Digital Dollar: Privacy and Transparency Dilemma

JIAYING JIANG[†]

Many have voiced concerns that the digital dollar, a digital form of central bank money, will facilitate government surveillance, thus depriving users of privacy. This Article investigates critical technical designs proposed by leading think tanks, central banks, and scholars from interdisciplinary fields, reaching a surprising conclusion that contradicts popular belief: 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 digital dollar data is fully transparent regarding personal information and transaction details and (2) that the government or Federal Reserve has unrestricted access to this fully transparent data, posing a significant risk for misuse. In reality, the designs directly oppose these assumptions by allowing for a certain degree of anonymity—whether through payer anonymity, transaction anonymity, or a combination of both—while 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, reporting, and information-sharing 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 research at the CBDC conference hosted by the Bank for International Settlements, which brought together general counsels from 63 central banks. Their invaluable feedback significantly shaped this piece. Special thanks are extended to industry experts Mike Alonso, Robert Oleschak, Jennifer Devlin, and Herve Troupe for their insightful discussions. The author also acknowledges the many academics who generously shared their perspectives or commented on this piece, including Jane Bambauer, Amy Stein, Peter Molk, Kathy Hwang, Ben Johnson, Chris Hampson, Matthew Kim, Tsang Cheng-yun, Yesha Yadav, Yulia Guseva, Heng Wang, Steven Schwarcz, Kevin Werbach, Lev Menand, Brett Hemenway Falk, Mark Lemley, Christopher Yoo, David Schwartz, as well as participants at the UF Law Junior Faculty Workshop, UF Business, Economic, and Law Workshop, the Junior Faculty Forum for Law and STEM at the University of Pennsylvania Carey Law School, and the American Association of Law Schools 2025 Annual Meeting. Finally, the authors thanks research assistants Christopher Radcliffe, Seth Frye, and Daniel Pinkus, as well as editors of the UC Law Journal for their valuable research support and careful edits.

TABLE OF CONTENTS

INTRODUCTION

In an era in which 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? 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] About one hundred and thirty four countries, representing 98% of global GDP, are actively exploring CBDCs, and three countries have successfully issued CBDCs.[3] The movement toward digital currency is gaining unprecedented momentum. In the United States, the exploration of 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 citizens' financial activities.

---

1. *Central Bank Digital Currency Tracker*, ATL. COUNCIL, https://www.atlanticcouncil.org/cbdctracker (last visited Apr. 25, 2025); *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. *Central Bank Digital Currency Tracker*, *supra* note 1; Jiang, *supra* note 1.

3. *Central Bank Digital Currency Tracker*, *supra* note 1.

4. FED. RSRV., MONEY AND PAYMENTS: THE U.S. DOLLAR IN THE AGE OF DIGITAL TRANSFORMATION 13–16 (2022) (writing that a digital dollar would be a digital liability issued by the Federal Reserve, available to the general public for making digital payments and highlighting how this type of liability would differ from the Federal Reserve's current offerings because at present, the Federal Reserve only issues paper money and minted coins).

Introducing a digital dollar would create complex legal issues that affect many legal disciplines, including central banking, monetary policy, financial regulation, tax, contract, privacy and data protection, insolvency, property, and private international laws.[5] At the core of these multifaceted legal issues lies what can be termed the "privacy and transparency dilemma."

The digital dollar's privacy and transparency dilemma weighs individual privacy expectations against the government's interest in countering financial crimes. Individuals generally expect privacy, meaning they expect their financial transactions to remain inaccessible to unrelated parties, particularly the government.[6] However, the government must retain the ability to access transaction details and monitor financial activities through financial institutions 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.[7] This situation creates significant tension between the desire for privacy and the need for regulatory transparency in financial data.

Literature on the legal aspects of CBDCs is notably scarce, with even fewer sources addressing the specific legal issues of the digital dollar.[8] Even rarer are discussions on privacy and transparency within the United States context. Arguably, the first substantial exploration of the legal aspects of CBDCs is presented in an International Monetary Fund (IMF) working paper, which offers a detailed framework for analyzing the legal foundations and treatments of CBDCs under central bank law and monetary law.[9] However, the IMF working paper does not address critical issues related to

5. Nadia Pocher & Andreas Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*, 19 IEEE TRANSACTIONS ON NETWORK & SERV. MGMT. 1776, 1777–78 (2022); *see also* Wouter Bossu, Masaru Itatani, Catalina Margulis, Arthur D. P. Rossi, Hans Weenink & Akihiro Yoshinaga, *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations* 5 (Int'l Monetary Fund, Working Paper No. 254, 2020), https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827; BANK FOR INT'L SETTLEMENTS, GENERAL GUIDANCE FOR NATIONAL PAYMENT SYSTEM DEVELOPMENT 38–41, 63–68 (2006) (discussing Guidance 10, which promotes legal certainty, and Annex, which provides a legal framework and model laws on payments).

6. WORLD ECON. F., 6 DIGITAL CURRENCY GOVERNANCE CONSORTIUM WHITE PAPER SERIES: PRIVACY AND CONFIDENTIALITY OPTIONS FOR CENTRAL BANK DIGITAL CURRENCY 13 (2021) [hereinafter WORLD ECON. F. WHITE PAPER], https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.

7. *Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)*, INT'L MONETARY FUND, https://www.imf.org/en/Topics/Financial-Integrity/amlcft (last visited Apr. 25, 2025).

8. As of December 2023, approximately 400 articles on CBDCs were available on SSRN. Among these, about 50 to 60 articles broadly tackled legal issues, predominantly from international viewpoints, with fewer than 10 articles specifically focusing on the US context.

9. Bossu et al., *supra* note 5.

privacy and transparency nor does it mention the specifics of the digital dollar.

Among the limited articles that do address the legal issues of the digital dollar, discussions on the balance between privacy and transparency are insufficient. Crawford, Menand, and Ricks discuss the potential benefits of a digital dollar and advocate for a "FedAccount" which would allow the public to hold accounts directly with the Federal Reserve to use government-issued digital money.[10] They raise the question of whether anonymous payments that protect the privacy of citizens should be a policy goal for the Federal Reserve at all.[11] Schwarcz argues that Article 4A of the Uniform Commercial Code (UCC) could serve as the foundation for a regulatory framework governing the digital dollar.[12] 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.[13] Yadav, Fernandez da Ponte, and Kim examine the regulatory complexities within the United States payment system, particularly the interplay between state and federal jurisdictions in overseeing payment service providers.[14] Skinner argues that a CBDC is a bundle of rights, including sovereignty, property, and privacy.[15] Yet, they do not explore how privacy and transparency requirements intersect under the 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 they are mutually exclusive; and (3) almost no belief in the feasibility of achieving anonymity in a CBDC.

More specifically, Tsang, Yang, and Chen explore privacy concerns surrounding CBDCs from both Taiwanese and international perspectives, advocating for a robust disciplinary mechanism to address these issues,

---

10. John Crawford, Lev Menand & Morgan Ricks, *FedAccounts: Digital Dollars*, 89 GEO. WASH. L. REV. 113, 116–17 (2021) (defining FedAccounts as accounts that complement the physical currency that is maintained and monitored by the central bank).

11. *Id.* at 152.

12. Steven L. Schwarcz, *Regulating Digital Currencies: Towards an Analytical Framework*, 102 B.U. L. REV. 1037, 1053–54 (2022).

13. *Id.* at 1059–60.

14. Yesha Yadav, Jose Fernandez da Ponte & Amy Davine Kim, *Payments and the Evolution of Stablecoins and CBDCs in the Global Economy* 76–78 (Vand. Univ. L. Sch. Legal Stud. Rsch. Paper Series, Working Paper No. 23-19, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4425922.

15. Christina Parajon Skinner, *Central Bank Digital Currency as New Public Money*, 172 U. PA. L. REV. 151, 160 (2023) ("[T]his Article argues that money in America can be disaggregated into three distinct individual economic rights: *(1)* popular monetary sovereignty, which concerns the right of issuance; *(2)* property in monetary value, which confers derivative rights to the unfettered use and enjoyment of money's value; and *(3)* monetary privacy, which protects an individual's right to enjoy privacy from the State in one's lawful financial transactions.").

while deeming anonymization impractical.[16] Carrillo emphasizes that "[g]overnment agencies can use new payment technology to surveil the public and augment social control" and argues that "U.S. privacy laws does not meaningfully restrict the government acquisition of data that we share with firms."[17] Pocher offers a broader legal analysis of anonymity in CBDCs based on their structural design but does not propose specific design strategies for ensuring anonymity in a digital dollar system.[18]

Among central banks, the Deutsche Bundesbank has examined AML/CFT legal frameworks concerning CBDC designs, yet maintains that full anonymity is not feasible.[19] The Bank of Canada provides one of the most comprehensive analyses, suggesting ways a CBDC could balance privacy with AML/CFT compliance within Canada's regulatory framework, though it notes that anonymity is not a desired feature.[20] Similarly, the European Central Bank (ECB) and the Digital Pound Foundation have discussed potential design choices and the interplay between anonymity and compliance with AML/CFT laws, though their focus remains within the context of European legal framework.[21]

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

---

16. Cheng-Yun Tsang, Yueh-Ping Yang & Ping-Kuei Chen, *Disciplining CBDCs: Achieving the Balance Between Privacy Protection and Central Bank Independence*, 43 NW. J. INT'L L. & BUS. 235, 245 (2023) (noting that 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. Raúl Carrillo, *Seeing Through Money: Democracy, Data Governance, and the Digital Dollar*, 57 GA. L. REV. 1207, 1213–14 (2023).

18. Pocher & Veneris, *supra* note 5, at 3–5.

19. David Ballaschk & Jan Paulick, *The Public, the Private and the Secret: Thoughts on Privacy in Central Bank Digital Currencies*, 15 J. PAYMENTS STRATEGY & SYS. 277, 279 (2021); *see also* Francesco Mazzetti, *The Legal Obstacles on the Road to Central Bank Digital Currency (CBDC): The Digital Euro Project* 32 (Cardozo Sch. of L., Working Paper, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176167 (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).

20. *See* Sriram Darbha & Rakesh Arora, *Privacy in CBDC Technology*, BANK OF CAN. (June 2020), https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9.

21. *Exploring Anonymity in Central Bank Digital Currencies*, IN FOCUS, no. 4, Dec. 2019, at 1–2, https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.en.pdf (addressing many of the gaps which this paper wishes to fill, but is done so within the European context and not the United States context); Claire Conby, *CBDCs and Other New Forms of Digital Money: Goodbye Privacy and Anonymity?*, DIGIT. POUND FOUND. (Sept. 20, 2022), https://digitalpoundfoundation.com/cbdcs-and-other-new-forms-of-digital-money-goodbye-privacy-and-anonymity.

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, reaching a surprising conclusion: these technical designs can protect privacy more effectively than existing digital payment systems. A recurring theme in 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 entities cannot access identity data and transaction details. Those who express concerns about surveillance or loss of privacy often assume that CBDC data is fully transparent and that the government has unlimited access to such data. However, these assumptions are not always accurate.

The Article then addresses a real challenge: introducing privacy-preserving designs for the digital dollar may lead to conflicts with existing AML/CFT regulations. There are potential clashes between the stringent record-keeping, reporting, and information sharing requirements mandated by the AML/CFT regulations and payer anonymity. This Article delves into this tension by examining Project Tourbillon—a project advocating for payer anonymity in digital transactions—as a case study. This exploration exposes intricate dynamics between the desire for privacy in transactions and the increasing demand by law enforcement for greater transparency.

In mitigating this crucial conflict, the Article calls for a thoughtful modernization of AML/CFT laws. The objective is twofold: to safeguard privacy by allowing users to retain some anonymity, and to preserve AML/CFT law effectiveness in 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 contributions at both theoretical and practical levels. Theoretically, it addresses a gap in the existing literature, which is

predominantly focused on macroeconomic issues,[22] monetary policy,[23] financial inclusion,[24] international relations[25], technical designs,[26] and institutional designs.[27] Diverging from this trend, this Article concentrates

22. Jorge Abad, Galo Nuño & Carlos Thomas, *CBDC and the Operational Framework of Monetary Policy* 2 (Bank for Int'l Settlements, Working Paper, Paper No. 1126, 2024), https://www.bis.org/publ/work1126.pdf; *see also* Schwarcz, *supra* note 12, at 1051–52; Saule T. 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 T. Omarova, *Financial Innovation: Three Fallacies in the Debate*, *in* HIDDEN FALLACIES IN CORPORATE LAW AND FINANCIAL REGULATION: REFRAMING THE MAINSTREAM NARRATIVES 225, 238 (Saule T. Omarova, Alexandra Andhov & Claire A. Hill eds., 2024) [hereinafter, Omarova, *Financial Innovation*] (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); Wei Shen & Heng Wang, *Global Stablecoins and China's CBDC: New Moneys with New Impacts on the Financial System?*, 41 REV. BANKING & FIN. L. 258, 283–84 (2021).

23. Abad et al., *supra* note 22; *see also* Omarova, *The People's Ledger*, *supra* note 22, at 1258–59 (discussing the possibility of credits and debits to FedAccounts as a method to control the money supply); Omarova, *Financial Innovation*, *supra* note 22, at 249 (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, Jason Allen, Will Bateman, Rose Lastra, Simon Gleeson & Saule T. Omarova, *Central Bank Money: Liability, Asset, or Equity of the Nation?* 38 (Cornell L. Sch. Rsch. Paper, Paper No. 20-46, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3730608# (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); Marco Dell'Erba, *Stablecoins in Cryptoeconomics: From Initial Coin Offerings to Central Bank Digital Currencies*, 22 N.Y.U. J. LEGIS. & PUB. POL'Y 1, 3, 42 (2019).

24. ASHLEY LANNQUIST & BRANDON TAN, INT'L MONETARY FUND, CENTRAL BANK DIGITAL CURRENCY'S ROLE IN PROMOTING FINANCIAL INCLUSION 4–8 (2023); *see also* Dell'Erba, *supra* note 23, at 39–40.

25. Heng Wang & Simin Gao, *The Future of the International Financial System: The Emerging CBDC Network and its Impact on Regulation*, 18 REGUL. & GOVERNANCE 288, 289 (2024); *see also* Shen & Wang, *supra* note 22, at 303–04; Heng Wang, *China's Approach to Central Bank Digital Currency*, 18 U. PA. ASIAN L. REV. 77, 78, 102–06 (2022).

26. Raphael Auer & Rainer Böhme, *The Technology of Retail Central Bank Digital Currency*, BIS Q. REV., Mar. 2020, at 85, 85–86; *see also* James Lovejoy, Cory Fields, Madars Virza, Tyler Frederick, David Urness, Kevin Karwaski, Anders Brownworth & Neha Narula, *A High Performance Payment Processing System Designed for Central Bank Digital Currencies* 2–3 (USENIX Ass'n, Paper No. 2022/163, 2022), https://eprint.iacr.org/2022/163.pdf; NIKHIL GEORGE, TADGE DRYJA & NEHA NARULA, MIT DIGIT. CURRENCY INITIATIVE, A FRAMEWORK FOR PROGRAMMABILITY IN DIGITAL CURRENCY 3–4 (2023); Tsang et al., *supra* note 16, at 258–60; Dell'Erba, *supra* note 23, at 9, 21, 38; Wang & Gao, *supra* note 25, at 290–91.

27. Auer & Böhme, *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, *Financial Innovation*, *supra* note 22, at 248–51 (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); Tsang et al., *supra* note 16, at 258–60; Dell'Erba, *supra* note 23, at 14–15; Yuliya Guseva, Sangita Gazi & Douglas S. Eakeley, *On Innovation and the Coexistence of Stablecoins and Central Bank Digital Currencies*, 87 LAW & CONTEMP. PROBS. 91, 127–28 (2025) (advocating that

on the legal challenges and solutions associated with the digital dollar. This perspective broadens the scope of the CBDC conversation and pioneers an exploration into the legal intricacies within the United States 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 a resource for policymakers, guiding them through the complex legal challenges. This Article is timely, given the ongoing debate in the United States about whether to issue a digital dollar.[28] The United States has faced criticism for lagging behind other countries in the research and development of a digital dollar,[29] especially as 19 of the G20 nations are now in the advanced stage of CBDC development and three countries have fully launched their CBDCs.[30] This Article helps policymakers make better-informed decisions through a legal lens. Although this Article remains neutral on whether the United States should issue a digital dollar, it offers insights into the design, deployment, and legal considerations, responding to urgent inquiries outlined in President Biden's executive order.[31]

Additionally, this Article clarifies common misunderstandings about the purpose of a digital dollar and helps dispel concerns about mass surveillance. 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. A CBDC certainly can and would be an effective surveillance tool if governments intend to use it as such and can achieve the goal 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, this Article concludes that current efforts largely reflect citizens' desires for privacy. These efforts demonstrate a

---

CBDCs and stablecoins and coexist). "The coexistence may offer individuals and businesses *options* for conducting transactions and managing affiars. . . . [It] could [also] accomodate different economic actors and adapt to the changing technological landascape[] . . . ." *Id.*

28. Omarova, *Financial Innovation*, *supra* note 22, at 251.

29. *Id.* at 250–51.

30. *Central Bank Digital Currency Tracker*, *supra* note 1.

31. Ensuring Responsible Development of Digital Assets, Exec. Order No. 14,067, 87 Fed. Reg. 14143 (Mar. 14, 2022).

commitment to ensuring that CBDCs are not used as a surveillance tool. This insight highlights the Article's contribution toward demystifying the functionalities of a digital dollar and fostering an environment in which public and academic discourse is informed by facts and thorough objective analysis rather than fear or speculation.

This Article proceeds as follows: Part I describes the fundamentals of CBDCs, the popular debates surrounding them, and the current state of international and domestic CBDC decelopment. Part II addresses a prevalent but misplaced concern: the fear that the digital dollar will serve as an instrument for governmental surveillance, thereby eroding user privacy. Part III delves into the real problem in the United States context: privacy-preserving designs of a digital dollar could clash with existing AML/CFT regulations. Part IV advocates for changes to financial institutions' record-keeping, reporting, and information sharing 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 UK and Japan with their prototypes, the Bahamas with the sand dollar, and the ECB 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. For instance, the Federal Reserve has begun soliciting expert and public opinions on the potential risks and benefits of a digital dollar, releasing discussion papers regarding recent digital dollar research and development. However, stakeholders have expressed a broad spectrum of concerns and hold divergent opinions. These differences have notably slowed the pace of research and development, 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.[32] Wholesale CBDCs are specifically designed for financial institutions holding reserve deposits with a central bank.[33] 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.[34] On the other hand, retail CBDCs are designed for widespread use by the general public.[35] This Article is focused exclusively on retail CBDCs.

Designing a CBDC involves considerable nuances. For instance, many believe the first design choice is between a one- or two-tier issuance model.[36] In a one-tier model, the central bank issues a CBDC directly to the general public.[37] In a two-tier model, the central bank issues a CBDC to financial institutions, such as commercial banks, which then distribute the CBDC to the public.[38] However, CBDC design choices are more complicated than commonly assumed.[39] The existing categories are too limited to capture the complexity of the designs regarding access, intermediation, institutional roles, and data retention.[40] Each of these elements involve intricate trade-offs that can significantly impact a CBDC's functionality, security, and privacy, making the design process far more complex than it initially appears.

---

32. Mazzetti, *supra* note 19, at 14; *see also* Bossu et al., *supra* note 5, at 9; ANNEKA KOSSE & ILARIA MATTEI, BANK FOR INT'L SETTLEMENTS, MAKING HEADWAY—RESULTS OF THE 2022 BIS SURVEY ON CENTRAL BANK DIGITAL CURRENCIES AND CRYPTO 2 (2023), https://www.bis.org/publ/bppdf/bispap136.pdf.

33. Bossu et al., *supra* note 5, at 9; *see also* Mazzetti, *supra* note 19, at 14; KOSSE & MATTEI, *supra* note 32.

34. Schwarcz, *supra* note 12, at 1051.

35. KOSSE & MATTEI, *supra* note 32.

36. Auer & Böhme, *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.

37. *Id.*

38. *Id.*

39. *See* Lovejoy et al., *supra* note 26, at 1, 5 (discussing consideration required for designs).

40. *Id.* at 2; *see also* Auer & Böhme, *supra* note 26, at 87–88; BANK FOR INT'L SETTLEMENTS, ANN. ECON. REP. 70–71 (2021), https://www.bis.org/publ/arpdf/ar2021e.pdf; BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, CENTRAL BANK DIGITAL CURRENCIES 4 (2018), https://www.bis.org/cpmi/publ/d174.pdf; Rod Garratt, Michael Lee, Brendan Malone & Antoine Martin, *Token- or Account-Based? A Digital Currency Can Be Both*, FED. RSRV. BANK OF N.Y. (Aug. 12, 2020), https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both; Charles M. Kahn, Francisco Rivadeneyra & Tsz-Nga Wong, *Should the Central Bank Issue E-Money?* 8–9 (Fed. Rsrv. Bank of St. Louis, Working Paper, Paper No. 2019-003A, 2019), https://doi.org/10.20955/wp.2019.003; Tommaso Mancini-Griffoli, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu & Celine Rochon, *Casting Light on Central Bank Digital Currency*, IMF STAFF DISCUSSION NOTE 8–9 (Nov. 12, 2018), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233.

Common motivations to explore and potentially issue CBDCs across the globe include promoting financial inclusion by providing easier, safer access to money for unbanked and underbanked populations;[41] introducing competition and resilience in the domestic payments market, which might require incentives to provide cheaper and easier access to money; [42] increasing efficiency in payments and lowering transaction costs;[43] creating programmable money and improving transparency in money flows;[44] and providing for the seamless flow of monetary and fiscal policy.[45] Each of these motivations has been debated extensively. It is crucial to recognize that while central banks aim to achieve these goals with CBDCs, the actual outcomes remain to be seen.[46]

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.[47] This perspective, however, represents a misunderstanding of the nature of a CBDC. A CBDC is "not simply another payment technology." [48] "As a direct liability of the sovereign government, [a] CBDC's place is at the very top of the money hierarchy."[49] It can be a "uniquely potent lever of structural change, the core element of a qualitatively new—more efficient, stable, and democratic—financial ecosystem." [50] Realizing this potential requires policymakers to think beyond the basic payment framework.[51] Policymakers must acknowledge the implications of "changing the nature and composition of central banks'

41. Ensuring Responsible Development of Digital Assets, Exec. Order No. 14,067, 87 Fed. Reg. 14143, 14144 (Mar. 14, 2022); *see also* Yadav et al., *supra* note 14, at 64–68; KOSSE & MATTEI, *supra* note 32, at 6–7. Many unbanked populations lack access to traditional bank accounts due to geographic, regulatory, or financial barriers. CBDCs can provide individuals with a direct account or wallet with the central bank, bypassing the need for commercial banks. Additionally, traditional banking and remittance systems often charge high fees, discouraging people with low income from using them. CBDCs can reduce the need for costly infrastructure by facilitating peer-to-peer transactions with low or no fees. Distributing government benefits and subsidies to the unbanked can be inefficient, with funds lost to corruption or intermediaries. Governments can digitally distribute welfare payments, subsidies, or emergency aid directly into citizens' CBDC wallets, ensuring fast and accurate delivery.

42. KOSSE & MATTEI, *supra* note 32, at 9.

43. *Id.* at 6–7; *see also* Yadav et al., *supra* note 14, at 25–27; Morgan Ricks, *Money as Infrastructure*, 2018 COLUM. BUS. L. REV. 757, 830–31.

44. Alexander Lee, *What Is Programmable Money?*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (June 23, 2021), https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html; Yadav et al., *supra* note 14, at 45–47.

45. *Central Bank Digital Currency Tracker*, *supra* note 1; *see also* KOSSE & MATTEI, *supra* note 32, at 6–7.

46. Jiang, *supra* note 1, at 85–91.

47. Christopher J. Waller, *CBDC—A Solution in Search of a Problem?*, BANK FOR INT'L SETTLEMENTS (Aug. 6, 2021), https://www.bis.org/review/r210806a.htm.

48. Omarova, *Financial Innovation*, *supra* note 22, at 250.

49. *Id.*

50. *Id.*

51. *Id.*

primary liabilities."[52] Currently, central banks' primary liabilities to the general public are in physical form. For example, in the United States, the Federal Reserve's primary liabilities include notes and coins. Moving from a physical form of currency to a digital one "can change the entire relational dynamics between the central bank, private finance, and the broader economy."[53]

The belief that money is already digital also misrepresents 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 systems when they provide loans or credit to businesses or individuals.[54] This money is the bank's promise to pay the deposit holder a certain amount.[55] 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 bank 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.[56] Unlike central bank money representing a liability of the central bank, commercial bank money is a liability of the individual bank that issues it.[57]

A significant difference between central bank and commercial bank money lies in their risk: central bank money is free from credit risk, while commercial bank money carries 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.[58] Therefore, central bank-issued money is often considered safer than that from commercial banks.[59] Nevertheless, the benefit of CBDCs in this regard may be limited in countries like the United States, where strong regulations and government guarantees protect individuals from losing their funds in the event of bank

52. *Id.*

53. *Id.*; *see also* Omarova, *The People's Ledger*, *supra* note 22, at 1253.

54. Tsang, *supra* note 16, at 247–48.

55. *Id.*

56. Heng Wang & Ross Buckley, *The Coming Central Bank Digital Currency Revolution and the E-CNY*, 2023 SINGAPORE J. LEGAL STUD. 145, 145.

57. Tsang, *supra* note 16, at 247–48.

58. Martin Chorzempa, *How Are Central Bank Digital Currencies Different from Other Payment Methods?*, PETERSON INST. FOR INT'L ECON. (Apr. 26, 2021), https://www.piie.com/research/piie-charts/how-are-central-bank-digital-currencies-different-other-payment-methods.

59. *Id.*; *see, e.g.*, *E-krona*, SVERIGES RIKSBANK (Mar. 25, 2024), https://www.riksbank.se/en-gb/payments--cash/e-krona.

failure.[60] In contrast, in countries that lack reliable protections for account holders, CBDCs may provide meaningful security benefits.[61]

Recent developments in CBDCs have been notable. According to data from the Atlantic Council, out of 134 tracked countries, three have launched CBDCs, 44 have implemented pilot programs, 19 are developing CBDCs, 39 are researching them, 21 are inactive, and two have canceled CBDC projects.[62] Nearly 60% of central banks have cited the continued rise of crypto assets and stablecoins as catalysts to accelerate their work on CBDCs.[63] The ECB has entered the preparation phase of its digital euro initiative, aiming to make public money available for digital payments and strengthen monetary sovereignty.[64] 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.[65] China started research in 2014 and has been piloting a digital yuan program since 2020.[66] The pilot program has reached 260 million people in 28 cities, and the digital yuan is being tested in over 200 scenarios, some of which include public transit, stimulus payments, and e-commerce.[67] Some government employees have even begun receiving the digital yuan for their salaries.[68]

B. DOMESTIC DEVELOPMENT

These international developments have urged the United States to evaluate the feasibility of a digital dollar more intensely. In this context, President Biden issued an executive order calling for the responsible

60. Chorzempa, *supra* note 58. In the United States, the Federal Deposit Insurance Corporation (FDIC) provides insurance up to $250,000 per account, offering some degree of protection to depositors. However, such safeguards may not be available in other jurisdictions.

61. *Id.*

62. *Central Bank Digital Currency Tracker*, *supra* note 1 (citing figures as of Apr. 2025); *see also* KOSSE & MATTEI, *supra* note 32, 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).

63. KOSSE & MATTEI, *supra* note 32, at 2, 13–15; *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).

64. *Digital Euro*, EUR. CENT. BANK, https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (last visited Apr. 25, 2025).

65. *Central Bank Digital Currency Tracker*, *supra* note 1.

66. Jiaying Jiang & Karman Lucero, *Background and Implications of China's E-CNY*, 33 U. FLA. J.L. & PUB. POL'Y 237, 242 (2023); *see also* Elijah Journey Fullerton & Peter J. Morgan, *The People's Republic of China's Digital Yuan: Its Environment, Design, and Implications* 10 (Asian Dev. Bank Inst., Discussion Paper No. 1306, 2022).

67. *Central Bank Digital Currency Tracker*, *supra* note 1.

68. Laura He, *China Makes Major Push in Its Ambitious Digital Yuan Project*, CNN (Apr. 24, 2023, 1:40 AM EDT), https://www.cnn.com/2023/04/24/economy/china-digital-yuan-government-salary-intl-hnk/index.html; Ananya Kumar, *Practice Makes Perfect: What China Wants from Its Digital Currency in 2023*, ATL. COUNCIL (Apr. 24, 2023), https://www.atlanticcouncil.org/blogs/econographics/practice-makes-perfect-what-china-wants-from-its-digital-currency-in-2023; *Central Bank Digital Currency Tracker*, *supra* note 1.

development of digital assets and placing "the highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC."[69]

The administration acknowledges the potential benefits of a digital dollar: it could support efficient, low-cost transactions and promote broader access to the financial system with fewer risks than those posed by private cryptocurrencies.[70] It may also facilitate faster and more affordable cross-boarder payments, helping to sustain the United States' central role in the international financial system.[71]

The Biden administration also acknowledges the need for a careful assessment of potential risks and downsides. Specifically, the executive order highlights several areas of concern, including financial stability, systemic risk, national security, illicit finance, and privacy.[72] Therefore, the executive order requires the Secretary of the Treasury, the Federal Reserve, the Attorney General, and other relevant agencies to make legislative proposals and assess the implications a digital dollar might have on the financial system, democracy, and national security interests.[73]

In furtherance of this research agenda, the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology are currently collaborating on exploratory research known as Project Hamilton, which is a research project that explores design choices, technical challenges, and opportunities of the digital dollar.[74] The goal is to design a core transaction system that meets the robust speed, throughput, and fault tolerance requirements of a retail payment system.[75] Project Hamilton suggests decoupling transaction validation from execution, ensuring that the transaction format and protocol are secure, and also suggests providing flexibility for potential functionalities, such as self-custody, programmability, and efficiency.[76] It emphasizes that policy and design are interconnected and that a successful implementation of a digital dollar will require novel solutions to balance key policy goals, such as financial stability or inclusion.[77]

The Office of Science and Technology Policy's report on the technical feasibility of the digital dollar follows Project Hamilton's recommendation

69. Ensuring Responsible Development of Digital Assets, Exec. Order No. 14,067, 87 Fed. Reg. 14143, 14145 (Mar. 14, 2022).

70. *Id.*

71. *Id.* at 14145–46.

72. *Id.* at 14143.

73. *Id.* at 14146.

74. Lovejoy et al., *supra* note 26, at 1.

75. *Id.* at 3.

76. *Id.*

77. *Id.* at 31–33.

to establish goals to guide the technical design.[78] The Office outlines the digital dollar's policy objectives, including expanding equitable access to the financial system, preserving the role of physical cash, collecting only strictly necessary data, ensuring sustainability, and maintaining functionality.[79] The report analyzes eighteen major design choices and lists pros and cons.[80] However, it points out that although the digital dollar could technically be permissionless, being permissionless does not make sense for a system with a trusted entity, such as the Federal Reserve.[81]

Opinions vary regarding the necessity of issuing a digital dollar. Governor Christopher J. Waller, a member of the Federal Reserve Board of Governors, describes it as "a solution in search of a problem."[82] Governor Waller rejects the notion that foreign CBDCs, most notably China's E-CNY, will undermine the primacy of the United States dollar, arguing that non-Chinese firms will not find enough benefits from the switch to outweigh the surveillance concerns of the Chinese government through E-CNY.[83] Even if this were a concern, he further argues that issuing a digital dollar would not resolve it simply by allowing Americans to pay their bills with a digital dollar instead of commercial bank money.[84] Additionally, he argues that the threat to privacy far outweighs any potential benefit derived from the digital dollar. These privacy concerns include federal surveillance on citizens' financial activities, foreign terrorist financing, or money laundering.[85] Finally, he asserts that any threat to the stability of the United States dollar

78. Dr. Alondra Nelson, Alexander Macgillivray & Nik Marda, *Technical Possibilities for a U.S. Central Bank Digital Currency*, THE WHITE HOUSE: OFF. OF SCI. AND TECH. POL'Y BLOG (Sept. 16, 2022), https://bidenwhitehouse.archives.gov/ostp/news-updates/2022/09/16/technical-possibilities-for-a-u-s-central-bank-digital-currency; Lovejoy et al., *supra* note 26, at 32–33.

79. Nelson et al., *supra* note 78.

80. THE WHITE HOUSE: OFF. OF SCI. AND TECH. POL'Y, TECHNICAL DESIGN CHOICES FOR A U.S. CENTRAL BANK DIGITAL CURRENCY SYSTEM 11 (2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/09/09-2022-Technical-Design-Choices-US-CBDC-System.pdf.

81. *Id.* at 11. "Permissionless" refers to a type of blockchain or decentralized network where anyone can participate without requiring approval or permission from a central authority.

82. Waller, *supra* note 47; *see also Fed's Waller Remains Unconvinced of Need for CBDC*, AM. BANKERS ASS'N BANKING J. (Oct. 6, 2023), https://bankingjournal.aba.com/2023/10/feds-waller-unconvinced-of-need-for-cbdc (saying Waller remained unconvinced by CBDC in 2023 Brookings Institute conference as a unique solution to any particular problem); Minneapolis Fed, *Neel Kashkari Fireside Chat at the 2022 Journal of Financial Regulation Annual Conference*, YOUTUBE (Aug. 3, 2022), https://www.minneapolisfed.org/speeches/2022/neel-kashkari-fireside-chat-at-the-2022-journal-of-financial-regulation-conference; *Central Bank Digital Currencies: A Solution in Search of a Problem? Report Published*, UK PARLIAMENT: COMMS. (Jan. 13, 2022), https://committees.parliament.uk/committee/175/economic-affairs-committee/news/160221/central-bank-digital-currencies-a-solution-in-search-of-a-problem-report-published.

83. Waller, *supra* note 47.

84. *Id.*

85. *Id.*

can be adequately addressed by private-sector financial innovations, such as cryptocurrencies tied to the value of the United States dollar.[86]

Meanwhile, Chairman Jerome Powell of the Federal Reserve has stated that there is no urgency to issue a digital dollar and that the Federal Reserve will not proceed without congressional approval.[87] Because of President Biden's executive order, Chairman Powell feels that there is a mixed message surrounding the development of a digital dollar, and he is hesitant to move forward without explicit permission from all relevant authorities to avoid potential backlash.[88] This approach, which emphasizes that American leadership needs to be a united front before developing the digital dollar, is very unique. Chairman Powell is open to the possibility of incorporating the digital dollar, whereas Governor Waller believes the digital dollar should never be researched, developed, or issued.

Conversely, the Treasury Department's report on CBDCs has been interpreted as positive.[89] Secretary Janet Yellen agrees that CBDCs may offer benefits, such as increased financial stability or financial inclusion, but she also cautions that these benefits should be fully assessed through necessary research and testing.[90] She specifically points out that some aspects of the existing financial system are too slow and expensive and that researching CBDCs is essential to determine whether the Treasury could address these issues.[91] Further, Secretary Yellen believes that understanding the underlying design policies, strengths, and weaknesses of CBDCs will better equip the United States to handle contemporary monetary challenges abroad, even if the United States ultimately decides not to issue a digital dollar.[92] For all of these reasons, Secretary Yellen believes that researching and potentially developing a digital dollar is in the United States' best interests.

Additionally, some scholars have started advocating for the digital dollar. Yadav, Fernandez da Ponte, and Kim critique the current United States payment system as being outdated and inefficient.[93] A digital dollar could modernize this system.[94] Omarova sees advantages in issuing a digital dollar, including the potential to diminish the roles of traditional financial

86. *Id.*

87. Jeanna Smialek, *Jerome Powell Says the Fed Won't Issue a Digital Currency Without Congressional Approval*, N.Y. TIMES (Mar. 22, 2021), https://www.nytimes.com/2021/03/22/business/jerome-powell-says-the-fed-wont-issue-a-digital-currency-without-congressional-approval.html.

88. *Id.*

89. Fatima Hussein, *Treasury Recommends Exploring Creation of a Digital Dollar*, A.P. NEWS (Sept. 16, 2022, 9:29 AM PST), https://apnews.com/article/cryptocurrency-biden-technology-united-states-ae9cf8df1d16deeb2fab48edb2e49f0e.

90. *Id.*

91. *Id.*

92. *See id.*

93. Yadav et al., *supra* note 14, at 3 (explaining the inefficiencies of the United States' financial system, including its routine financial exclusion and outdated architecture).

94. *Id.*

institutions, such as too-big-to-fail banks or "shadow banking" institutions such as money market funds.[95] Crawford, Menand, and Ricks 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).[96] They recommend making these accounts, termed "FedAccounts," accessible to the general public, including individuals, businesses, and other institutions.[97]

II. EXAGGERATED CONCERN: SURVEILLANCE

CBDCs and a potential 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 Part addresses a common but exaggerated concern that CBDCs serve as a tool for government surveillance, thereby 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 CBDCs 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.

A. ASSUMPTIONS

Many politicians have voiced concerns that the digital dollar could become a tool for surveillance. In the United States, Republican Congressman French Hill has highlighted the potential for more significant data collection and privacy issues associated with a government-backed digital dollar.[98] Florida Governor Ron DeSantis[99] and officials from a few

95. Omarova, *The People's Ledger*, *supra* note 22.

96. Crawford et al., *supra* note 10.

97. *Id.*

98. Press Release, U.S. Congressman French Hill, Rep. Hill Protects the Personal Rights of Central Arkansans and Americans (May 23, 2024), https://hill.house.gov/news/documentsingle.aspx?DocumentID=9317; *see also* Press Release, U.S. Congressman Tom Emmer, Emmer's Flagship CBC Anti-Surveillance State Act Passes House of Representatives (May 23, 2024), https://emmer.house.gov/2024/5/emmer-s-flagship-cbdc-anti-surveillance-state-act-passes-house-of-representatives.

99. Press Release, Exec. Off. of the Governor Ron DeSantis, Governor Ron DeSantis Signs First-in-the-Nation Legislation to Protect Against Government Surveillance of Personal Finances (May 12, 2023),

other states, such as North Carolina,[100] Utah,[101] South Carolina,[102] South Dakota,[103] and Tennessee,[104] have indicated a desire to ban the digital dollar if the federal government decides to issue one.[105] These states argue that a digital dollar could infringe on citizens' financial privacy and autonomy, reflecting a growing skepticism toward digital currencies under government control.[106]

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.[107] Additionally, in a series of town hall meetings in the United States, citizens frequently raised concerns about financial privacy in the context of the digital dollar.[108] Similarly, a report from a think tank in

---

https://www.flgov.com/eog/news/press/2023/governor-ron-desantis-signs-first-nation-legislation-protect-against-government (highlighting 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.

100. Sandali Handagama, *North Carolina House Unanimously Votes to Ban Digital Dollar Payments to the State*, COINDESK (May 4, 2023, 10:58 AM PDT), 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 and banning states from participating in any pilot tests for CBDCs).

101. David Pokima, *United States Lawmakers Introduce Bills to Exclude CBDCs from the Definition of Money*, CRYPTONEWS (Jan. 17, 2024, 3:48 AM PST), https://cryptonews.com/news/united-states-lawmakers-introduce-bills-to-exclude-cbdcs-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).

102. *Id.*

103. *Id.*

104. *Id.*

105. Amaka Nwaokocha, *Multiple US Senate Bills Object to CBDC's Definition of 'Money'*, COINTELEGRAPH (Jan. 17, 2024), https://cointelegraph.com/news/us-senate-bills-exclude-cbdcs-money-definition (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).

106. *See* Peter Goettler, *CBDCs Threaten Privacy*, CATO INST. (June 26, 2023), https://www.cato.org/commentary/cbdcs-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).

107. EURO. CENT. BANK, EUROSYSTEM REPORT ON THE PUBLIC CONSULTATION ON A DIGITAL EURO 10 (2021), https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf (finding that 43% of respondents to this survey stated that privacy was the most important feature that they wanted to see in a CBDC).

108. *See Public Comments*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (June 24, 2022), https://www.federalreserve.gov/cbdc-public-comments.htm (including nine sets of public comments that were received by the Federal Reserve after publishing their paper about a potential U.S. CBDC and

Asia highlighted the general public's privacy concerns as a battleground for the power struggle between political leaders and central banks.[109] While many central banks do not require user data from a CBDC to fulfill their mandates, other government agencies may find this information very useful.[110] Canadian citizens are also immensely concerned with financial privacy, and they do not trust the institutions responsible for handling data privacy and protection.[111] Canadian approval for a Canadian CBDC is extremely low, with 86% of survey respondents expressing strong criticisms against a Canadian CBDC and 52% of respondents considering it a bad idea that they have no intention of using.[112]

Scholars have also scrutinized CBDCs, raising privacy concerns.[113] 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.[114] Many point out that, unlike physical cash, digital transactions leave a digital trail that can be easily monitored and analyzed.[115] This capability could lead to unprecedented levels of government oversight and control over individual

---

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).

109. Tsang et al., *supra* note 16, at 257–58 (discussing the current balancing act that many central banks are currently undertaking to balance privacy rights within a CBDC and the desire to utilize the data to comply with existing regulations).

110. *Id.*

111. Anwar Sheluchin, *Canadians Have Serious Trust Issues When It Comes to a Central Bank Digital Currency*, THE CONVERSATION (Dec. 11, 2023, 2:46 PM EST), https://theconversation.com/canadians-have-serious-trust-issues-when-it-comes-to-a-central-bank-digital-currency-219192 (explaining the concerns that the Canadian public has with the possibility of a Canadian CBDC infringing on people's privacy rights).

112. F. RSCH., DIGITAL CANADIAN DOLLAR PUBLIC CONSULTATION REPORT 40 (2023), https://www.bankofcanada.ca/wp-content/uploads/2023/11/Forum-Research-Digital-Canadian-Dollar-Consultation-Report.pdf. This report provides the statistics mentioned above as well as several comments that participants in the survey shared.

113. Auer & Böhme, *supra* note 26, at 86–87 (refer to Graph 1 for an uptake in privacy discussions in CBDC literature that has been produced over time); WORLD ECON. F. WHITE PAPER, *supra* note 6, at 17 (indicating the need to balance privacy with financial crime management); *see* Emanuele Borgonovo, Stefano Caselli, Alessandra Cillo, Donato Masciandaro & Giovanni Rabitti, *Cryptocurrencies, Central Bank Digital Cash, Traditional Money: Does Privacy Matter?* 28–30 (Universitá Bocconi, Working Paper, Paper No. 95, 2018) (indicating that anonymity in a CBDC is important to users, that an important tradeoff between privacy and anonymity will occur based on the design of the CBDC, and adoption of a CBDC may depend on how anonymous the system actually is).

114. Tsang et al., *supra* note 16, at 257–58 (explaining that while central banks usually do not require private data to achieve their mandates, other government agencies may find the private data useful, so privacy concerns are not only about how central banks manage user data, but also about central banks' partnerships with other agencies).

115. Ballaschk & Paulick, *supra* note 19, at 277–78 (stating that digital payments data offers valuable insights into people's personal lives and that privacy is vital to ensure a trusting relationship between customers and the parties handling their payments).

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 bank-monitored transactions that track identity data to completely unregulated anonymous cash transactions. Therefore, CBDCs must have privacy incorporated into their designs to satisfy the general public's concerns.[116]

But what does privacy mean in this context? Defining privacy has been challenging.[117] There are six conceptions of privacy,[118] but each of them is either overly broad or unduly narrow.[119] They all fail to effectively capture the dynamics of CBDCs.[120] In my prior work, I argued that privacy must be understood contextually.[121] Privacy should not be viewed as a separate, abstract concept but rather as "a dimension of certain practices and aspects of life."[122] 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. Therefore, when we state that we are "protecting privacy," we are essentially committing to safeguarding specific practices from unauthorized disruptions.[123] What should be considered private is a normative argument and may vary across jurisdictions, cultures, and times.[124] When conducting normative analysis, it is necessary to balance the value of privacy and other conflicting values.[125]

Unfortunately, numerous assumptions have been made regarding the privacy implications of CBDCs. This Article argues that the prevailing

116. Pocher & Veneris, *supra* note 5, at 5.

117. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 43 (7th ed. 2021).

118. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1092 (2002) ([The six conceptions of privacy are] "(1) the right to be let alone—Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self—the ability to shield oneself from unwanted access by others; (3) secrecy—the concealment of certain matters from others; (4) control over personal information—the ability to exercise control over information about oneself; (5) personhood — the protection of one's personality, individuality, and dignity; and (6) intimacy—control over, or limited access to, one's intimate relationships or aspects of life.").

119. *Id.* at 1094 (critiquing six categories of conceptions of privacy and explaining why each conception is either too broad or too narrow); *see also* WORLD ECON. F. WHITE PAPER, *supra* note 6, at 17 (discussing that central banks will need to balance privacy with law enforcement); 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).

120. Jiang, *supra* note 1, at 99–100.

121. *Id.*; *see also* Solove, *supra* note 118, at 1129.

122. Solove, *supra* note 118, at 1129.

123. Jiang, *supra* note 1, 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 118, at 1129.

124. Jiang, *supra* note 1, at 96.

125. *Id.* at 96, 104.

narrative, which suggests that CBDCs inherently compromise privacy and facilitate surveillance, is based on flawed assumptions.

The first assumption is that all data within a 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 data governance, 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 against its users or for surveillance purposes. Specifically, there is a 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: CBDC design can significantly shift the privacy dynamic. Regarding the first assumption of fully transparent data, the digital dollar can be designed to anonymize or encrypt specific identity information or transaction details, severely limiting 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, government surveillance could be significantly curtailed through incorporating a design which restricts central banks or governments' access to CBDC data. Therefore, CBDCs' intrinsic digital nature 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 a CBDC system for surveillance, they certainly have the capability to design it accordingly. They could employ various methods, 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 without any anonymous or pseudonymous features. Such a design could, of course, lead to significant privacy breaches. The point is that 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 inherently diminish privacy and enable surveillance; it all depends on the design.

The question then arises as to whether the entities involved in issuing and designing CBDCs, as well as their prospective users, desire a system

geared toward surveillance. The following Subpart will argue that this is not the case by examining various technical designs.

B. REALITY

Contrary to those speculative 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 being explored and tested.

The European System of Central Banks (ESCB) has established a proof of concept[126] focused on anonymity in transactions.[127] The goal is to provide users degrees of privacy for lower-value transactions while monitoring higher-value transactions.[128] 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.[129] The ESCB's proof of concept is built around intermediaries with a dedicated AML authority responsible for AML/CFT checks.[130] It uses distributed ledger technology involving four entities: two intermediaries, one central bank, and one AML authority.[131] The CBDC takes the form of digital tokens that contain information on past and current ownership and include cryptographic proofs verifying transaction authenticity without revealing additional details.[132] Intermediaries validate tokens upon receipt and ensure they are redeemable by the central bank.[133] Each intermediary onboards its users and assigns them pseudonymous identities that serve as network addresses for CBDC transactions.[134]

The ESCB system uses "anonymity vouchers" that are spent at a ratio of each unit of CBDC that is transferred. These vouchers allow the CBDC to be spent anonymously up to a certain amount, but excess payments are not afforded anonymity.[135] These vouchers "are issued free of charge and

126. HERVE TOURPE, ASHLEY LANNQUIST, & GABRIEL SODERBERG, IMF, A GUIDE TO CENTRAL BANK DIGITAL CURRENCY PRODUCT DEVELOPMENT: 5P METHODOLOGY AND RESEARCH AND DEVELOPMENT 15 (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, and in the context of CBDCs, a proof of concept is the second step in exploring CBDCs).

127. ECB, *supra* note 21, at 1.

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.* at 4; Morten Bech & Rodney Garratt, *What Is Distributed Ledger Technology?*, *in International Banking and Financial Market Developments*, BIS Q. REV., Sept. 17, 2017, at 1, 58 ("Distributed ledger technology (DLT) refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronised way across a network").

132. ECB, *supra* note 21, at 5.

133. *Id.*

134. *Id.* at 6.

135. *Id.*

are not transferrable," as "[t]hey are simply [the] technical tool" which limits how much CBDC an individual can spend anonymously.[136] Each wallet has a set cap on the amount of CBDC that can be held, ensuring that CBDC supplies are not limited in a way that could lead to excess user demand.[137] CBDC transfers occur without the involvement of the central bank because users transfer CBDC tokens among intermediaries.[138] 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.[139] With this proof of concept, the ESCB has shown that it is possible to have a degree of privacy for lower-value transactions while still ensuring that "higher-value transactions are subject to mandatory AML/CFT checks."[140]

The Bank of Canada has recognized that the public overwhelmingly values privacy and anonymity and believes that the central bank should not collect or have access to Canadians' personal and spending information.[141] Canadians desire a digital dollar that performs the function of a banknote without the need to share personal information.[142] To meet this demand, the Bank of Canada has proposed a credential issuance and verification scheme that complies with Know Your Customer (KYC) requirements. This scheme allows authorized issuers to authenticate users and then issue pseudonymous credentials that can be used to pseudonymously register with financial service providers.[143] 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.[144]

The Bank of Canada has also discussed the trade-off between privacy and anonymity.[145] It defines privacy as the extent to which holdings and transaction data are concealed from participating entities in the CBDC system.[146] These entities include banks, money service businesses, government institutions, payment providers, and the general public.[147] A

136. *Id.*
137. *Id.*
138. *Id.* at 7.
139. *Id.*
140. *Id.* at 9.
141. *A Digital Canadian Dollar: What We Heard 2020-23 and What Comes Next*, BANK OF CAN., https://www.bankofcanada.ca/digitaldollar/a-digital-canadian-dollar-what-we-heard-2020-23-and-what-comes-next (last visited Apr. 25, 2025).
142. *Id.*
143. Raza Ali Kazmi, Duc-Phong Le & Cyrus Minwalla, *Privacy-Preserving Post-Quantum Credentials for Digital Payments* 1–2 (Bank of Can., Staff Working Paper, Paper No. 2023-33, 2023).
144. *Id.* at 14.
145. Darbha & Arora, *supra* note 20.
146. *Id.*
147. *Id.*

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.[148] 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.[149] Still, a greater level of privacy requires the system to encapsulate data in reliable controls, which adds complexity and raises operational costs and computational overhead.[150] 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.[151] 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 frameworks across countries.

The People's Bank of China (PBOC) shares the similar principle of anonymity for lower-value transactions and traceability for higher-value transactions.[152] The digital yuan has four wallet types, each allowing for progressively higher transaction limits.[153] Users only need a mobile phone number to obtain the anonymous wallet,[154] which has a limit of 500 yuan (about $77) per payment, 1,000 yuan (approximately $154) per day, and 10,000 yuan ($1,536) per month.[155] To obtain the other three wallet types, users are subject to varying degrees of regulation, with the requirements increasing for higher transaction limits.[156]

---

148. *Id.*; *see also* Carrillo, *supra* note 17, 1279 (arguing the Digital Dollar system should include online bank accounts and potentially digital wallets, and that policymakers would need to provide devices that enable offline transactions to protect privacy); Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1341–42 (2013) (arguing privacy by design requires translating privacy principles into code, both in the back-end infrastructure of data collection and front-end user interfaces).

149. Darbha & Arora, *supra* note 20.

150. *Id.*

151. *Id.* Homomorphic encryption is an advanced form of encryption that allows computations to be performed directly on encrypted data (ciphertext) without the need to decrypt it first. The results of these operations remain encrypted, and when decrypted, they yield the same outcome as if the operations had been conducted on the original, unencrypted data.

152. PEOPLE'S BANK OF CHINA, PROGRESS OF RESEARCH & DEVELOPMENT OF E-CNY IN CHINA 7 (2021) (noting the People's Bank of China calls this principal "managed anonymity").

153. *China Promotes Digital Yuan Privacy as CBDC Trials Enter Second Phase*, LEDGER INSIGHTS (Mar. 22, 2021), https://www.ledgerinsights.com/china-promotes-digital-yuan-privacy-as-cbdc-trials-enter-second-phase.

154. *Id.*

155. *Id.*

156. *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 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.

To further balance privacy and transparency requirements, the PBOC distributes the digital yuan to authorized operators such as commercial banks, which then provide exchange and circulation services to the public.[157] These authorized operators collect and store the personal information generated by the digital yuan wallet.[158] Identification anonymization technology ensures that personal data exchanged between wallets remains anonymous to counterparties and other commercial entities.[159] For legitimate transactions, none of the entities above can obtain complete transaction information to protect consumers' privacy.[160] "Only when suspicious transactions arise can the authori[z]ed operators apply to obtain relevant data for further analysis."[161] The PBOC does not hold personal information; it simply processes "inter-institutional transaction information."[162] When relevant authorities require access to users' personal data, they must obtain legal warrants.[163]

Many scholars from various fields have proposed creative designs to protect user privacy. Prior to the idea of a CBDC being discussed, David Chaum proposed a mechanism that could protect users' anonymity called a "group signature."[164] A group signature is a generalization of credential mechanisms where a member of a group can convince a verifier of information that they belong to the group without revealing their identity.[165] 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 group signature to view the individual who signed it.[166] Group signatures and his research form the foundation of many anonymity projects.[167] Many central banks also rely on group signatures in developing their CBDCs.

---

157. Changchun Mu, Balancing Privacy and Security: Theory and Practice of the E-CNY's Managed Anonymity 1 (Nov. 1, 2022) (unpublished) (on file with the People's Bank of China), http://www.pbc.gov.cn/en/3688006/4706656/4696666/2022110110364344083.pdf.

158. *Id.* at 2.

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*

163. *Id.* at 2–3; *see also* PEOPLE'S BANK OF CHINA, *supra* note 152, at 7 ("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.").

164. *See* David Chaum & Eugène van Heyst, *Group Signatures*, *in* 547 LECTURE NOTES IN COMPUT. SCI. 257, 257 (1991) (proposing a mechanism to protect user anonymity called "group signature").

165. *Id.* at 257–58.

166. *Id.* at 257.

167. For instance, the BIS's Project Tourbillon and the Bank of Canada's CBDC design.

Katrin Tinn and Christophe Dubach propose a hybrid CBDC deliberately designed with asymmetric features for sending and receiving money.[168] This system is intended to separate the link between individuals and their purchases to ensure near-complete anonymity for payers.[169] In their proposal, Tinn and Dubach argue 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.[170] Incoming flows can be linked to individual identities to facilitate the prevention of fraud, money laundering, or tax evasion.[171] Accomplishing hybrid anonymity can be done through a "ZeroCash" approach that leverages zero-knowledge proofs to offer privacy for the payer while identifying the receiver.[172]

Christian Grothoff and Thomas Moser focus on identifying payers while keeping transaction data private through a proposed software-only CBDC.[173] These CBDCs are issued and distributed just like banknotes.[174] They are referred to as "coins," and customers can withdraw coins by withdrawing money from their bank accounts and exchanging them for coins.[175] The coins would be stored locally on a computer or smartphone without the use of an account or ledger, and they would carry no record linking them to the owner.[176] They offer privacy through blind signatures, in which a blinding operation is performed on the user's device to hide the numeric value of the coin from the central bank before requesting a signature.[177] Because users carry out these blind signatures, they do not have to trust a central bank or commercial bank to safeguard their private spending history.[178] This system would not use distributed ledger technology or zero-knowledge proofs due to the high computational demand.[179] It would prevent double-spending by providing the central bank

168. Katrin Tinn & Christophe Dubach, Central Bank Digital Currency with Asymmetric Privacy 2 (Feb. 11, 2021) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3787088.

169. *Id.*

170. *Id.*

171. *Id.*

172. *Id.*

173. Christian Grothoff & Thomas Moser, *How to Issue a Privacy-Preserving Central Bank Digital Currency*, 114 SUERF POL'Y BRIEFS, June 17, 2021, at 1, 2–3. 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.

174. *Id.* at 1.

175. *Id.* at 3.

176. *Id.*

177. *Id.*

178. *Id.*

179. *Id.*

a list of coins that have already been spent.[180] If a payee receives a coin that has already been spent, the payee can reject the transaction as invalid.[181]

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 to identity data or transaction details by central banks or government bodies is prohibited or greatly restricted, which alleviates surveillance concerns.

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.[182] Additionally, law enforcement agencies can obtain unmasked identity and transaction data based on reports from these banks.[183] Even more concerning is the practice of financial institutions selling user data to third parties or utilizing this data in loan origination.[184] These practices starkly contrast 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 in the existing payment systems.

III. REAL CHALLENGE: MISALIGNMENT WITH AML/CFT LAWS

The previous Part argues that the prevailing privacy and surveillance concerns associated with CBDCs are rooted in speculation and concludes that CBDCs can be designed to provide better privacy protection. This Part points out the real challenge: the potential conflict between privacy-preserving designs and AML/CFT laws. Focusing on the digital dollar within the United States context, it begins by outlining the AML/CFT

180. *Id.* at 4.

181. *Id.*

182. *See generally id.* at 2 (discussing how citizens "are not fully aware of the extent to which technological advances have improved the ability to track, aggregate, and disseminate personal information").

183. *Id.* at 4.

184. *Why Do Banks Share Your Financial Information and Are They Allowed To?*, GAO (Dec. 9, 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, and that 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).

framework. Next, it uses Project Tourbillion as a case study to illustrate how payer privacy can be secured through its payer anonymity design. Finally, it analyzes how such a design could fail to meet the record-keeping, reporting, and information sharing requirements under AML/CFT laws.

A. AML/CFT FRAMEWORK

The AML/CFT laws include the Bank Secrecy Act (BSA) of 1970[185] and its subsequent amendments, notably the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act) of 2001[186] and the Anti-Money Laundering Act (AMLA) of 2020.[187]

The BSA stands as a cornerstone in United States anti-money laundering legislation.[188] Passed in 1970 to prevent banks from engaging in tax evasion, it also provides tools for fighting organized crime by mandating that financial institutions assist United States government agencies in detecting and preventing money laundering, primarily through record-keeping, reporting, and information sharing.[189]

Key requirements include the following: (1) reporting transactions (including deposit, withdrawal, exchange, or other payment or transfer) over $10,000 through a currency transaction report (CTR);[190] (2) keeping various records regarding numerous fund transfers, cash purchases of negotiable instruments such as money orders, cashier's checks, traveler's checks, and so on, under different circumstances;[191] and (3) filing reports of suspicious

185. Currency and Foreign Transactions Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1118.

186. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272.

187. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 3388.

188. *The Bank Secrecy Act*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act (last visited Apr. 25, 2025).

189. SEC'Y OF THE TREAS., A REPORT TO CONGRESS IN ACCORDANCE WITH § 357 OF THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT OF 2011, at 4 (2002), https://www.fincen.gov/sites/default/files/shared/ReportToCongress357.PDF.

190. 31 C.F.R. §§ 1010.311, 1010.330 (2023) (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).

191. The CFR requires purchasers' names, the purchase date, the kinds of instruments purchased, and the amount spent on the purchase to be recorded if the purchaser has a deposit account with the institution. If they do not have such an account, then the CFR requires the purchaser's address, their social security or alien identification number, date of birth, and a verified identifying document such as a driver's license to also be recorded. The CFR also requires a record, either the original or a reproduction, of most credit extensions 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 should 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* FDIC, RISK MANAGEMENT MANUAL OF EXAMINATION POLICIES 8.1-6 to -7 (2024)

activity that might signify money laundering, tax evasion, or other criminal activities.[192] Additionally, records kept in compliance with the BSA are generally required to be held for five years, either after the record was made or after the closure of the account,[193] and kept in an easily accessible form such as paper and microfilm.[194]

The Patriot Act of 2001,[195] enacted after the September 11 attacks as part of a government effort to bolster United States national security, strengthened United States AML laws by first expanding the scope of financial institutions to include a variety of nonbank entities such as commodity brokers and dealers, loan or finance companies, operators of credit card systems, insurance companies, and travel agencies.[196] Next, the law introduced additional requirements for financial institutions, including (1) the formal statutory requirement for all covered institutions to establish AML programs,[197] (2) enhanced due diligence procedures, particularly for accounts involving foreign individuals or entities,[198] (3) enhanced KYC requirements to verify and keep records of the identity of their clients,[199]

[hereinafter FDIC MANUAL], https://www.fdic.gov/resources/supervision-and-examinations/examination-policies-manual/risk-management-manual-complete.pdf.

192. 31 C.F.R. § 1010.540(c) (2023) (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").

193. *Id.* § 1010.430(d).

194. *See FDIC Manual*, *supra* note 191, at 8.1-7.

195. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (addressing anti-money laundering and counter-terrorism financing laws).

196. 31 U.S.C. § 5318(g) (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); *id.* § 5312(a)(2)(Z) (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").

197. *Id.* § 5318(h) (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").

198. *Id.* § 5318(i)(1) (requiring 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" 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").

199. *Id.* § 5318(l)(2) ("The regulations shall, at a minimum, require financial institutions to 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) maintaining 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.").

and (4) increased information sharing between financial institutions about potential money laundering threats.[200]

The Patriot Act also expanded record-keeping requirements, including foreign transactions or transactions in foreign currency or coin.[201] In addition, it offered legal liability protection to financial institutions, incentivizing more extensive record-keeping and reporting without concern for liability.[202] Notably, the Patriot Act allowed for greater sharing of information regarding such reports between federal intelligence agencies.[203] The law also made the Financial Crimes Enforcement Network (FinCEN) a bureau of the United States Department of the Treasury, tasked with monitoring financial institutions' compliance with the new laws and regulations, gathering financial data related to compliance and financial crimes, and offering recommendations.[204]

The Anti-Money Laundering Act (AMLA) of 2020 was passed as part of the National Defense Authorization Act of 2021 to enhance and modernize the AML/CTF laws.[205] It expanded the definition of "financial institutions" under the BSA and the Patriot Act to include antiquities dealers and certain virtual currency activities.[206] The 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).[207] Section 6212 of the AMLA proposes to establish a limited-duration pilot program for sharing SARs.[208] The program allows financial institutions with a SAR reporting obligation to share SARs and related information with the institution's foreign branches, subsidiaries, and affiliates in order to combat illicit finance risks.[209]

---

200. *Id.* § 5311(5) ("[E]stablish 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.").

201. *Id.* § 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).

202. *Id.* § 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).

203. *Id.* § 5318(g)(4)(B); *id.* § 5319.

204. *Id.* § 310.

205. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 3388.

206. 31 U.S.C. § 5312.

207. *Id.* § 5336.

208. *Id.* § 5318(g)(8).

209. *Id.*

However, FinCEN has not yet promulgated rules to implement section 6212.[210] This final rule has been delayed several months from FinCEN's prior rulemaking agenda.[211] Additionally, the AMLA encouraged 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.[212] The AMLA also mandated the creation of new subcommittees of the Bank Secrecy Act Advisory Group, designed to bring together regulatory and law enforcement agencies with financial institutions to coordinate and discuss technological innovation, information security, and confidentiality.[213] As a part of this innovation, the AMLA created a whistleblower program for reporting money laundering violations, the first of its kind within the AML/CFT legal framework.[214]

B. PAYER ANONYMITY DESIGN

The Bank for International Settlements introduced Project Tourbillon in November 2023, a pioneering initiative that seeks to strike a balance between safeguarding user privacy and meeting public policy goals.[215] Project Tourbillon introduces a creative privacy paradigm: payer anonymity, aiming to provide cash-like privacy in CBDC payments.[216] Under this paradigm, privacy is defined as the right to keep personal information confidential and accessible only to a select, trusted group of people.[217]

Project Tourbillon builds on the existing two-tier banking system and engages four primary stakeholders: a central bank, commercial banks (or simply banks), consumers (i.e., payers), and merchants.[218] Consumers and merchants maintain deposit accounts with banks, and banks hold reserve

210. Kaley Schafer, *FinCEN Provides Key Updates on Rulemaking Agenda Timeline*, BALLARD SHAPHR LLP: MONEY LAUNDERING WATCH (July 9, 2023), https://www.moneylaunderingnews.com/2023/07/fincen-provides-key-updates-on-rulemaking-agenda-timeline.

211. *Id.*

212. 31 U.S.C. § 310.

213. Brett Wolf, *US Senate Passes Defense Bill with New Anti-Money Laundering Measures*, THOMSON REUTERS (Dec. 15, 2020), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/defense-bill-anti-money-laundering.

214. *Id.*

215. BANK FOR INT'L SETTLEMENTS, PROJECT TOURBILLON: EXPLORING PRIVACY, SECURITY AND SCALABILITY FOR CBDCS 3–4 (2023) (noting contributors to this project included members of IBM's Research Lab, Consulting, and Technology Currency Network, the Taurus Group, and ETH Zurich).

216. *Id.* at 3. I only selected and summarized necessary technical details for legal analysis in the following Part. For readers interested in a deeper exploration of technical designs and details, please refer to the original paper.

217. *Id.* at 7.

218. *Id.* at 11.

accounts with the central bank.[219] Consumers and merchants can use the Tourbillon app to conduct payments by sending and receiving digital coins.[220]

The app features two types of digital coins: unsigned and signed.[221] "An unsigned coin is a consumer[-]generated digital file with a unique serial number that [has] not (yet) [been signed] by the central bank."[222] A signed coin, on the other hand, is one that has been signed by the central bank and becomes a CBDC coin.[223] Each CBDC coin is a single-use CBDC designed to prevent double spending and ensure that a merchant's sales are duly recorded at their bank.[224]

Banks are tasked with utilizing their existing procedures to combat illicit transactions within this system.[225] They have two key measures: first, all CBDC users—consumers and merchants—must undergo a thorough KYC process to verify their identities.[226] Only those who have completed this process can withdraw, hold, pay, and redeem CBDCs.[227] This initial onboarding process is similar to existing banking practices. Just as a person must have a bank account to withdraw cash from an ATM and undergo KYC procedures (including sharing personal details such as name, address, and social security number with the bank), the same requirements apply here. 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.[228] Banks must also take necessary actions in cases of noncompliance.[229]

Project Tourbillon developed two prototypes to demonstrate how a payer's privacy can be preserved while simultaneously preventing the illicit use of money.[230] Although these prototypes share a similar design ethos, they differ in how the central bank records CBDCs.[231] 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 first prototype

219. *Id.*
220. *Id.*
221. *Id.*
222. *Id.*
223. *Id.*
224. *Id.* at 11–12.
225. *Id.* at 23.
226. *Id.*
227. *Id.*
228. *Id.*
229. *Id.*
230. *Id.* at 11–12.
231. *Id.* at 11.

illustrates two processes: (1) withdrawal and (2) payment and redemption of the CBDC.[232]

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

> (1) Consumer Initiation: The consumer logs into the application and requests to withdraw a specific amount of coins (e.g., 15 coins, which represent 15 dollars).[233] The app then generates two distinct coins with unique identifiers of different denominations: one 10-dollar coin and one 5-dollar coin.[234] At this stage, the coins have not yet been signed by the central bank; therefore, they are not considered CBDCs.
>
> (2) Hashing[235] and Blinding: Utilizing cryptographic techniques, the app hashes and then blinds these coins.[236] Blinding is crucial as it places a signature on each coin without disclosing the unique identifiers to the bank or the central bank.[237]
>
> (3) Bank Processing: These blinded coins are sent to the consumer's bank.[238] The bank then blocks 15 dollars in the consumer's deposit account and forwards the blinded coins to the central bank.[239]
>
> (4) Central Bank Action: The central bank debits 15 dollars from the bank's reserve account and signs the blinded coins with its private key for the respective denominations.[240] Once these coins are signed by the central bank, they become CBDCs.[241] The signature signifies the issuance of the CBDCs. The central bank then sends these signed but still-blinded CBDCs (one 10- and one 5-dollar CBDC) back to the bank.[242]
>
> (5) Finalizing Withdrawal: The consumer's bank debits the consumer's deposit account by 15 dollars and forwards the CBDCs to the consumer.[243]

Consumer Receives CBDCs: Upon receiving the CBDCs, the app unblinds and stores them in the digital wallet.[244]

---

232. *Id.* at 12 (refer to the original description in the BIS report for a detailed understanding of these processes).

233. *Id.* at 11, 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).

234. *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).

235. *Id.* at 13.

236. *Id.*

237. *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).

238. *Id.*

239. *Id.*

240. *Id.* at 13–14.

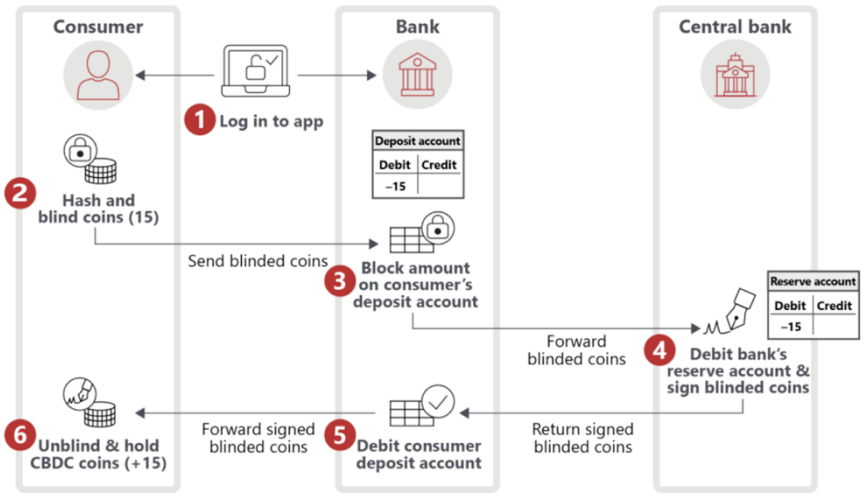
241. *Id.* at 11.

242. *Id.* at 14.

243. *Id.*

244. *Id.*

GRAPH 2 WITHDRAWAL[245]



During this withdrawal process, the consumer's bank knows the consumer's identity and the withdrawal amount.[246] However, the central bank remains unaware of the consumer's identity and the specific amounts withdrawn.[247] The central bank only knows that the bank has withdrawn 15 dollars in total.[248] 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.[249] This process ensures consumer privacy at the central bank level while maintaining necessary transparency at the consumer's bank.

Once the consumer has CBDCs in their wallet, they 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 dollars.[250]

(2) Merchant's Transaction Initiation: Using his app, the merchant creates a pending transaction at the merchant's bank.[251] The merchant then generates a Quick Response (QR) code containing all relevant payment

245. *Id.* at 14.
246. *Id.* at 23.
247. *Id.* at 14.
248. *Id.* at 15.
249. *Id.* at 14.
250. *Id.*
251. *Id.*

details, such as the amount, the merchant's deposit account details, and a transaction number.[252]

(3) QR Code Scanning by Consumer: The consumer uses their app to scan the QR code, which transfers all the necessary payment information to the consumer's app.[253]

(4) Consumer's Payment to Merchant's Bank: The consumer's app selects the 10-dollar CBDC from the wallet and sends it to the merchant's bank, and the merchant's bank then links it to the pending transaction and forwards it to the central bank.[254]

(5) Central Bank Verification: The central bank verifies the signature on the 10-dollar CBDC and checks against a list to ensure this CBDC has yet to be spent.[255] If everything checks out, the central bank redeems the CBDC, adding it immediately to the "spent" list to prevent it from being spent again.[256]

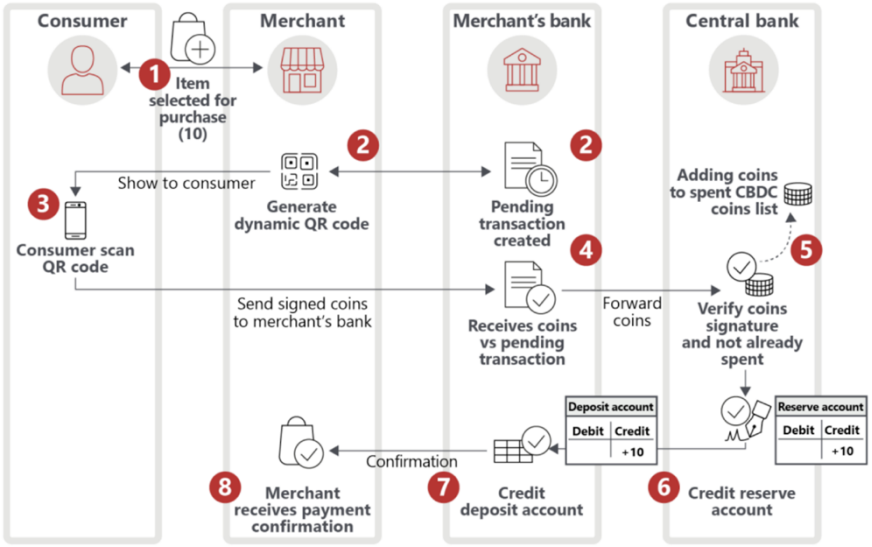
(6) Credit to Merchant Bank's Reserve Account: After redemption, the central bank credits the merchant bank's reserve account and sends a confirmation to the merchant's bank.[257]

(7) Merchant's Bank Credits Deposit Account: The merchant's bank then credits the merchant's deposit account with the 10 dollars.[258]

(8) Notification to Merchant: The merchant's bank notifies the merchant that the transaction has been successfully completed.[259]

252. *Id.*
253. *Id.*
254. *Id.* at 14–15.
255. *Id.* at 15.
256. *Id.*
257. *Id.*
258. *Id.*
259. *Id.*

GRAPH 3 PAYMENT AND REDEMPTION[260]



In this payment and redemption process, the consumer information is not disclosed to any party, including the merchant, banks, and the central bank.[261] The payer is anonymous in this process.[262] The merchant's identity, however, is disclosed to the merchant's bank as part of the payment process but remains confidential there.[263] The central bank will not know the identities of the consumer or merchant.[264] The central bank "does not see any personal payment data but cannot monitor CBDC circulation at an aggregate level."[265]

The key technology in Project Tourbillon is the "blind signature,"[266] 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.[267] Because of this technology, neither the central

260. *Id.*
261. *Id.* at 23.
262. *Id.*
263. *Id.*
264. *Id.*
265. *Id.*
266. *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.").
267. *Id.*

bank nor any third party can trace the coin's spending history back to the payer.[268] This traceability is hindered because the random number crucial for the coin's identification and tracking is known only to the payer and remains blinded in the transaction process.[269] Thus, when the coin is spent, the payer's identity remains anonymous, as the central bank and other entities only see the blinded version of the number.[270] This technical feature is critical in reconciling the privacy concerns of digital dollar users with the transparency requirements of United States 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, reporting, and information-sharing 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 such as 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.[271] The anonymity feature in Project Tourbillon will make compliance with this requirement impossible. Although 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, compliance with the Patriot Act's requirement to establish an AML program can present significant challenges. To establish an AML program, the law mandates that financial entities develop internal policies, designate a compliance officer, conduct employee training, and implement an audit function to test the programs.[272] Although it might appear straightforward to meet these requirements by, for instance, simply hiring a compliance officer to meet the designation requirement, the reality is more

268. *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).

269. *Id.*

270. *Id.*

271. 31 C.F.R. § 1010.312 (2023).

272. 31 U.S.C. § 5318(h).

complex. Without a clear mechanism for filing the reports required by the law, such as being unable to file a CTR report due to the lack of payer information, the compliance officer may struggle to fulfill their duties effectively. As a result, hiring a compliance officer might only satisfy the procedural requirement. It could fail to meet the substantive obligations of the law.

Compliance challenges also 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.[273] Financial institutions must then search their records to see if they have conducted transactions with these parties and report back to the authorities.[274] Because 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.

The enhanced KYC requirement is probably the only requirement that can be met under the Patriot Act. Consumers' and merchants' banks can comply with the requirements for 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.[275] If they want to use a digital dollar, they must open an account at their respective banks. The banks will fulfill KYC requirements by collecting and verifying names, addresses, and other identifying information.

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.[276] Should FinCEN implement this provision, financial institutions handling the digital dollar could struggle to meet these information-sharing requirements given payers' information is anonymous to the merchant's bank. Consequently, the merchant's bank would have difficulty collecting, let alone sharing, such

273. 31 U.S.C. § 5311(5); *see also* Peter D. Hardy & Juliana B. Carter, *AML Information Sharing in the U.S.—Section 314 of the Patriot Act*, BALLARD SPAHR LLP (Oct. 22, 2017), https://www.moneylaunderingnews.com/2017/10/aml-information-sharing-in-the-u-s.

274. 31 U.S.C. § 5311(5).

275. BANK FOR INT'L SETTLEMENTS, *supra* note 215, at 11.

276. Coordinating Oversight, Upgrading and Innovating Technology, and Examiner Reform Act of 2019, H.R. 2514, 116th Cong. § 205 (2019).

personally identifiable information with other financial institutions and the government.

AML/CFT obligations	**Can payer anonymity align with the requirements?**
Currency transaction report	No
AML program	No
Suspicious activity report	No
Enhanced KYC procedures	Yes
Enhanced information sharing	No

IV. MODERNIZATION OF AML/CFT PRACTICES AND LAWS

In the previous Part, the case study of Project Tourbillon illustrates that payer anonymity conflicts with the record-keeping, reporting, and information-sharing requirements under existing AML/CFT laws. To maximize the privacy protection benefits this design could provide for the digital dollar, the Part 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, reporting, and information-sharing 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 customer identification and verification processes, 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. Once consumers initiate a transaction using the digital dollar, 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. Once consumers initiate a transaction (e.g., make a payment request), transaction data begins to accumulate. Upon the collection of transaction data by financial institutions, this data should undergo a rigorous anonymization process.[277] The purpose of this process is to remove or mask personally identifiable information, therefore ensuring the integrity and conditionality of consumer identity.[278]

Data anonymization is a crucial process employed to prevent private information from being traced back to an individual.[279] 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, and encrypting them.[280] This prevents direct identification while preserving the data's utility for analysis.
- Pseudonymization replaces identifying details, such as names, with pseudonyms, effectively concealing the individual's identity to facilitate data usage in analyses without revealing personal information.[281]
- Generalization reduces data precision by modifying it to broader categories or ranges, thus preventing the identification of individuals.[282]
- Data swapping disrupts direct linkages by rearranging variables within the dataset, such as exchanging names with another individual's date of birth.[283]

277. Darbha & Arora, *supra* note 20.

278. *Id.*

279. *Data Anonymization*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/business-intelligence/data-anonymization (last visited Apr. 25, 2025).

280. *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.").

281. *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.").

282. *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.").

283. *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 using methods such as rounding numbers and adding statistical noise, thus maintaining the overall dataset structure while obscuring individual values.[284]
- 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.[285]

These methods are frequently utilized together rather than separately, as different data types may necessitate distinct anonymization techniques for optimal results.[286] For instance, while pseudonymization can effectively conceal 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 preserve the utility of data, whereas synthetic data and data perturbation prioritize privacy preservation. The effectiveness of each technique also depends on the specific context and how the techniques are implemented.

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 and classification, can also be employed to uncover relationships in the dataset and predict outcomes based on historical patterns of detecting suspicious activities. This approach leverages advanced technologies to extract valuable insights from data without compromising the customers' transaction anonymity.

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 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 thirty calendar days after

284. *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.").

285. *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.").

286. *Id.*

the initial detection of facts.[287] However, this timeframe can be too late for addressing illegal transactions, as the acts may have already been completed by the time the information reaches law enforcement agencies. Upon receiving the anonymized account 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. [288] 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.[289]

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, AML/CFT laws should update the record-keeping requirements. Existing requirements, as detailed in Section III, face significant criticism. The need to store, manage, and secure large volumes of data, including sensitive personal information, imposes considerable operational burdens on financial institutions, particularly because much of this data may never be used for combating money laundering and terrorist financing.[290] Critics argue that these extensive record-keeping requirements not only increase the risk of consumer harm in cases of data breaches or privacy violations but also grant these entities the power to access and potentially misuse this information.[291] Additionally, the current record-keeping requirements are criticized for lacking proportionality, as they do not scale appropriately with risk levels.[292] For instance, low-risk transactions are subject to the same stringent rules as high-risk ones, which is seen as unnecessary. Some

287. *Suspicious Activity Reports (SAR)*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html (last visited Apr. 25, 2025).

288. 31 U.S.C. § 5318(k)(2).

289. *Id.*

290. *See, e.g.*, SIMONE DI CASTRI & JEREMIAH GROSSMAN, GSMA, RAADHIKA SHIN, CONSULTANT, PROPORTIONAL RISK-BASED AML/CFT REGIMES FOR MOBILE MONEY: A FRAMEWORK FOR ASSESSING RISK FACTORS AND MITIGATION MEASURES 18 (2015), https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2015/10/Proportional-risk-based-AMLCFT-regimes-for-mobile-money.pdf.

291. *See, e.g.*, Tsang et al., *supra* note 16, at 284.

292. ROBERT G. ROWE, AM. BANKERS ASS'N, RE: REVIEW OF BANK SECRECY ACT REGULATIONS AND GUIDANCE, DOCKET NUMBER FINCEN–2021–0008, at 9 (2022), https://www.aba.com/-/media/documents/comment-letter/clbsa20220214.pdf?rev=1e5cfcc8474843829ad98d10e377bf02.

financial institutions even question the need to retain certain personal records, such as customers' social security numbers.[293]

In a digital dollar system that embraces payer anonymity, record-keeping requirements should evolve to allow for the use of pseudonyms or unique identifiers for individuals instead of recording actual identity details, such as names and social security numbers. Record-keeping requirements could be adjusted based on the risk level of the transactions. Low-risk transactions could be subject to minimal record-keeping, such as recording only the pseudonym and transaction amount, whereas higher-risk transactions might require additional details. The law could also require that sensitive transaction data be encrypted to add an additional layer of security. Record-keeping requirements should also be adaptive, allowing for updates and changes as new technologies and threats emerge.

Second, AML/CFT laws should also change 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, which increases privacy risk.[294] Due to concerns about noncompliance, financial institutions often report any minor suspicious activities, even if they are ultimately found to be legal.[295] The sector has criticized 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.[296]

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 and reported by financial institutions to law enforcement authorities.[297] Most

---

293. *Id.* at 13.

294. FIN. CRIMES ENF'T NETWORK, DEP'T OF TREAS., FIN-2016-A005, ADVISORY TO FINANCIAL INSTITUTIONS ON CYBER-EVENTS AND CYBER-ENABLED CRIME 4–6 (2016).

295. *Id.* at 7.

296. Rowe, *supra* note 292, at 8; *see also* NORBERT J. MICHEL & NICHOLAS ANTHONY, CATO INST., RE: REVIEW OF BANK SECRECY ACT REGULATIONS AND GUIDANCE, DOCKET ID: FINCEN-2021-0008, at 2–3 (2022), 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).

297. PENNY LEE, FIN. TECH. ASS'N, RESPONSE TO REQUEST FOR INFORMATION ON REVIEW OF BANK SECRECY ACT REGULATIONS AND GUIDANCE (FINCEN-2021-0008), at 5–6 (2022), https://www.ftassociation.org/wp-content/uploads/2022/02/FTA_Fincen-Comment-Letter-2.14.22-1.pdf.

importantly, the law should empower financial institutions to exercise discretion in reporting transactions based on clear 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.[298] The study also suggested 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.[299]

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 law should revisit CTR requirements. Currently, the law mandates the reporting of transactions exceeding $10,000 with personally identifiable data.[300] Despite existing exemptions for certain customers, the financial sector advocates for streamlined processes to obtain and apply these exemptions, particularly for low-risk entities.[301] Many financial institutions also complain that the $10,000 threshold is too low without adjusting for inflation.[302] The $10,000 reporting threshold, enacted in 1970, has not kept pace with the decreasing value of the dollar.[303] After adjusting for inflation, $10,000 in 1970 now has the same purchasing power as roughly $74,000, making the reporting threshold increasingly onerous each year.[304]

298. *Risk Assessment Support for Money Laundering/Terrorist Financing*, WORLD BANK GRP. (Feb. 29, 2016), https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support.

299. *Id.*

300. *Suspicious Activity Reports (SAR)*, *supra* note 287.

301. Rowe, *supra* note 292.

302. Michel & Anthony, *supra* note 296, at 3–4.

303. *Id.* at 4.

304. *Id.*

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.[305] In 2018, the Bank Policy Institute conducted an empirical study where a sample of 19 financial institutions reviewed approximately 16 million alerts and filed over 5.2 million CTRs.[306] These reports resulted in an average of only 0.44 percent of CTRs warranting additional review from law enforcement, with even fewer leading to the apprehension of criminals.[307] The second reason is that a real-time reporting system which utilizes 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 identity information and transaction details. This effectively shields payers' financial statuses 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, payer information can still be protected because the attacker would only have access to anonymized data rather than unmasked details. Security is further enhanced if the data has been anonymized in a way that makes it difficult for an attacker to decrypt. This approach not only safeguards personal financial information but also significantly reduces the potential for unauthorized access and misuse of data.

---

305. *Id.* at 2–3, n.2 ("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 . . . .'").

306. BANK POL'Y INST., GETTING TO EFFECTIVENESS—REPORT ON U.S. FINANCIAL INSTITUTION RESOURCES DEVOTED TO BSA/AML & SANCTIONS COMPLIANCE 2 (2018), https://bpi.com/wp-content/uploads/2018/10/BPI-AML-Sanctions-Study-vF.pdf.

307. Michel & Anthony, *supra* note 296, at 2 n.4 ("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.").

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 thirty days to report suspicious activities.[308]

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.[309] What's more, the privacy impact is mitigated by the fact that the data shared remains anonymized, preserving payer privacy while enhancing the efficiency of law enforcement responses. It is important to note that deanonymized 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 risk, 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 toward more value-adding activities. These include investing in advanced technologies and developing expertise, which are more effective at detecting suspicious activities. Law enforcement agencies, instead of being inundated with an overwhelming volume of reports, many of which are unhelpful, now receive more targeted and useful information. This shift allows them to concentrate

308. 12 C.F.R. § 21.11(d) (2012).

309. ANGELENA BRADFIELD, BANK POL'Y INST., RE: REQUEST FOR INFORMATION AND COMMENT REGARDING REVIEW OF BANK SECRECY ACT REGULATIONS AND GUIDANCE (DOCKET NO. FINCEN-2021-0008), at 3–4 (2022), https://bpi.com/wp-content/uploads/2022/02/BPI-Comments-on-FinCEN-Review-of-Bank-Secrecy-Act-Regulations-and-Guidance.pdf.

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 is the quality of the anonymized data, especially when analyzing suspicious activities based on anonymized payer information. Poorly anonymized data can lead to false positives or the omission of 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. Anonymized data 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 legislative bodies, regulatory agencies, financial institutions, merchants, individuals, tech companies, and sometimes the general public. Each group has its own interests and concerns, making it difficult to reach a consensus. Legislatures and regulatory bodies need time and expertise to update laws and promulgate regulations, 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 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.[310] Currently, the expenses associated with regulatory compliance can be mitigated by access to comprehensive client data, which can then be analyzed to enhance the

310. BRIAN JOHNSTON & OMER SOHAIL, DELOITTE, FINALLY: CUSTOMER ANALYTICS FOR BANKS 1 (2011), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-customer-analytics-102711.pdf.

sale of existing services or be sold in bulk to data brokers.[311] 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, even though the payer's identity is anonymized, the payee's (the merchant's) information remains visible.[312] 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 burdens and calls for simplification and modernization of AML/CFT requirements,[313] this presents an opportunity to advocate for these changes and their advantages to financial institutions.

CONCLUSION

This Article demystifies the exaggerated concern that a digital dollar would serve as a tool for government surveillance, demonstrating instead that a digital dollar can offer enhanced privacy protections through the examination of current technical designs. This Article advocates for the integration of privacy-preserving features into the digital dollar system and the modernization of AML/CFT laws. The successful design and implementation of such a framework would not only make the digital dollar a viable option, should the Federal Reserve choose to issue it, but would also positively impact digital payment systems more broadly, leading to stronger privacy protections in the digital age. By adopting privacy-preserving designs and modernizing AML/CFT regulations, we can strike a careful balance between safeguarding individual privacy and achieving public interest objectives, such as combating money laundering and terrorist financing.

---

311. *Id.*; *see also* Anick Jesdanun, *For Banks, Data on Your Spending Habits Could Be a Gold Mine*, A.P. NEWS (Dec. 2, 2019, 9:49 AM PDT), https://apnews.com/general-news-2f5ed45a59d0439fad6b9641f30b65a8.

312. BANK FOR INT'L SETTLEMENTS, *supra* note 215, at 8.

313. Rowe, *supra* note 292, at 2; Michel & Anthony, *supra* note 296, at 3; Bradfield, *supra* note 309, at 1–2.

As we move toward the potential issuance of a digital dollar in the United States or any CBDC around the world, it is crucial to address broader issues that fall outside the scope of this Article. Future research should focus on building trust between the government and individuals, as trust is foundational to the widespread adoption of a CBDC or any financial infrastructure in which the government participates. Additionally, the collaboration among different entities, including private sector participants and international stakeholders, will be vital for the successful deployment of CBDCs. More research is needed on the economic impacts of CBDCs, particularly on financial stability and the broader economy. Addressing these issues will be essential for ensuring that a CBDC not only protects privacy but also supports a resilient and inclusive financial system.