}\)

The Patriot Act of 2001,\(^{210}\) enacted after the September 11 attacks as part of a government effort to tighten U.S. national security, strengthened U.S. anti-money laundering laws by first expanding the scope of financial institutions to include a variety of non-bank entities such as commodity brokers and dealers, loan or finance companies, operators of credit card systems, insurance companies, and travel agencies.\(^{211}\) Next, the law introduced additional requirements for financial institutions, including: (1) the formal statutory requirement for all


\(^{205}\) 31 CFR §§ 1010.311, 1010.330 (requiring the reporting of the receipt of $10,000 or more, be it in one payment or multiple “related” payments, received in the course of business, with various regulations and specifications for particular circumstances and transactions).

\(^{206}\) 31 CFR § 103.29 (requiring the name of the purchasers, the date of the purchase, the kinds of instruments purchased, and the amount spent on the purchase be recorded if the purchaser has a deposit account with the institution; if they do not have such an account, then the address of the purchaser, their social security or alien identification number, date of birth, and a verified identifying document such as a driver’s license should also be recorded); 31 CFR § 103.33 (requiring that a record, either the original or a reproduction, of most extensions of credit exceeding $10,000, as well as a record of any request or instruction received or given that results in the transfer of currency or any other monetary instruments or funds, greater than $10,000 to or from any person or account outside the USA; such records would contain the name and address of the borrower, the amount in question, the nature/purpose of the credit, and the date that the loan was made); See also Risk Management Manual of Examination Policies, FDIC, 339-40 (2024), https://www.fdic.gov/resources/supervision-and-examinations/examination-policies-manual/risk-management-manual-complete.pdf.

\(^{207}\) 31 CFR § 1010.540(c) (requiring that financial institutions shall file reports as laid out in the act to the appropriate federal agency if the financial institution knows or suspects “an individual, entity, or organization is involved in, or may be involved in terrorist activity or money laundering.”)

\(^{208}\) Id at 344-45.

\(^{209}\) Id at 340.

\(^{210}\) Title III is the part of the Patriot Act dealing specifically with AML/CFT laws.

\(^{211}\) 31 USC § 5318(g) (2018) (applying requirements and regulations to newly covered institutions and non-bank entities that had not had to comply with prior to the passage of the Patriot Act); 31 USC § 5312 (defining financial agencies and institutions covered by these new regulations and requirements, including allowing for the Secretary of the Treasury to designate any non-specified institution as falling under the scope of the act if their “cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters”).
covered institutions to establish AML programs,\textsuperscript{212} (2) enhanced due diligence procedures, particularly for accounts involving foreign individuals or entities,\textsuperscript{213} (3) enhanced KYC requirements to verify and keep records of the identity of their clients,\textsuperscript{214} (4) increased sharing of information between financial institutions about potential money laundering threats.\textsuperscript{215}

The Patriot Act also expanded record keeping requirements, including foreign transactions or transactions in foreign currency or coin.\textsuperscript{216} It also offers legal liability protection to financial institutions, incentivizing more extensive record keeping and reporting without concern for liability.\textsuperscript{217} Notably, the Patriot Act allowed for greater sharing of information regarding such reports from financial institutions between federal intelligence agencies.\textsuperscript{218} Additionally, the law created the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, to monitor financial institutions’ compliance with the new laws and regulations and offer recommendations, analysis, and to gather financial data relating to compliance and financial crimes.\textsuperscript{219}

The Anti-Money Laundering Act of 2020 was passed as part of the National Defense Authorization Act of 2021, with the intention of enhancing and modernizing the AML/CTF laws of the United States. It expanded the definition of “financial institutions” under the BSA and the Patriot Act to include antiquities dealers and certain virtual currency activities.\textsuperscript{220} AMLA advocates for enhanced information sharing among financial institutions and between financial institutions and the government, especially through expanding the purpose and use of FinCEN’s suspicious activity reports (SARs).\textsuperscript{221} Section 6212 of the law proposes to establish a limited-

\textsuperscript{212} 31 USC § 5318(h) (2018) (requiring financial institutions to establish anti-money laundering programs, including, at a minimum, (A) the development of internal policies, procedures, and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs.)

\textsuperscript{213} 31 USC § 5318(i)(1) (2018) (Requiring financial institutions to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering if the financial institution establishes, maintains, administers, or manages a private banking account or a correspondent account in the United States for a non-United States person.)

\textsuperscript{214} 31 USC § 5318(l) (2018) (requiring financial institutions to, at a minimum, implement, and customers to comply with, reasonable procedures for (A) verifying the identity of any person seeking to open an account to the extent reasonable and practicable, (B) maintain records of the information used to verify a person’s identity, including name, address, and other identifying information, and (C) consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.)

\textsuperscript{215} 31 USC § 5311(5) (2018) (establishing appropriate frameworks for information sharing among financial institutions, their agents and service providers, their regulatory authorities, associations of financial institutions, the Department of the Treasury, and law enforcement authorities to identify, stop, and apprehend money launderers and those who finance terrorists.)

\textsuperscript{216} 31 USC § 5331 (requiring the filing of a report from any who receives more than $10,000 in coins, domestic currency, or foreign currency in the course of their business, with such a report including the details of the transaction, as well as the identification information of both the individual transacted with/reported on and the filer of the report.)

\textsuperscript{217} 31 USC § 5318(g)(3) (granting, generally, immunity from liability to individuals or institutions who, when making a voluntary disclosure of potentially illegal activity, may otherwise incur a legal liability as a result of such disclosure, either at the federal or state level.)

\textsuperscript{218} 31 USC § 5318(g)(4)(B), § 5319.

\textsuperscript{219} 31 USC § 310 (2018).

\textsuperscript{220} COUNTER Act of 2019 § 211.

\textsuperscript{221} Id. at § 205.
duration pilot program for sharing SARs. The program allows financial institutions with a SAR reporting obligation to share SARs and information related to SARs with the institution’s foreign branches, subsidiaries, and affiliates to combat illicit finance risks. However, FinCEN has not yet promulgated rules to implement section 6212. This final rule has been delayed several months from FinCEN’s prior rulemaking agenda. Additionally, the law encourages technological innovation and the use of modern tools and methods, such as artificial intelligence and digital identity technologies, to improve AML compliance and the efficiency of government AML programs. It also mandated the creation of new subcommittees of the Bank Secrecy Act Advisory Group, subcommittees that would bring together regulatory and law enforcement agencies with financial institutions to coordinate and discuss technological innovation and information security and confidentiality. And as a part of this innovation, the AMLA also created a whistleblower program for reporting money-laundering violations, the first of its kind within the AML/CFT legal framework.

B. Payer Anonymity Design
This subsection uses Project Tourbillon as a case study to examine the compatibility of payer anonymity with existing U.S. AML/CFT laws. It details Project Tourbillon's payer anonymity design, particularly examining its prototype that specifically focuses on two key processes: (1) withdrawal and (2) payment and redemption of the digital currency. Following this, the Article analyzes how this design aligns or conflicts with the detailed regulatory requirements of the Bank Secrecy Act (BSA) of 1970, the Patriot Act of 2001, and the Anti-Money Laundering Act of 2020 (AMLA). The conclusion drawn is that while payer anonymity partially satisfies AML/CFT requirements, such as the need for financial institutions (i.e., banks in the prototype) to establish an AML program, it falls short in fulfilling other critical aspects, notably in some report-keeping and reporting requirements. These findings indicate a need for further legal refinement, alternative technical solutions, or a combination of both, to integrate payer anonymity into the design of a digital dollar without significantly compromising regulatory compliance.

Project Tourbillon represents a significant development in balancing between user privacy needs and public policy objectives. It introduces a creative privacy paradigm: payer anonymity, aiming to provide cash-like privacy in CBDC payments. Under this paradigm, privacy is defined as the right to keep personal information confidential and accessible only to a select, trusted group of people.

---

222 Id. at § 201.
223 Id.
225 Id.
226 COUNTER Act of 2019 §§ 301-05.
228 Id.
230 Id. at 4.
231 Id. at 7.
In Project Tourbillon’s framework, the first crucial step involves consumers and merchants being onboarded by a bank, thereby ensuring the adequate fulfillment of Know Your Customer (KYC) procedures.\(^{232}\) When a consumer makes a payment to a merchant using CBDCs, the consumer’s personal information is not disclosed to any party, including the merchant, the banks, or the central bank.\(^{233}\) The merchant’s identity, however, is disclosed to their bank as part of the payment process but remains confidential there.\(^{234}\) The central bank, on its part, “does not see any personal payment data but can monitor CBDC circulation at an aggregate level.”\(^{235}\)

Commercial banks are tasked with utilizing their existing procedures to combat illicit transactions within this system.\(^{236}\) They have two key measures: first, all CBDC users – consumers and merchants – must undergo a thorough KYC process to verify their identities.\(^{237}\) Only those who have completed this process can withdraw, hold, pay, and redeem CBDCs.\(^{238}\) Next, similar to today's two-tier financial system, the merchant’s bank is responsible for ensuring that transactions comply with regulatory requirements, including AML, CFT, and tax evasion prevention.\(^{239}\) Commercial banks must also take necessary actions in cases of non-compliance.\(^{240}\)

This design bears some similarities to traditional cash withdrawals.\(^{241}\) Just as a person must have a bank account to withdraw cash from an ATM and undergo KYC procedures (including the provision of personal details like name, address, and social security number) to open that account, the same principle applies here. Once the individual withdraws cash, the payment remains untraceable until another holder of the cash decides to deposit it back into a bank. This analogy illustrates the balance Project Tourbillon seeks to strike between user privacy and adherence to regulatory requirements.

Project Tourbillon developed two prototypes to demonstrate how a payer’s privacy can be preserved while simultaneously preventing the illicit use of money.\(^{242}\) While these prototypes share a similar design ethos, they differ in how the central bank records CBDCs.\(^{243}\) This difference does not directly affect the banks' compliance with AML/CFT regulations; therefore, this Article focuses solely on analyzing the first prototype’s compatibility with the existing AML/CFT framework. The two accompanying graphs illustrate the processes of (1) withdrawal and (2) payment and redemption of the CBDC (which is represented as coins or CBDC coins in these illustrations) that are involved in the first prototype.\(^{244}\)

It begins with the withdrawal by the consumer. Here is a step-by-step breakdown of the process, as shown in Graph 2:

\(^{232}\) *Id.* at 11.
\(^{233}\) *Id.* at 23.
\(^{234}\) *Id.*
\(^{235}\) *Id.* 15.
\(^{236}\) *Id.* at 23.
\(^{237}\) *Id.*
\(^{238}\) *Id.*
\(^{239}\) *Id.*
\(^{240}\) *Id.*
\(^{241}\) *Id.* 14-15.
\(^{242}\) *Id.* at 11.
\(^{243}\) *Id.* at 11-12.
\(^{244}\) *Id.* at 14-15 (Refer to the original description in the Bank for International Settlements (BIS) report for a detailed understanding of these processes).
1. Consumer Initiation: The consumer logs into the application and requests to withdraw a specific amount of digital dollars, for example, 15 digital dollars. The app then generates two distinct coins with unique identifiers of different denominations: one 10-dollar coin and one 5-dollar coin.

2. Hashing and Blinding: Utilizing cryptographic techniques, the app hashes and then blinds these coins. Blinding is crucial as it places a signature on each coin without disclosing the unique identifiers to the bank or the central bank.

3. Bank Processing: These blinded coins are sent to the consumer's bank. The bank then blocks 15 digital dollars in the consumer's deposit account and forwards the blinded coins to the central bank (such as the Federal Reserve).

4. Central Bank Action: The central bank debits 15 digital dollars from the bank’s reserve account and signs the blinded coins with its private key for the respective denominations. This action effectively issues digital dollars. The central bank then sends these signed but still blinded digital dollars back to the bank.

5. Finalizing Withdrawal: The consumer's bank debits the consumer's deposit account by the withdrawn amount and forwards the blinded digital dollars to the consumer.

6. Consumer Receives Digital Dollars: Upon receiving the digital dollars, the app unblinds and stores them in the digital wallet.

Graph 2 withdrawal

---

245 Id. at 13 (Explaining that an unsigned coin is a consumer generated digital file with a unique serial number that is not (yet) signed by the central bank, and once a coin is signed by the central bank, that coin becomes a CBDC coin).
246 Id. at 13-14 (Illustrating that whenever the consumer spends CBDC coins, the algorithm assesses the optimal denomination of the remaining coins and rebalances the denomination if it is incorrect).
247 Id. at 13.
248 Id. (Noting that the consumer blinds the coins, not the bank or the central bank, and only the consumer can unblind the coins and neither the bank nor the central bank can see the unblinded coin at the time of withdrawal).
249 Id. at 13.
250 Id. at 13-14
251 Id. at 13-14.
252 Id. at 14.
253 Id.
254 Id.
During this withdrawal process, the consumer’s bank knows the consumer's identity and the withdrawal amount. However, the central bank remains unaware of the consumer’s identity and the specific amounts withdrawn. The central bank only knows that the bank has withdrawn 15 digital dollars in total. Additionally, neither the bank nor the central bank knows which coins the consumer owns because the coins remain blinded throughout the entire process until they are unblinded upon entering the consumer's account. This process ensures consumer privacy at the central bank level while maintaining necessary transparency at the consumer's bank.

Once the consumer has digital dollars in her wallet, she can use them to pay merchants. The payment process at the point-of-sale is outlined in the following steps, as depicted in Graph 3:

1. Consumer's Purchase Decision: The consumer selects an item for purchase and agrees with the merchant on the price, say 10 digital dollars.
2. Merchant's Transaction Initiation: Using his app, the merchant creates a pending transaction at the merchant’s bank. The merchant then generates a Quick Response (QR) code containing all relevant payment details, such as the amount, the merchant's deposit account details, and a transaction number.

---

255 Id. at 13.
256 Id. at 14.
257 Id. at 15.
258 Id. at 14.
259 Id.
260 Id.
261 Id.
3. QR Code Scanning by Consumer: The consumer uses her app to scan the QR code, which transfers all the necessary payment information to the consumer’s app. 262

4. Consumer’s Payment to Merchant’s Bank: The consumer’s app selects the required digital dollars from the wallet and sends them to the merchant’s bank, and the merchant’s bank then links these digital dollars to the pending transaction and forwards them to the central bank. 263

5. Central Bank Verification: The central bank verifies the signature on the digital dollars. It then checks against a list to ensure these digital dollars have yet to be spent. If everything checks out, the central bank redeems the digital dollars, adding them immediately to the 'spent' list to prevent them from being spent again. 264

6. Credit to Merchant Bank’s Reserve Account: After redemption, the central bank credits the merchant bank’s reserve account and sends a confirmation to the merchant's bank. 265

7. Merchant’s Bank Credits Deposit Account: The merchant’s bank then credits the merchant’s deposit account with the transaction amount. 266

8. Notification to Merchant: The merchant’s bank notifies the merchant that the transaction has been successfully completed. 267

262 Id.
263 Id. at 14-15.
264 Id. at 15.
265 Id.
266 Id.
267 Id.
In this payment and redemption process, the central bank will not know the identities of the consumer or merchant. The payer’s identity is not visible to the merchant’s bank. The key technology in Project Tourbillon is the ‘blind signature,’ which is integral to ensuring privacy. A blind signature allows a user to obtain a signature on a message whose content is unknown to the signer but can attest to its validity. Because of this technology, neither the central bank nor any third party can trace the coin’s spending history back to the payer. This traceability is hindered because the random number crucial for the coin’s identification and tracking is known only to the payer and remains unblinded in the transaction process. Thus, when the coin is spent, the payer’s identity remains anonymous, as the central

---

268 Id.
269 Id.
270 Id. at 17 (Blind signatures follow a three-step process. First, the payer creates a coin by choosing a random number and blinds it (1) using a random blinding factor. Second, the central bank receives the blinded coin and applies its digital signature (2). Since the coin is blinded, the central bank has no knowledge of the actual random number of the coin. Third, the payer unblinds (3) the received signed blinded coin by removing the blinding factor but keeping the signature on the original coin. The payer can now use the unblinded coins to pay digitally.).
271 Id.
272 Id. (Explaining that because of blind signatures in a digital cash system, users can obtain valid coins signed by a central authority while simultaneously keeping their ownership of specific coins private and preventing commercial and central banks from tracing individual spending patterns).
273 Id.
bank and other entities only see the blinded version of the number. This technical feature is critical in reconciling the privacy concerns of digital dollar users with the transparency requirements of U.S. AML/CFT regulations.

C. Incompatibility
Given the current AML/CFT laws, should the digital dollar adopt Project Tourbillon's payer anonymity design, the digital dollar may encounter compliance challenges, especially concerning record-keeping and reporting requirements, as discussed below.

First, implementing payer anonymity, especially via blind signatures, creates a compliance challenge with the BSA’s requirements for CTRs. For transactions exceeding $10,000, the CTR form requires details like names and addresses of the individuals involved, along with the account number and social security or taxpayer identification number of any person or entity on whose behalf the transaction is conducted. The anonymity feature in Project Tourbillon will make compliance with this requirement impossible. The reason is that while the payer's bank knows the individual's identity and withdrawal amounts, it may lack complete visibility into subsequent transactions of these withdrawn funds, hindering accurate reporting. It would also be impossible for the merchant’s bank to file a CTR because the payer’s identity information is anonymous to the merchant’s bank. Similarly, it would also be difficult to fully report or detect suspicious activities involving specific individuals when the merchant's bank cannot access the payer's identity.

Second, under the Patriot Act, consumers’ and merchants’ banks can comply with the requirements for establishing an AML program and conducting enhanced KYC procedures during account setup to verify customers’ identities. Some of these processes are generally completed before any person withdraws digital dollars. As previously mentioned, the critical first step for Project Tourbillon requires that all consumers and merchants be onboarded by their respective banks. If they want to use a digital dollar, they must open an account at their respective banks. The banks will conduct KYC requirements by collecting and verifying names, addresses, and other identifying information. The required steps for an AML program, such as developing internal policies, designating a compliance office, conducting employee training, and having an audit function to test the programs, remain unchanged with the introduction of a digital dollar.

However, compliance challenges arise with Section 314 of the Patriot Act, which requires increased information sharing between financial institutions about potential money laundering threats. Section 314(a) enables federal law enforcement agencies to request information from financial institutions about individuals, entities, and organizations involved in or suspected of being involved in terrorism or money laundering. Financial institutions must then search their records to see if they have conducted transactions with these parties and report back to the authorities. Since the merchant’s bank cannot access the payer's identity, it cannot report if it has conducted transactions with individuals suspected of involvement in money laundering or terrorism.

274 Id.
275 31 CFR § 1010.312.
277 Id.
Third, the merchant’s bank faces challenges in meeting the AMLA’s mandates for broader information sharing among financial institutions and between financial institutions and the government, especially through the obligation to share SARs and information related to SARs with the institution’s foreign branches, subsidiaries, and affiliates. Should FinCEN implement this provision, financial institutions handling the digital dollar could struggle to meet these information-sharing requirements given payers’ information is anonymous. Consequently, the merchant’s bank would have difficulty collecting, let alone sharing, such personally identifiable information.

<table>
<thead>
<tr>
<th>AML/CFT obligations</th>
<th>Detailed requirements / information to be collected</th>
<th>Can payer anonymity align with the requirements?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency Transaction Report</td>
<td>This report must be filled out whenever a customer attempts a currency transaction of more than $10,000. A financial institution shall verify and record the name and address of the individual presenting the transaction, as well as record the identity, account number, and the social security or TIN, if any, of any person or entity on whose behalf the transaction is to be effected.</td>
<td>N</td>
</tr>
<tr>
<td>Suspicious Activity Report</td>
<td>If a financial institution knows, suspects, or has reason to suspect that an individual, entity, or organization is involved in, or may be involved in terrorist activity or money laundering, and such institution is subject to a suspicious activity reporting requirement... the institution shall file a Suspicious Activity Report (“SAR”). Bank is required to file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute filing of an SAR. A transaction requires reporting if it is conducted or attempted by, at, or through the bank, it involves or aggregates at least $5,000 in funds or assets, and the bank knows, suspects, or has reason to suspect that (i) the transaction involves funds derived from illegal activities or is conducted in order to hide or disguise funds or assets derived for illegal activities as part of a plan to violate or evade any federal law or regulation, (ii) the transaction is designed to evade any requirements of this chapter or any regulations under the Bank Secrecy Act, (iii) the transaction has no</td>
<td>N</td>
</tr>
</tbody>
</table>

278 COUNTER Act of 2019 § 205.
279 31 CFR § 1010.311, 1010.330(a)(1)(i).
280 31 CFR § 1010.312
281 31 CFR 1010.540(c)
282 12 CFR 208.62(d)
business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage. Under 1020.320(a)(2)(ii), when a bank suspects that a person is structuring transactions to evade CTR filing, it must file a SAR. A SAR must include the suspect’s information including name, address, occupation, forms of identification and relationship to the financial institution. A description of the suspicious activity must also be included in the report.

### AML Programs

An AML program must (1) comply with 1010.610 and 1010.620 of this chapter, (2) include a system of internal controls to assure ongoing compliance, independent testing for compliance conducted by bank personnel or an outside party, designation of an individual responsible for coordinating and monitoring day-to-day compliance, training for appropriate personnel, and appropriate risk-based procedures for conducting ongoing customer due diligence, and (3) complies with the regulation of its Federal functional regulator governing such programs. There is a reduced requirement for banks lacking a federal functional regulator.

### IV. Modernization of AML/CFT Practices and Laws

In the previous section, the case study of Project Tourbillon illustrates that payer anonymity conflicts with the record-keeping and reporting requirements under existing AML/CFT laws. To maximize the privacy protection benefits this design could provide for the digital dollar, the section advocates for two key modifications to reconcile the need for privacy with public interests in combating money laundering and terrorist financing. The first modification suggests that financial institutions should change the way they collect and manage data. However, financial institutions will not make any changes unless they are mandated by law. Therefore, the second modification involves changing the record-keeping and reporting requirements of the AML/CFT Laws. All these changes will come with tremendous benefits and, unavoidably, some challenges.

Before detailing the changes below, it is important to note that the proposed modernization of AML/CFT practices and laws is based on the overarching design wherein the digital dollar operates within a two-tier system. In this system, as illustrated in Project Tourbillon, the central bank issues digital dollars to financial institutions, which then distribute them to the general public. Notably, neither the central bank nor any government agency will have access to identity information or transaction data. Financial institutions will be responsible for AML/CFT checks, including the initial step of onboarding consumers through rigorous

---

283 31 CFR 1010.320(2).
284 31 CFR § 1020.210(a).
customer identification and verification processes, known as Know Your Customer (KYC), mirroring the existing practices of financial institutions.

A. Change practices
After the financial institutions onboard customers, a significant change starts with how they collect and manage transaction data. With the initiation of transactions using the digital dollar by consumers, the principle of payer anonymity is introduced. This principle guides the life cycle of digital dollar data through the following three steps.

Step one: data collection and anonymization. Upon the collection of transaction data by financial institutions, this data should undergo a rigorous anonymization process.\(^{285}\) The purpose of this process is to remove or mask personally identifiable information, therefore ensuring the integrity and conditionality of consumer identity.\(^{286}\)

Data anonymization is a crucial process employed to prevent private information from being traced back to an individual.\(^{287}\) This is achieved by deleting or encoding identifiers that link the individual to the stored data. There are six principal methods of anonymizing data, including data masking, pseudonymization, generalization, data swapping, data perturbation, and the creation of synthetic data.

- **Data Masking** alters data with modified values through techniques such as shuffling characters, substituting characters, or encrypting them.\(^{288}\) This prevents direct identification while preserving the data's utility for analysis.
- **Pseudonymization** replaces identifying details, like names, with pseudonyms, effectively concealing the individual's identity to facilitate data usage in analyses without revealing personal information.\(^{289}\)
- **Generalization** reduces data precision by modifying it to broader categories or ranges, thus preventing the identification of individuals.\(^{290}\)
- **Data Swapping** disrupts direct linkages by rearranging variables within the dataset, such as exchanging names with another individual's date of birth.\(^{291}\)

---

285 Darbha, supra note 19.
286 Id.
288 Id. (“Data masking refers to the disclosure of data with modified values. Data anonymization is done by creating a mirror image of a database and implementing alteration strategies, such as character shuffling, encryption, term, or character substitution. For example, a value character may be replaced by a symbol such as “*” or “x.” It makes identification or reverse engineering difficult”).
289 Id. (“Pseudonymization is a data de-identification tool that substitutes private identifiers with false identifiers or pseudonyms, such as swapping the “John Smith” identifier with the “Mark Spencer” identifier. It maintains statistical precision and data confidentiality, allowing changed data to be used for creation, training, testing, and analysis, while at the same time maintaining data privacy”).
290 Id. (“Generalization involves excluding some data purposely to make it less identifiable. Data may be modified into a series of ranges or a large region with reasonable boundaries. For example, the house number at an address may be deleted, but make sure the name of the lane does not get deleted. The aim is to remove some of the identifiers while maintaining the accuracy of the data”).
291 Id. (“Data swapping – often known as permutation and shuffling – rearranges dataset attribute values so that they do not fit the original information. Switching attributes (columns) that include recognizable values, such as date of birth, can make a huge impact on anonymization”).
• Data Perturbation adjusts the original data by methods like rounding numbers or adding statistical noise, maintaining the overall dataset structure while obscuring individual values. 292

• Synthetic Data consists of entirely generated data that simulates the statistical properties of the original dataset but does not correspond to any actual individuals, thus offering an enhanced privacy level without sacrificing analytical value. 293

These methods are frequently utilized together rather than separately, as different data types may necessitate distinct anonymization techniques for optimal privacy protection. 294 For instance, while pseudonymization can effectively anonymize names, other data forms might require the application of data swapping or perturbation for adequate anonymization. Each technique presents unique benefits: data swapping and generalization help maintain the utility of data, whereas synthetic data and data perturbation prioritize privacy preservation.

Step Two: Data Aggregation and Analysis. Financial institutions can pool anonymized payer data along with their transaction information from various sources for analysis. Advanced data analytics can be used to identify trends, patterns, and correlations within the anonymized data that may indicate money laundering or terrorist activities. Machine learning models, such as clustering or classification, can also be employed to uncover relationships in the dataset and predict outcomes based on historical patterns to detect suspicious activities. This approach leverages advanced technologies to extract valuable insights from data without compromising the anonymity of customers involved in transactions.

Step Three: Real-Time Reporting and Unmasking Upon Reevaluation. When financial institutions detect suspicious activities, such as a series of rapid, high-value transactions that deviate from typical transaction behavior, they report the anonymized account (or the identifier of the account) to law enforcement agencies in a timely manner, ideally close to real time. Currently, financial institutions are required to report to law enforcement no later than 30 calendar days after the initial detection of facts. 295 However, this timeframe can be too late for addressing illegal transactions, as the act may have already been completed by the time the information reaches law enforcement agencies. Upon receiving the masked identity data with suspicious transaction histories, law enforcement conducts a reexamination; if this reexamination reveals no illegal activities, the investigation is concluded, and the data should be discarded. 296 Conversely, if illegal activities are suspected, law enforcement may request the financial institution to unmask the data or decrypt the identifiers to access the customer’s identity and transaction details. 297

292 Id. (“Data perturbation modifies the initial dataset marginally by applying round-numbering methods and adding random noise. The set of values must be proportional to the disturbance. A small base can contribute to poor anonymization, while a broad base can reduce a dataset’s utility. For example, a base of 5 should be used for rounding values like age or house number”).

293 Id. (“Synthetic data is algorithmically generated information with no relation to any actual case. The data is used to construct artificial datasets instead of modifying or utilizing the original dataset and compromising privacy and protection. The synthetic data method includes the construction of mathematical models based on patterns contained in the original dataset. Standard deviations, linear regression, medians, or other statistical methods can be used to produce synthetic results”).

294 Id.


297 Id.
B. Change laws

Although the proposed changes reflect methods to incorporate payer anonymity, financial institutions will not make such changes unless legally mandated. Therefore, AML/CFT laws must be amended to formally recognize and legalize payer anonymity features. Amendments should focus primarily on record-keeping and reporting requirements.

First, record-keeping requirements should be updated. Currently, financial institutions must maintain detailed transaction records, including the nature, amount, date, and parties involved, without any form of anonymization. 298 Additionally, in instances of abnormal transactions, financial institutions are expected to gather more information and closely monitor the account in question, often irrespective of the risk level of illegal conduct. 299 Some financial institutions even question the need to retain certain personal records, like a customer’s social security number. 300 In a digital dollar system that embraces payer anonymity, record-keeping should evolve to allow for the use of pseudonyms in place of actual identity details, such as names and social security numbers, in transaction records.

Second, changes are also imperative in the reporting requirements. Currently, whenever a financial institution identifies suspicious activity from unmasked data, it reports all personally identifiable information of the involved parties, along with the transaction activities, to law enforcement agencies. 301 Due to concerns about noncompliance, financial institutions often report any minor suspicious activities, even if they are ultimately found to be legal. 302 The banking sector has voiced concerns over the inefficiency and focus on 'technical compliance' rather than on effective and relevant reporting. 303 The sector has complained about the exhaustive, wasteful, and overly long investigations into any possibly suspicious conduct, which not only deplete financial institutions' resources but also divert law enforcement agencies' attention from more critical investigations. 304

In the context of the digital dollar, reporting requirements should be amended to permit the use of pseudonyms when reporting suspicious activities. The law should also reduce the monitoring or reporting of low-risk customers, which will decrease the amount of data gathered

298 31 C.F.R. § 1023.220.
300 Id. at 13.
302 Id.
303 Id.
304 Rowe, supra note 299. See also Norbert J. Michel & Nicholas Anthony, Re: Review of Bank Secrecy Act Regulations and Guidance Docket ID: FINCEN-2021-0008, Cato Inst. 2-3 https://www.cato.org/sites/cato.org/files/2022-02/michel-anthony-public-comment-2-7-2022.pdf (describing “reporting floods” and “reporting fatigue,” both of which risk undermining FinCEN’s ability to combat financial crimes; “reporting floods” can be thought of as overly broad sweeps for information that overwhelm scarce resources e.g., the employees that file and review reports, and ultimately undermine the credibility of FinCEN, the BSA, and law enforcement, and “reporting fatigue” refer to the scenario in which employees of financial institutions are fatigued from filing many reports that they know to be unnecessary but it is safer to mistakenly over report rather than underreport.)
and reported by financial institutions to law enforcement authorities. Most importantly, the law should empower financial institutions to exercise discretion in reporting transactions based on clear and sufficient evidence. This will mitigate the risk of ineffective compliance practices. A study by the World Bank underlined the efficacy of risk-based approaches in enhancing the detection of financial crimes, suggesting that allowing institutions to focus on genuinely suspicious transactions rather than adhering to a blanket reporting threshold increases the chances of identifying and preventing illicit activities.

The third, and probably the most important, change in the reporting requirements is that the law should facilitate real-time reporting in the digital dollar system. This change further addresses the issue of ‘technical compliance’ and allows for more effective investigation of illegal activities. The law should be revised to streamline the submission of anonymized data in real time through advanced technological platforms. There should be clear criteria for platform providers, ensuring that these platforms are capable of handling and transmitting data securely and efficiently. Unmasked personal information should only be accessible to law enforcement after transactions are confirmed as suspicious and indicative of money laundering or terrorist financing. To ensure the effectiveness and integrity of this system, clearly defined protocols for the transmission of masked data to law enforcement agencies are essential. These protocols should detail the specific steps that law enforcement agencies must follow to verify and confirm illegal activities before requesting unmasked data.

Last but not least, the Currency Transaction Reports (CTR) requirement should be revisited. Currently, the law mandates the reporting of transactions exceeding $10,000 with personally identifiable data. Despite existing exemptions for certain customers, the financial sector advocates for streamlined processes to obtain and apply these exemptions, particularly for low-risk entities. Many financial institutions also complain that the $10,000 threshold is too low without adjusting for inflation. The $10,000 reporting threshold, enacted in 1970, has not kept pace with the decreasing value of the dollar. After adjusting for inflation, $10,000 in 1970 now has the same purchasing power as roughly $74,000 today, making the reporting threshold increasingly onerous each year.

In the context of the digital dollar, this Article argues that the CTR requirement should be eliminated for two reasons. The first reason is the lack of clear evidence that the extensive personal data reported for transactions exceeding $10,000 leads to successful investigations. In 2018, the Bank Policy Institute conducted an empirical study where a sample of 19 financial

---

308 Rowe, supra note 299.
309 Michel, supra note 304.
310 Id.
311 Id.
312 Id at 2-3 (“As noted by the Bank Policy Institute, “there is no established metric for measuring whether financial institutions’ BSA reports are “useful” to law enforcement, and little to no feedback from law enforcement on the matter…”.”).
institutions reviewed approximately 16 million alerts and filed over 5.2 million CTRs. These reports resulted in an average of only 0.44% of CTRs warranting additional review from law enforcement, with even fewer leading to the apprehension of criminals. The second reason is that a real-time reporting system, utilizing advanced data analytics techniques, could more effectively identify suspicious activities than merely recording and reporting transactions exceeding $10,000 to law enforcement agencies.

C. Benefits and challenges

The most significant advantage of these changes is the enhanced protection of individual privacy. By anonymizing data, no entity—especially intermediaries—will have complete access to a payer's transaction details. This effectively shields individuals' financial status and spending preferences from any unwanted analysis or other potential harms, such as racial profiling. Furthermore, these changes address concerns related to government surveillance by ensuring that transactional data, particularly concerning the identities of the transacting parties, remains inaccessible to governmental bodies, including law enforcement. Law enforcement will only gain access to such data at the last stage of an investigation when they confirm that financial crimes have occurred or are highly likely to occur. Moreover, in the event of a data breach, the security of the anonymized data is preserved, provided it has been anonymized in a way that makes decryption challenging. This approach not only safeguards personal financial information but also significantly reduces the potential for unauthorized access and misuse of data.

The second benefit of these changes is the enhanced ability to identify and investigate suspicious activities more effectively and efficiently. By aggregating data from various sources and leveraging emerging technologies for data and transactional analysis, financial institutions can gain a more comprehensive view of transactions, even when dealing with anonymized data. This approach enables the detection of complex money laundering schemes or terrorist activities that might remain undetected with more limited datasets in the current systems. Real-time reporting will also aid law enforcement agencies in apprehending criminals more swiftly, as opposed to the current system, which gives financial systems 30 days to report suspicious activities.

Some may argue that real-time reporting may result in too much information being shared with law enforcement in real time, potentially compromising privacy. The system is designed to report data only when financial institutions reasonably believe, based on sufficient evidence, that illegal activity has occurred. This can reduce the large volume of data currently being reported, especially when employees of financial institutions recognize some data as unnecessary or irrelevant but still report due to the fear of incompliance, as identified by the Bank Policy Institute. What’s more, the privacy impact is mitigated by the fact that the data shared remains

314 Michel, supra note 304 (“Unfortunately, these numbers only represent follow-up actions by law enforcement, not legal action or conviction. However, the findings are illustrative nonetheless considering both the number of legal actions and the number of convictions would most likely be far less than the number of follow-up actions”).
315 12 C.F.R. § 21.11(d).
anonymized, preserving individuals' privacy while enhancing the efficiency of law enforcement responses. It is important to note that de-anonymized data will only become accessible to law enforcement if suspicious activity is detected and confirmed, ensuring a balanced approach between privacy protection and security measures.

The third benefit of these changes is the significant enhancement in the strategic allocation of resources and operational focus for both financial institutions and law enforcement agencies. By shifting the reporting criteria to be based on evidence and discretion, financial institutions are relieved from the pressures of "technical compliance," which often results in a considerable regulatory burden. Also, by streamlining the record-keeping and reporting processes and eliminating the CTR requirements, financial institutions can reallocate labor and capital towards more value-adding activities. These include investing in advanced technologies and developing expertise that are more effective in detecting suspicious activities. For law enforcement agencies, instead of being inundated with an overwhelming volume of reports, many of which are unhelpful, they now receive more targeted and useful information. This shift allows them to concentrate their efforts and resources on investigations that are more likely to lead to successful outcomes, thereby increasing the efficiency and effectiveness of law enforcement operations against illegal activities.

However, these proposed changes are not without challenges or trade-offs. One of the primary challenges concerns the quality of the anonymized data, especially when analyzing suspicious activities based on anonymized payer information. If data is poorly anonymized, it can lead to false positives or omit critical information. There exists a delicate balance between the degree of anonymization and the utility of the data. Over-anonymization may diminish the data's usefulness, potentially undermining benefits such as improved AML/CFT law enforcement effectiveness or cost reductions achieved through streamlined data recording and reporting. It also challenges the tech industry to develop advanced technologies capable of extracting useful information from highly anonymized data. Conversely, under-anonymization poses a risk to reidentification, potentially leading to privacy breaches. This trade-off underscores the need for a carefully calibrated approach to anonymization that preserves both privacy and the data's value for analysis.

Next, amending and updating AML/CFT regulations can also be complex and lengthy. This process involves a variety of stakeholders, including government agencies, financial institutions, international bodies, and sometimes the public. Each group has its own interests and concerns, making it difficult to reach a consensus. Regulators may require time and expertise to understand and implement updates to the laws, leading to a period of uncertainty for financial institutions. Financial institutions may also be concerned about the potential high adoption and compliance costs of the new system, possibly exceeding those of existing systems. They may be hesitant to invest in or adopt expensive technology to achieve regulatory compliance if they anticipate that these investments could become obsolete due to uncertainty in the regulatory landscape.

In addition, financial institutions are highly likely to push back against the idea of anonymity because they are reluctant to forfeit the ability to collect and analyze fully transparent data. Their business model is deeply rooted in understanding clients’ financial statuses and detailed transaction habits, as this knowledge allows them to monetize such data.317 Currently,
the expenses associated with regulatory compliance can be mitigated by access to comprehensive client data, which can then be analyzed to enhance the sale of existing services or be sold in bulk to data brokers. Consequently, financial institutions are likely to resist any system that drastically disrupts established revenue streams. This resistance underscores the broader tension between privacy concerns and the financial industry's profit motives, emphasizing the need for a balanced approach that respects both privacy and economic interests.

Regulators must carefully explain the system to avoid misunderstandings and highlight its benefits to financial institutions. It is important to convey that anonymized data can still yield valuable insights for their businesses. This involves exploring how advanced technologies can be used to glean insights into transactions, even when data is anonymized. However, not all data in a transaction is anonymized; for example, in the design of Project Tourbillon, while the payer's identity is anonymized, the payee's (the merchant's) information remains visible. Financial institutions are also encouraged to actively explore alternative revenue sources instead of solely relying on payment information. Moreover, given the financial sector’s grievances regarding regulatory burden and calls for simplification and modernization of AML/CFT requirements, this presents an opportunity to advocate for these changes and their advantages to financial institutions.

Conclusion

This article demystifies the unjustified concern that a digital dollar would be a tool for government surveillance, showing instead that it offers enhanced privacy protections through an examination of current technical designs. It calls for integrating privacy-preserving features into the digital dollar system and modernizing AML/CFT laws. The successful design and implementation of such a framework would not only make the digital dollar viable, should the Federal Reserve choose to issue it, but also positively impact digital payment systems broadly, leading to enhanced privacy protection in the digital age. By adopting privacy-preserving designs and modernizing AML/CFT laws, we can achieve a careful balance between protecting privacy and fulfilling public interest objectives, such as combating money laundering and terrorist financing.

319 Bank for Int’l Settlements, supra note 229 at 8.
320 Rowe, supra note 299. Michel, supra note 304. Bradfield, supra note 316.