PRIVACY IMPLICATIONS OF CENTRAL BANK DIGITAL CURRENCIES

Jiaying Jiang*

Abstract

One hundred five countries, representing over 95 percent of global GDP, are exploring central bank digital currencies (CBDCs), a new form of digital money that is different from privately issued cryptocurrencies and stablecoins. As central banks worldwide grapple with CBDC design options, privacy has become a critical feature and concern. Many central banks, government agencies, NGOs, think tanks, and even the general public have already addressed the importance of privacy and called for privacy in CBDC systems. Some economists, computer scientists, engineers, and legal scholars have already moved forward to design a privacy-preserving CBDC.

However, when addressing the importance and preservation of privacy, all parties seem to overlook two very important issues: (1) What does privacy mean here? and (2) What privacy problems do CBDCs create? Before proposing solutions, one must understand which problems must be solved. In this article, I explore these two critical issues. I first adopt Daniel Solove's pragmatic approach to conceptualizing privacy in the context of CBDCs. Next, I investigate the dataflow of four structural and foundational CBDC designs and conclude that each design will result in various potential privacy issues, including mass surveillance, misuse and abuse of CBDC data by central banks and intermediaries, and more.

This article makes four contributions. First, it fills the gap in the privacy and CBDC literature (which lacks a thorough analysis of the concept of privacy in the CBDC context) and lays the foundation for future work on solutions to protect privacy by first identifying privacy problems that could occur in various CBDC designs. Second, this article helps central banks rethink their roles in the digital age, especially in a situation where the use of central bank money (i.e., cash) is shrinking dramatically and central banks' authority is constantly challenged by the privately issued digital currencies such as cryptocurrencies and stablecoins. Third, this article benefits commercial banks and payment service providers and helps them seize the opportunity to work with central banks to provide a CBDC that meets users' needs and strengthen their roles in the financial and payment markets. Fourth, this article particularly benefits individuals, both everyday mobile-payment users and the unbanked and underbanked populations. It not only educates individuals about the privacy problems that could occur if one decides to use CBDCs but also equips potential users with the knowledge necessary to demand privacy protection in CBDC systems.

[*] Jiaying Jiang, Assistant Professor of Law, University of Florida Levin College of Law. I started this project when I was a Hauser Global Fellow at New York University School of Law, so I am grateful to many NYU Law colleagues for their early-stage feedback. Special thanks to Joseph Weiler, Grainne de Burca, Katherine Strandburg, Alexandre de Streel, Thomas Bustamante, You Kyung Huh, Henning Lahmann, Yuanyuan Ren, Ying Zhou, Sergio Alonso de Leon, Andrej Lang, Francesca Episcopo, Thomas Streinz, Aniket Kesari, Elettra Bietti, Abert Fox Cahn, Stav Zeitouni, Tomer Kenneth and Kate Geddes. I am also indebted to many industry experts, central bank officials (whose names remain confidential), and academics. Special thanks to Herve Troupe, Sonja Davidovic, Jonas Gross, Karl Wust, Jamiel Sheikh, Henry Holden, Mike Alonso, Robert Oleschak, and participants at the 2022 Law and Society Annual Meeting for their generous time and valuable insights. I also greatly appreciate my research assistant, Aslesha Parchure, for her excellent work on this project.

INTRODUCTION

Institutions around the globe define central bank digital currencies (CBDCs) differently. The Federal Reserve Bank defines a CBDC as "a digital liability of a central bank that is widely available to the general public."[1] 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."[2] 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"[3] and that works as "a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank."[4] The European Central Bank envisions that CBDC could be an alternative to euro banknotes and could complement cash by serving as "an electronic form of money, issued by the Eurosystem, [that] would be accessible to all citizens and firms."[5]

Broadly speaking, CBDCs can be defined as a new form of money—a digital liability issued and guaranteed by a central bank. Depending on its purpose and design, a CBDC could be a "retail" CBDC or a "wholesale" CBDC. If the CBDC is intended to be a digital equivalent of cash and widely accessible by end users (households and businesses), it is referred to as a "retail" or "general purpose" CBDC.[6] In contrast, if the CBDC is available only to selected institutions, mostly banks, it is referred to as a "wholesale" CBDC, similar to today's central bank reserve and settlement accounts.[7] This paper will address only retail CBDCs because retail CBDCs directly involve individuals and raise the research questions of this paper.

The Atlantic Council has been tracking the current state of CBDC development across the globe. One hundred five countries, representing over 95 percent of global GDP, are exploring a CBDC.[8] Of the 105 countries tracked by the Atlantic Council, as of May 2022, 9 percent have launched CBDCs, 14 percent are in the pilot stage, 23 percent are in the development stage, and 41 percent are in the research stage.[9] The Bahamas launched its Sand Dollar in October 2020, making it the first country to launch a CBDC.[10] In May 2022, the Bank of Jamaica announced a phased rollout of its CBDC, the JAM-DEX.[11] The Eastern Caribbean Central Bank launched

[1] Board of Governors of the Federal Reserve System, *Central Bank Digital Currency (CBDC)*, https://www.federalreserve.gov/central-bank-digital-currency.htm (last updated Jun 30, 2022).
[2] TOMMASO MANCINI-GRIFFOLI, ET AL., CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY INTERNATIONAL MONETARY FUND 7 (2018).
[3] Bank for International Settlements, CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, 3 (2020), https://www.bis.org/publ/othp33.pdf (citing Bank for International Settlements, COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES - MARKETS COMMITTEE: REPORT ON CENTRAL BANK DIGITAL CURRENCIES 4 (2018), https://www.bis.org/cpmi/publ/d174.pdf).
[4] CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, *supra* note 3, at 3.
[5] European Central Bank, *A Digital Euro*, https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (last visited Jul. 28, 2022).
[6] Codruta Boar & Andreas Wehrli, *Ready, Steady, Go?: Results of the Third BIS Survey on Central Bank Digital Currency* (BIS Papers No. 114, Jan. 27, 2021), https://www.bis.org/publ/bppdf/bispap114.pdf.
[7] *Id.*
[8] Ananya Kumar, et al.
, *Central Bank Digital Currency Tracker*, ATLANTIC COUNCIL, https://www.atlanticcouncil.org/cbdctracker/ (last visited Jul. 22, 2022).
[9] *Id.*
[10] *Id.*
[11] *Id.*

DCash in March 2021 in four member states and later expanded to three more.[12] Nigeria also has a live retail CBDC.[13]

In addition, 72 central banks have communicated publicly in positive tones about their CBDC work.[14] China's central bank is at a very advanced stage of experimenting with its CBDC, and it has run pilot programs in ten cities.[15] The European Central Bank has issued a report on a digital euro that examines the issuance of a CBDC from the perspective of the Eurosystem.[16] The Federal Reserve of the United States is still debating whether the United States needs a CBDC and has fostered a broad and transparent public dialogue about the potential benefits and risks of a US CBDC.[17] The Federal Reserve Bank of Boston and MIT have tested the technology, publishing a report called Project Hamilton, and in March 2022, the White House published an executive order on digital assets. The Biden administration places the highest urgency on research and development efforts exploring the potential design and deployment options of a US CBDC.[18]

As central banks experiment with CBDCs and grapple with the ideal design of a CBDC, privacy has become one of the most prominent aspects of this development and a great concern they must consider and address. Major central banks have already addressed the importance of privacy. The European Central Bank conducted a public consultation on a digital euro.[19] Both citizens and professionals participating in the consultation considered privacy the most important feature of a digital euro.[20] The Federal Reserve emphasized that one key policy consideration when examining the pros and cons of a potential US CBDC is how to preserve the privacy of citizens and maintain the ability to combat illicit finance.[21] China's central bank, the People's Bank of China, has adopted strict compliance with regulations on data and privacy protection as a key principle of the institutional design of its CBDC system and has already moved forward

[12] *Id.*

[13] Jack Ree, *Five Observations on Nigeria's Central Bank Digital Currency*, (Nov. 16, 2021) https://www.imf.org/en/News/Articles/2021/11/15/na111621-five-observations-on-nigerias-central-bank-digital-currency (last visited: Jul. 28, 2022)

[14] *Id.*

[15] Working Group on E-CNY Research and Development of the People's Bank of China, *Progress on Research and Development of E-CNY in China*, PEOPLE'S BANK OF CHINA (Jul. 2021) http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf. See also Joasia Popowicz, *China Expands E-yuan Pilot,* (Apr. 4, 2022) https://www.centralbanking.com/fintech/cbdc/7945516/china-expands-e-yuan-pilot

[16] EUROPEAN CENTRAL BANK, REPORT ON A DIGITAL EURO 3 (2020).

[17] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, FEDERAL RESERVE, https://www.federalreserve.gov/publications/january-2022-cbdc.htm (last updated: Jan. 20, 2022). Eleven cities will begin trials of the CBDC, in addition to ten existing pilot cities, according to the People's Bank of China.

[18] Ensuring Responsible Development of Digital Assets, 87 FED. REG. 14,143, 14145 (Mar. 14, 2022).

[19] EUROPEAN CENTRAL BANK, EUROSYSTEM REPORT ON THE PUBLIC CONSULTATION ON A DIGITAL EURO 2 (2021), https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf.

[20] *Id.* at 10. What the respondents want most from a digital euro is privacy (43%), security (18%), usability across the euro area (11%), the absence of additional costs (9%) and offline use (8%). The preference for privacy is also high among citizens of all ages but increases mildly with age: 39% of respondents under 35 years, 45% between 35 and 55 years and 46% of respondents aged 55 and over give the highest prominence to privacy.

[21] BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, *supra* note 17.

with the design of "managed anonymity" to protect privacy and user information in its CBDC pilot program.[22] The Bank of Canada has outlined what is technologically feasible for privacy in a CBDC and suggested a design approach for CBDC privacy.[23]

Governments, NGOs, and think tanks have also called for privacy protection in the design of a CBDC. The White House executive order on digital assets demanded privacy protections in any future dollar payment system, including a US CBDC.[24] The Digital Dollar Project emphasized that privacy "is of the essence for living in a free country that respects individuals and individual rights" and proposed a few guiding principles for privacy when designing a potential US CBDC.[25] The World Economic Forum studied privacy architecture examples in use today and particularly addressed the role of digital identity in privacy for CBDCs.[26] It further suggested that central banks should balance privacy and financial crime management in a CBDC world.[27] The Bank for International Settlements has repeatedly directed society's attention to the importance of privacy and the need to strike this balance between public privacy and reducing illegal activity.[28] Neha Narula, director of MIT Media Lab, said that there is still a policy discussion happening around privacy, how much data should be stored at the central bank, and how much should be stored in intermediaries.

Some economists, computer scientists, engineers, and legal scholars have already moved forward to design a CBDC with privacy protection. For instance, Sarah Allen et al. discussed from whom the CBDC should protect sensitive identity and/or transaction data.[29] Jonas Gross et al. argued that a CBDC system should provide at least the same privacy-preserving features as cash in order to secure access to a fully private, regulation-compliant form of money.[30] They proposed a software-based CBDC that imposes limits on anonymous payments in order to support full privacy while addressing constraints related to anti-money laundering and countering the

[22] Working Group on E-CNY Research and Development of the People's Bank of China, *supra* note 15, at 5.

[23] Sriram Darbha & Rakesh Arora, *Privacy in CBDC Technology*, BANK OF CANADA (Jun. 2020) https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/.

[24] Exec. Order. No. 14,067, 87 FED. REG. 14143 (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

[25] People should be able to use a U.S. CBDC without making themselves subject to undue corporate tracking or government surveillance. People may benefit from above-board, contractual sharing of information with financial services providers, or they may refuse it. Law enforcement access to CBDC usage data should be strictly controlled by due process, and other applicable U.S. law, including the Fourth Amendment. The Digital Dollar Project Privacy Sub-Committee, *Privacy Principles for a Digital Dollar*, DIGITAL DOLLAR PROJECT (Oct. 2021) https://digitaldollarproject.org/wp-content/uploads/2021/10/DDP-Privacy-Principles-10.25.21_Final.pdf.

[26] WORLD ECONOMIC FORUM, PRIVACY AND CONFIDENTIALITY OPTIONS FOR CENTRAL BANK DIGITAL CURRENCY (2021) https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.

[27] *Id.*

[28] CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, *supra* note 3, at 6; *see also* Raphael Auer & Rainer Böhme, *The Technology of Retail Central Bank Digital Currency*, BIS Quarterly Review, 86 (Mar. 2020), http://ssrn.com/abstract_id=3561198 (They discuss different technical designs satisfy the criteria of safeguarding user privacy and allowing for effective law enforcement to varying degrees due to trade-offs associated with design choices. There is a trade-off between privacy and ease of access on one hand and ease of law enforcement on the other, with the associated design choice being whether access to the CBDC uses account-based technology or token-based technology.).

[29] Sarah Allen et al., *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations* 44 (NBER Working Paper 27634, 2020) http://www.nber.org/papers/w27634.pdf.

[30] Jonas Gross, et al., *Designing a Central Bank Digital Currency with Support for Cash-like Privacy* 2 (Jul. 26, 2021), http://ssrn.com/abstract=3891121.

financing of terrorism; privacy and regulatory compliance can be provided by design.[31] More specifically, they proposed using zero-knowledge proof to enable users to reveal their payment history to provide evidence for integrity and completeness without revealing personal or identifiable information.[32] Nadia Pocher et al. proposed implementing privacy-enhancing technologies (PETs) to protect individual privacy by protecting data.[33]

All the aforementioned central banks, government agencies, NGOs, think tanks, scholars, and even the general public seem to agree that privacy is important and that, if a central bank decides to issue a CBDC, it should design the CBDC to be privacy-preserving. However, when discussing the importance and preservation of privacy, all parties seem to miss two very important issues: (1) *What does privacy mean here?* and (2) *What privacy problems do CBDCs create?*

In this article, I address these two critical issues. I adopt Daniel Solove's pragmatic approach to conceptualizing privacy in the context of CBDCs by focusing on understanding privacy in specific contextual situations rather than attempting to illustrate an abstract conception of privacy. The first step is to understand CBDC practices: What are the contexts? Who are the actors? What are the norms? The next step is to explore which aspects of these practices should be considered private and what other values to balance when recognizing and protecting the value of privacy in CBDC practices.

I argue, in the context of CBDCs, that privacy is not a separate abstract conception but a dimension of the practice of CBDC payments. Privacy is a part of payment practices. Payment practices include a payer sending a payee some money (in the form of a CBDC), entities processing the payment by updating the balance sheet, and law enforcement agencies investigating certain information about the payment to make sure the payment is legitimate. Since privacy is a part of payment practices, certain information or actions related to CBDC payments should be considered private. Any disruption to those things considered private would be a violation of privacy. What should be considered private is a normative argument and may vary across jurisdictions, cultures, and times. When conducting normative analysis, it is necessary to balance the value of CBDC data privacy with other conflicting values.

Next, as a methodology for understanding what privacy problems would arise from various design choices, I first study the dataflow of four structural and foundational design choices. Following the dataflow, I investigate who could get access to what data. Each design varies in who can see, store, collect, and share CBDC-related data, which includes but is not limited to identity data and transaction data. Some data are encrypted, but some are not. All these factors contribute to potential disruptions in the practice of CBDC payment (i.e., privacy problems), including but not limited to state surveillance and the abuse and misuse of CBDC data by central banks and intermediaries.

[31] *Id.* at 33.

[32] *Id.*

[33] Nadia Pocher & Andreas Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme* 5 (Mar. 10, 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3759144.

This article makes four contributions at the theoretical and practical levels. First, at the theoretical level, this article fills a gap in privacy and CBDC discussions. Most existing CBDC literature focuses on the potential impacts of CBDCs on other forms of money (e.g., cryptocurrencies, commercial bank e-money); the relationship between central banks and other entities, especially commercial banks; the ability of CBDCs to improve financial inclusion; and cross-border applicability of CBDCs. Very limited attention has been paid to privacy in those discussions. Although central banks, government authorities, and some scholars have recognized the importance of privacy and called for privacy protection, they have failed to explain what privacy means and what privacy problems could occur in the CBDC context; thus, a robust privacy solution seems impossible without first understanding the issues. This article bridges the gap by providing a pragmatic approach to conceptualizing privacy and by identifying privacy issues in various CBDC designs, which lays a foundation for future work on designing privacy-preserving CBDCs.

At the practical level, this article educates technology specialists, legal scholars, and policymakers and bridges the gap between the tech world and the legal and policy world. Miscommunication and ignorance of each other's fields has been one of the biggest challenges in advancing technological innovations that benefit society. This piece educates technology specialists (e.g., engineers and computer scientists) on legal and policy considerations (e.g., anti-money laundering and combating the financing of terrorism) so they can take these issues into consideration at the design stage and design a CBDC that meets policy needs as well as regulatory requirements. This piece also helps legal scholars and policymakers understand the basic technical designs and uniqueness of CBDCs and the privacy issues in CBDC designs so they can propose rigorous policies, accurately apply privacy laws and regulations, and properly address legal issues.

Second, this paper helps central banks rethink their roles in the digital age, especially in a situation where the use of central bank money (i.e., cash) is shrinking dramatically[34] and central bank authority is constantly being challenged by the prevalence of privately issued digital currencies such as cryptocurrencies and stablecoins.[35] In response, central banks can provide an payment alternative, CBDC, that not only ensures the general public's continuous access to central bank money, but also restores central banks' authority in the area of payments. One of the most important features that users demand and are concerned about in the design of a CBDC is privacy. If privacy issues go unaddressed, widespread adoption of CBDCs will not be possible. This article helps the 95 percent of central banks worldwide that are actively engaging in some form of CBDC work to understand which privacy problems exist in four popular designs so that central banks can come up with an optimal CBDC design that meets the privacy needs of the general public, thus enabling widespread adoption.

Third, this paper enables intermediaries, especially commercial banks and other payment service providers, to navigate their roles in a world full of financial technology (fintech) innovations. Some ongoing fintech movements have been touting trustless infrastructure and peer-to-peer transactions with the goal of removing intermediaries. Such movements directly threaten

[34] Stephen Williamson, *Central Bank Digital Currency: Welfare and Policy Implications* 1-2, MICHIGAN STATE UNIVERSITY DEPARTMENT OF ECONOMICS (May 31, 2021), http://econ.msu.edu/seminars/docs/digital10.pdf.
[35] Kumar et al., *supra* note 8.

commercial banks and other traditional financial institutions. CBDCs led by central banks present intermediaries with a new opportunity to strengthen their roles in the financial and payment markets. Due to policy considerations, central banks are highly unlikely to disintermediate these intermediaries but rather will likely work with them to issue CBDCs. This paper will also help intermediaries understand users' privacy needs and choose a suitable CBDC design that meets those needs. By actively participating in CBDC designs and offering consumer-facing services, intermediaries will not only reinforce their roles and abilities in fintech movements but also improve their relationships with central banks and individuals.

Fourth, this article particularly benefits individuals, not only those who have access to digital payments and digital financial services, but also unbanked and underbanked populations. This article educates existing digital payment users on the differences between CBDCs and other payment tools. It further helps them understand the kinds of privacy problems or potential disruptions to individuals' privacy that could occur if one decides to use a CBDC. This article's privacy principles also equip individuals with sufficient knowledge to demand privacy protection from CBDC designers. In addition, many central banks have touted the use of CBDCs to improve financial inclusion. Through this paper, the unbanked population, which numbers 1.7 billion,[36] and the even greater underbanked population can learn that access to easier payment systems and financial services is not free and sometimes comes with high privacy costs. For instance, financial entities could constantly monitor and monetize users' CBDC data, and the worst-case scenario is state surveillance.

This article consists of two parts. Part I conceptualizes privacy in the context of CBDCs, using Daniel Solove's pragmatic approach. It argues that privacy should be understood contextually. What should be considered private in CBDC practice is a normative argument based on values and cultures, and the answer can vary in different jurisdictions and at different times. Part II investigates what privacy issues a CBDC might create. It studies the dataflow of four popular CBDC design options, examining their operational models and architecture. It reveals which entities can collect, store, get access to, and potentially make use of users' data in a CBDC system. Based on the dataflow and various entities' roles in CBDC systems, it concludes that privacy invasions—such as mass surveillance or misuse and abuse of CBDC data by the central bank and intermediaries—could occur within various design options.

I. Conceptualizing Privacy in the Context of CBDCs

All these central banks, relevant government agencies, NGOs, think tanks, scholars, and even the general public seem to agree that privacy is important and that, if a central bank decides to issue a CBDC, it should design the CBDC to be privacy-preserving. However, before discussing how important privacy is and how to preserve privacy, the first question to ask should be: *What does privacy mean here?*

A. Existing Conceptions of Privacy

[36] The World Bank, *Financial Inclusion*, https://www.worldbank.org/en/topic/financialinclusion/overview (last updated: Mar. 29, 2022).

The notion of privacy is not consistent across the globe.[37] Defining privacy has proven to be quite complicated, and many find it difficult to precisely define privacy.[38] According to Julie Inness, the legal and philosophical discourse of privacy is in a state of chaos.[39] Jurists, legal scholars, philosophers, psychologists, and sociologists appear to have a welter of different conceptions of privacy.[40] All these conceptions of privacy, as Daniel Solove argued, can be dealt with under six general headings that capture the recurrent ideas in the discourse.[41] These headings include:

"(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."[42]

However, many scholars have criticized that these conceptions and theories of privacy are either too narrow or too broad.[43] Take the conception of the right to be let alone as an example, although Samiel Warren and Louis Brandeis, in their famous article, *The Right to Privacy*,[44] inspired significant attention to privacy and framed the discussion of privacy in the United States throughout the twentieth century, [45] their conception of privacy as being let alone fails to provide much guidance about how privacy should be valued with regards to other interests, such as free speech, effective law enforcement, and other values.[46] Being let alone does not inform us about the matters in which we should be let alone.[47] Therefore, many commentators argue that defining privacy as the right to be let alone is too broad.[48]

[37] WORLD ECONOMIC FORUM, *Privacy and Confidentiality Options for Central Bank Digital Currency* 3 (2021), https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf (last visited Mar 29, 2022); *See also* 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).

[38] Daniel J. Solove & Paul M. Schwartz, INFORMATION PRIVACY LAW 43, (Wolters Kluwer eds., 7th ed. 2021).

[39] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2022) . *See also* Julie C. Inness, PRIVACY, INTIMACY, AND ISOLATION 3 (Oxford Univ. Press 1992).

[40] Solove, *supra* note 113, at 1092.

[41] Solove & Schwartz, *supra* note 112, at 43.

[42] Solove, *supra* note 113, at 1087.

[43] In Solove's paper, he critiqued all six categories of conceptions and explained why each conception is either too broad or too narrow or both. Solove, *supra* note 113 at 1094.

[44] Warren and Brandeis defined privacy as the "right to be let alone," a phrase adopted from Judge Thomas Cooley's treaties on torts in 1880. Cooley's right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defining a right to privacy. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); *See* Robert E. Smith, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOUSITY FROM PLYMOUTH ROCK TO THE INTERNET 128 (Chisheng Li ed. 2000).

[45] Solove, *supra* note 113 at 1100; *See also* Irwin P. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 704 (1990); Harry Kalven has even hailed it as the "most influential law review article of all." Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 481-82 (1990).

[46] Solove, *supra* note 113, at 1101.

[47] *Id.*

[48] *Id.* at 1102; *See also* David M. O'Brien, PRIVACY, LAW, AND PUBLIC POLICY 5, 16 (Praeger 1979); Tom Gerety, *Redefining Priva*cy, 12 HARV. C.R.-C.L. L. REV. 233, 234, 263 (1977).

Additionally, privacy is a deeply personal concept; individuals have their own barometer of what they consider private, including when and with whom their personal information can be shared.[49] Under different scenarios, what an individual considers private might no longer be such if the person or entity this individual is dealing with changes. It is difficult to have one conception that covers all scenarios a person might face.

B. Pragmatic Approach to Conceptualizing Privacy

The existing method of conceptualizing privacy has thus far proven to be problematic and unsatisfying.[50] In response, Daniel Solove proposed a pragmatic approach to conceptualizing privacy. Pragmatism recognizes context and contingency, rejects a priori knowledge, and focuses on concrete practices.[51] According to pragmatists, knowledge originates through experience.[52]

Pragmatism has its philosophical grounds. Just as John Dewey suggests, philosophical inquiry begins with problems in experience, not with abstract universal principles.[53] Pragmatism also has many affinities with Wittgenstein's notion of family resemblances.[54] This notion of family resemblances demonstrates that "universals are neither necessary nor even useful in explaining how words and concepts apply to different things."[55] "A new application of a word or concept will still have to be made out, explained, in the particular case and then the explanations themselves will be sufficient . . . ."[56] This notion frees us from engaging in the debate over necessary and sufficient conditions for privacy, from searching for rigid conceptual boundaries and common denominators.[57] It focuses on mapping out the terrain of privacy by examining specific problematic situations.[58]

In line with this pragmatic philosophy, Solove's pragmatic approach emphasizes the contextual and dynamic nature of privacy.[59] It conceptualizes privacy in particular contexts rather than

[49] *The Digital Dollar Project: Exploring a US CBDC*, DIGITAL DOLLAR FOUNDATION at 20.
[50] Solove, *supra* note 113, at 1126.
[51] *Id.* at 1127.
[52] *Id.* at 1127. Pragmatists reject the view of philosophy "as a purely theoretical quest for eternal truths or knowledge of an ultimate and unchanging reality." PRAGMATISM AND CLASSICAL AMERICAN PHILOSOPHY: ESSENTIAL READINGS AND INTERPRETIVE ESSAYS 3 (John J. Stuhr ed., 2000); *see also* John Dewey, *Reconstruction in Philosophy*, in 12 THE MIDDLE WORKS OF JOHN DEWEY 72 (Jo Ann Boydston ed., 1982); Many pragmatists go beyond making the epistemological claim that an ultimate or transcendent reality is not knowable. Some philosophers, observes John Dewey, "have not ventured to deny that [an ultimate reality] would be the appropriate sphere for the exercise of philosophic knowledge provided only it were within the reach of human intelligence." Dewey, *supra* at 72. Dewey claims that philosophy is still possible by exploring knowledge gleaned from experience.
[53] Solove, *supra* note 113, at 1127. *See also* John Dewey, EXPERIENCE AND NATURE 9 (George Allen and Unwin 1929). Thinking is thus a "tool" for solving problems. Michael Eldridge, TRANSFORMING EXPERIENCE: JOHN DEWEY'S CULTURAL INSTRUMENTALISM 4 (Vanderbilt Univ. Press, 1st ed. 1998).
[54] Solove, *supra* note 113, at 1126.
[55] Stanley Cavell, *Excursus on Wittgenstein's Vision of Language*, in THE NEW WITTGENSTEIN 35 (Alice Crary & Rupert Read eds., 2000).
[56] *Id.*
[57] Solove, *supra* note 113 at 1126.
[58] *Id.*
[59] *Id.* at 1127.

privacy in the abstract.[60] And it does not follow traditional accounts of privacy that seek to conceptualize privacy in general terms as an overarching category with necessary and sufficient conditions.[61] Conceptualizing privacy is about understanding and attempting to solve certain problems.[62] Solove contends that privacy problems involve disruptions to certain practices.[63] By "practices," he refers broadly to various activities, customs, norms, and traditions.[64] Examples of practices include writing letters, talking to one's psychotherapist, talking to one's lawyer, engaging in sexual intercourse, and so on.[65] Privacy is a dimension of these practices, and under this approach, privacy should be understood as part of these practices rather than a separate abstract conception.[66]

"When we protect privacy, we protect against disruptions to certain practices. A privacy invasion interferes with the integrity of certain practices and even destroys or inhibits such practices. 'Privacy' is a general term that refers to the practices we want to protect and to the protections against disruptions to these practices."[67]

To understand practices and disruptions to practices properly, two additional concepts are particularly relevant: private matters and the value of privacy. Turning our focus from disruptions to the practices they disrupt, we often refer to aspects of these practices as "private matters."[68] In other words, we say that certain things, places, and affairs are "private."[69] Traditionally, one considers one's house, one's diary, one's body, and one's sexual behavior private.[70] This is a territorial view of privacy. In a digital world or in cyberspace, this territorial view of privacy has very limited applications because privacy is no longer simply a form of space.[71] Instead, privacy is embedded in activities or norms that are naturally borderless. In the digital world, one can consider one's online photos, text messages, voice messages, emails, and investment portfolios private.

Determining what should be considered private and determining what the law should protect as private involve a normative analysis. Whether certain things, places, or affairs are private can vary in different jurisdictions, cultures, and times. The law should weigh the value of keeping certain things, places, or affairs private against other values that may be in conflict. For instance, keeping one's online photos and text messages private is valuable because it would protect one's safety, dignity, and autonomy, as well as the ability to control and live one's life as one desires. Any disclosure of those photos and messages could create enormous psychological stress and pain and/or physical threat and harm to the person. However, assuming these photos and text messages involve human trafficking, government (even the general public) obtaining access to

[60] *Id.*
[61] *Id.*
[62] *Id.* at 1129.
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.* at 1127.
[68] *Id.* at 1131.
[69] *Id.*
[70] *Id.* at 1132.
[71] Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 40 (1998).

photos and messages would benefit many families suffering from losing their children or other loved ones. Society would be better off if such information were public (in other words, one person's state of being private is violated or destroyed). The law should evaluate these conflicting values to decide if certain matters should be private.

A. Pragmatic Approach in the Context of CBDCs

The pragmatic approach is particularly helpful when thinking about privacy in the context of CBDCs. The first reason is that no other traditional conceptions of privacy can properly and accurately explain privacy in this context. It seems all conceptions are relevant, but they are either too broad or narrow when conceptualizing privacy in the CBDC context. For instance, under Samuel Warren and Louis Brandeis' famous formulation for the right to privacy, yes, privacy in the context of CBDCs is also about one's right to be let alone. One has the right to live one's life as one chooses, including one's financial life, such as whom one wants to transact with, where and when one makes a payment, free from intrusion or invasion. Government cannot conduct surveillance of the financial records of millions of Americans under the Fourth Amendment. However, this interpretation ignores the practice that a CBDC system should allow for limited government access to CBDC data to prevent money laundering and financing of terrorism. Brandeis could not have anticipated that the right to privacy would be pitted against national security and the challenge of terrorism.[72] The stakes are considerably higher today than in Brandeis' time in the 1890s.[73]

Another example is the conception of "limited access to the self." Yes, privacy in the context of CBDCs is also about one's ability to shield oneself from unwanted access by others. CBDC data holders probably do not want to share their financial data with the general public and take some measures to shield themselves from unwanted access. However, "unwanted" access can be a very subjective standard—some are very concerned about any unauthorized access by any unauthorized person(s) or by an authorized person(s) in an unauthorized manner, whereas some allow for a greater extent of access by others in various manners. The CBDC system would by default allow for access by others, regardless of whether the access is "unwanted" or "wanted." The person's preference does not matter in some cases because multiple parties, such as the central bank, commercial banks, or other money service providers, depending on the design, have to get access to CBDC data in order to process payments. The "limited access to the self" conception of privacy fails to consider this situation in the CBDC context.

The examples can go on and on under each of the headings of the current privacy conceptions, such as secrecy, control over personal information, personhood, and intimacy. All these traditional conceptions are too broad and abstract to capture all aspects of privacy in the context of CBDCs. Therefore, we need an alternative to understand privacy.

The second reason that this pragmatic approach is helpful for understanding privacy in the context of CBDCs is that this approach is flexible enough to capture many practical and nuanced questions. CBDC-related privacy questions are particularly practical and nuanced. Various

[72] Leah Burrows, *To be let alone: Brandeis foresaw privacy problems*, BRANDEISNOW, Jul. 24, 2013 https://www.brandeis.edu/now/2013/july/privacy.html (last visited Jul 4, 2022).
[73] *Id.*

designs can raise very different privacy questions. As elaborated in Section B below, one-tier and two-tier designs will allow for different parties to obtain access and collect and store CBDC data, which will raise different privacy questions. Centralized and DLT designs will expose very different CBDC information to different parties involved. Various parties, such as the payer, the payee, the central bank, commercial banks, and other authorized entities, would participate in a CBDC transaction. Each party has its unique set of privacy problems to address. Privacy thus means different sets of rights and obligations to each of the parties. No one single conception of privacy can capture all problems arising from different settings and for all parties. The pragmatic approach is more suitable because it addresses privacy contextually in different scenarios and addresses different problems that each party is facing. It ties in with particular problems in the given context, which allows for a better understanding of privacy in all dimensions.

Therefore, in this article, I adopt Daniel Solove's pragmatic approach to conceptualizing privacy in the context of CBDCs by focusing on understanding privacy in specific contextual situations rather than seeking to illustrate an abstract conception of privacy. The first step is to understand CBDC practices—what are the contexts? who are the actors? what are the norms/activities? The next step is to explore what aspects of these practices should be considered private and what other values to balance when recognizing and protecting the value of privacy in the CBDC practices.

The specific contextual situation related to CBDCs centers on the practice of payment or, to be more precise, making payments with CBDCs.[74] Four parties are involved in processing a payment: the payer, the payee, entities that carry out the payment (such as central banks, commercial banks, money service providers, and other authorized entities), and law enforcement agencies. The simplified[75] norm or activity of payment is that the payer initiates the process by asking relevant entities to send money (CBDCs) to the payee. The entities verify the payee (or the CBDC, depending on the design) and record debits and credits of the payer's and payee's accounts (I am not considering offline token-based systems here). Law enforcement agencies, as gatekeepers, make sure the payments comply with the law.

Privacy is one dimension of CBDC payments. It refers to the degree to which CBDC data such as identity and transaction data are hidden from others, including the payee, participating entities, and the general public. In other words, each party is provided with a varying degree of visibility to CBDC data. When one states that one protects privacy in the context of making payments using CBDCs, one is claiming to guard against certain disruptions to this practice. The disruptions could be irrelevant parties obtaining access to CBDC data, making use of the identity and transaction information without permission, disruption of reputation by disclosing some of the information, breach of confidentiality, surveillance, and so on.

[74] Central banks are primarily focusing on designing CBDCs for payment. In the future, CBDCs can be used for other purposes such as trade financing and double check with Bank of Singapore.

[75] The norm or activity I described above only shows a big picture of CBDC payment. The actual CBDC payment process is much more complicated and nuanced. Depending on the design, the detailed norms or activities could change, and the tasks of different actors could also change, which could slightly lead to different contextual situations at the micro level. But the big picture of CBDC payment remains the same as described above. I will describe design options and respective norms or activities in detail in Section B.

What aspects of the CBDC payment should be private is a normative analysis. We can argue that identity information and transaction information, for the purpose of CBDC payments, are private matters. It is no secret that retail payments leave behind a data trail that can be used to construct a detailed picture of an individual's personal life, including travel, financial circumstances, and much more.[76] Similarly, CBDCs as a new form of retail payment method share the same characteristics. Account data, identity data, and transaction data, separately or collectively, can be used to construct a detailed picture of an individual's personal life. Revealing these data would directly pose a threat to one's safety, dignity, autonomy, and liberty.

The degree of privacy also varies and relies on a normative assessment. We can consider our identity and transaction information private, but we do not consider them private in the same way. A CBDC system may be more private with respect to one entity (e.g., merchant) and less so for another (e.g., government).[77] The degree of privacy here depends on whether society should trust one entity over another or whether one entity adopts better mechanisms to protect users' data than other entities do. Central banks could engineer a CBDC system with higher levels of privacy than commercial products can offer—but with trade-offs.[78] Central banks should conduct cost and benefit analysis or use other mechanisms to decide to what extent CBDC data should be hidden from which entity.

When conducting normative analysis, it is necessary to balance various conflicting values. On the one hand, we recognize the value of keeping CBDC data private because we cherish the freedom to make payments whenever, wherever, and with whomever we desire without intrusion. On the other hand, we also acknowledge the value of social justice and national security, so disclosing CBDC data connected to money laundering, financing of terrorists, and fraud is valuable. It is up to the people in each jurisdiction, with the help of experts such as philosophers, legal scholars, sociologists, and so on, to decide what should be considered private after balancing all conflicting values.

The law is usually the result of balancing all these values. Take the Gramm-Leach-Bliley Act (GLBA) as an example,[79] the GLBA was designed to enable the creation of financial conglomerates that provide a host of different forms of financial services.[80] It authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies.[81] The GLBA recognized the social and economic value of providing broader financial services to ordinary Americans. Financial institutions sharing financial data with affiliated entities was seen as helping them target their customers to better meet their needs.[82]

[76] Geoffrey Goodell, Hazem Danny Al-Nakib & Paolo Tasca, *A Digital Currency Architecture for Privacy and Owner-Custodianship*, 13 FUTURE INTERNET 2 (2021).
[77] Sriram Darbha & Rakesh Arora, *Privacy in CBDC Technology*, BANK OF CANADA (June 2020) https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/.
[78] *Id.*
[79] In 1999, Congress passed the Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, codified at 15 U.S.C. §§ 6801-6809.
[80] Solove, *supra* note 113, at 792.
[81] *Id.*
[82] *Id.*

Meanwhile, the GLBA also acknowledges the value of protecting privacy, so Title V requires the Federal Trade Commission, along with the Federal banking agencies and other regulators, to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information.[83] After balancing these two conflicting values, the law limits the scope of privacy protection to "nonpublic personal information" that consists of "personally identifiable financial information."[84] The law also requires financial institutions to give notice to customers when they share customer information with affiliated entities.[85] If they share customer information with nonaffiliated entities, they should first provide customers with the ability to opt out of the disclosure.[86] More clauses like these show that the law seeks to balance maximizing social and economic benefits with privacy protection.

In summary, privacy should be understood contextually. In the context of CBDCs, privacy is not a separate abstract conception but a dimension of the practice of CBDC payments. Privacy is part of payment practices. Payment practices include a payee sending a payee some money (in the form of CBDC), entities processing the payment by updating the balance sheet, and law enforcement agencies investigating certain information about the payment to make sure the payment is legitimate. Since privacy is part of the payment practices, certain things or actions related to CBDC payments should be considered private. Any disruption to those things considered private would be a violation of privacy. What should be considered private is a normative argument and could vary in various jurisdictions, cultures, and times. When conducting normative analysis, it is necessary to balance the value of CBDC data privacy with other conflicting values.

III. Privacy Issues Arising from Various CBDC Designs

After conceptualizing privacy in the CBDC context, the next question to ask is what privacy problems a CBDC will create. Before proposing solutions, it is necessary to understand what problems we need to solve. The section below provides a contextual analysis of what new privacy problems (disruptions to practices) would arise under various popular CBDC designs.

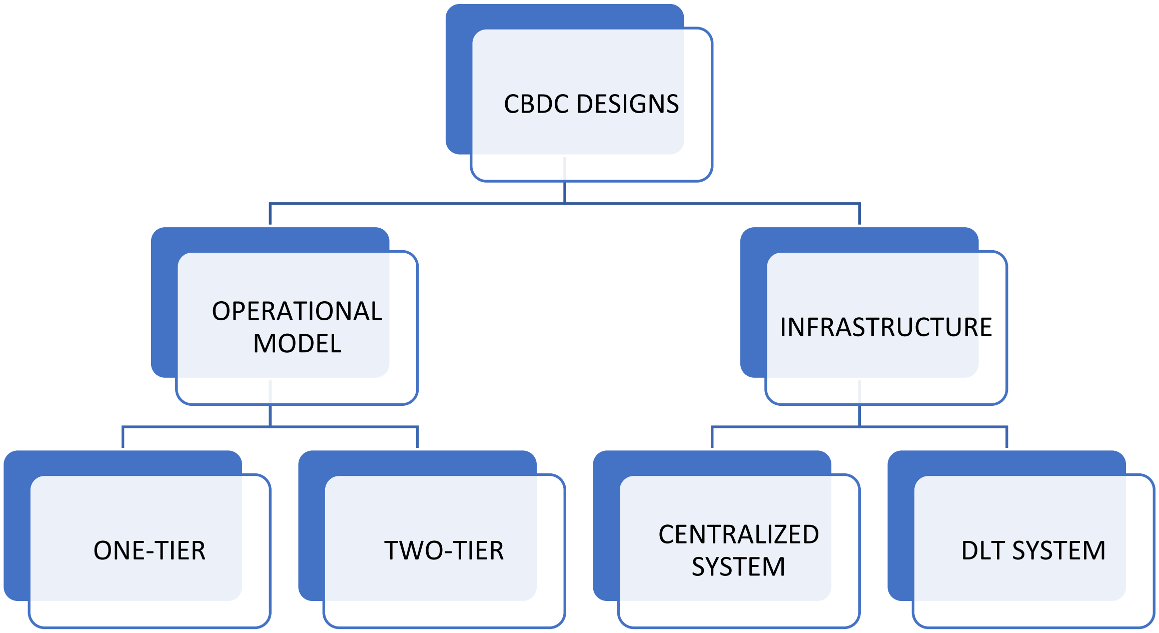
CBDCs can be designed in different ways with different characteristics and functions.[87] Different design choices will create different privacy issues (disruptions to CBDC practices). I agree with MIT and the Federal Reserve Bank of Boston's view that CBDC design choices are more granular than commonly assumed.[88] Many commonly assumed categories are still very

[83] https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act
[84] Gramm-Leach-Bliley Act, 15 U.S.C. §6809(4)
[85] Gramm-Leach-Bliley Act, 15 U.S.C. §6802(a)
[86] Gramm-Leach-Bliley Act, 15 U.S.C. §6802(b)
[87] Gabriel Soderberg, et al, *Behind the Scenes of Central Bank Digital Currency*, International Monetary Fund 12, https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174 (last visited Jun 13, 2022).
[88] *Project Hamilton Phase 1 A High Performance Payment Processing System Designed for Central Bank Digital Currencies*, Federal Reserve Bank of Boston & Massachusetts Institute of technology Digital Currency Initiative (Feb. 3, 2022) at 39.

limited; those categories are insufficient to bring to the surface the complexity of choices in access, intermediation, institutional roles, and data retention with regard to CBDC design.[89]

In this paper, I do not intend to go through all design choices (which is impossible, practically speaking) and explore their privacy implications. Instead, I investigate two structural and foundational design choices that all central banks will encounter and must decide on before they move on to other design choices. These two design choices cover the operational model and infrastructure (figure 1). The operational model deals with how CBDCs are distributed and who performs consumer-facing tasks. Two design choices are available: a one-tier model and a two-tier model. Infrastructure refers to the ways of recording transactions or updating credit and debit information. Two design choices are available: a centralized system and a distributed ledger technology (DLT) system.

FIGURE 1. CBDC DESIGN CHOICES



To understand what privacy problems would arise from these design choices, methodologically, I first studied the dataflow of each design choice. Following the dataflow, I further investigated who can get access to what data. Each design varies in who can see, store, collect, and share CBDC-related data, including but not limited to identity data and transaction data. Some data are encrypted whereas some are not. All these factors contribute to what kind of disruptions could occur in the practice of CBDC payment (i.e., privacy problems).

The operational model and infrastructure are structural and foundational because they both deal with a key issue: the trust model, which decides what roles central banks and intermediaries (i.e.,

[89] *Id. See also* Rod Garratt, et al., *Token- or Account-Based? A Digital Currency Can Be Both*, LIBERTY STREET ECONOMICS (2020), https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/ (last visited Jun 16, 2022).

commercial banks and other payment service providers in the private sector) will play. Some CBDC literature argues that the design of verification object (account-based model vs token-based model) is also a critical design choice.[90] I argue that the verification object is a very technical choice at the micro level, not a structural and foundational question like the choice of operational model and infrastructure. The section at the end will critique the need to distinguish between account-based and token-based systems and further elaborate why this design element is not considered a foundational and structural choice for the central bank to decide at the outset.

A. Operational Model

The operational model determines how CBDCs are distributed and who performs end user facing tasks. A one-tier operational model (figure 2), also called a direct distribution model, means the central bank directly issues CBDC to end users, such as individuals, corporations, and merchants. The central bank will have to communicate with all end users and provide banking services, such as opening accounts, administering payments for users, conducting know-your-customer checks, monitoring for money laundering, and clearing and settling transactions.

A two-tier operational model (figure 3) means the central bank first issues CBDC to intermediaries, including commercial banks, cashless payment services providers, and other authorized (financial) institutions, and the intermediaries then issue CBDC to end users. In other words, the obligation to provide CBDC on demand would fall to intermediaries rather than the central bank.[91] To guarantee that in all cases the customer's CBDC would be honored, the intermediary would have to hold an equal amount of CBDC at the central bank.[92] Additionally, the central bank also delegates most of the consumer-facing work and banking services to intermediaries. End users could pay with a CBDC just as today, with a debit card, online banking tool, or smartphone-based app, all operated by banks or other authorized intermediaries.[93] Depending on the design, the central bank can retain a copy of all retail CBDC holdings or wholesale CBDC holdings of the intermediaries.

FIGURE 2. ONE-TIER OPERATIONAL MODEL

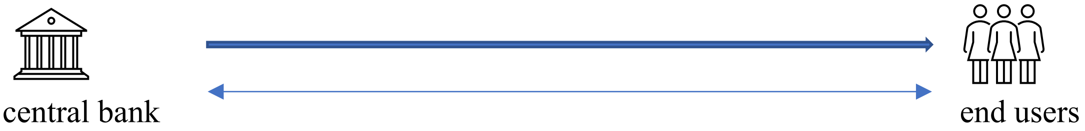


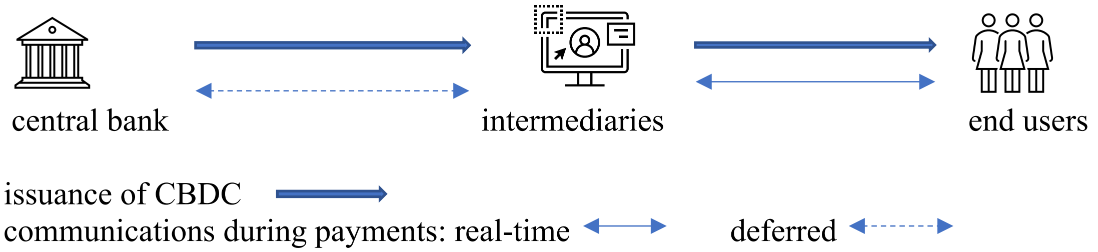
FIGURE 3. TWO-TIER OPERATIONAL MODEL

[90] *See* Raphael Auer & Rainer Boehme, *The Technology of Retail Central Bank Digital Currency* (2020), 87, 93. *See also The Digital Dollar Project: Exploring a US CBDC*, *supra* note 123, at 17.

[91] Gregory Baer, *Central Bank Digital Currencies: Costs, Benefits and Major Implications for the U.S. Economic System*, BANK POLICY INSTITUTE 22, 5, (Apr. 7, 2021).

[92] *Id.*

[93] Fabio Panetta, Member of the Exec. Bd. "Evolution or Revolution? The Impact of the Digital Euro on the Financial System" *Bruegel Online Seminar* (Feb. 10, 2021) https://www.bis.org/review/r210211d.pdf; Agustín Carstens, Gen. Mgr., Bank for Int'l Settlements "Digital Currencies and the Future of the Monetary System" Bank for International Settlements (Jan. 27, 2021) https://www.bis.org/speeches/sp210127.pdf.



Under the one-tier operational model, data flows between the central bank and end users. The central bank needs to manage the accounts of all end users and thus collects end users' relevant information such as name, address, phone number, profession, the amount of CBDC in the account, balance, etc. (note: by default, I am using an account-based model here). When the central banks handle payments in real time, the central bank will have a copy of transaction details, including transaction parties, the transaction amount, and when and where the transaction happened. Various departments within the central bank perform different services, such as account registration and management, KYC/AML, transaction risk assessment, clearing, settlement, and many more. Therefore, data also flows among various departments within the central bank.

Data flow under the two-tier operational model is more complex. Data mainly flows between intermediaries and end users because intermediaries handle all communication with end users, including collecting and managing end users' account information and clearing transactions. Intermediaries also clear transactions in real time and, therefore, will have a copy of transaction details. In terms of the record at the central bank, depending on the design, the central bank can have a copy of retail holdings or the wholesale balance sheet. If the former, then the central bank will also have at least the account and balance information of the end users; if the latter, the central bank will not have such information of an end user.

The biggest problem with the one-tier operational model, from a privacy point of view, is that the central bank by default will collect and store an enormous amount of end user data, which could enable mass surveillance, leading to abuse. Central banks are a government agency in many jurisdictions, for example, China's central bank (the People's Bank of China). A government agency having enormous financial information about users might have different implications in different countries. In some authoritarian countries, without checks and balances, a government agency, i.e., the central bank, can easily obtain access to its citizens' financial data stored at the central bank and share this information with other government agencies. Citizens are vulnerable to such intrusion to their financial data. Even in some democratic countries that have checks and balances, it is still unclear how central banks would protect users' privacy under this new system in which central banks would have unprecedented access to financial data about its citizens that are usually stored and handled by banks and other intermediaries. Unless rigorous rules are put in place and executed properly, protection of users' privacy remains unclear.

While the one-tier operational model enables mass surveillance by the central bank, the end users having very limited control over data worsens the situation. End users have limited control over data because allowing for control has never been in the design of a CBDC. To incentivize the use of CBDCs, many central banks focus on ease of use and cheaper adoption of CBDCs. Giving end users control over data would complicate the data collection and usage process and require additional effort for data control structure, which directly contradicts the goal of ease of use and cheaper adoption. From the central banks' perspective, it is not to their advantage to give end users control over data. Instead, central banks would enjoy full access and control over enormous quantities of data for both legitimate and illegitimate purposes, such as helping to implement monetary policy, combating money laundering and financing of terrorism, or even increasing surveillance ability. Moreover, from end users' perspective, even if the central bank allows end users to control their own data, many end users lack the expertise to understand very complex data structure, not to mention data control. Therefore, end users would be unable to control their data, making mass surveillance even more possible and widespread.

The problem with a two-tier operational model, again from a privacy point of view, is that more intermediaries will collect, store, and have access to end users' CBDC data, which weakens end users' ability to conceal certain matters from others and shield themselves from unwanted access by others. Some might argue that the two-tier model is similar to the existing payment systems where banks and other financial institutions and technology providers collect end users' data as long as end users use their products or services. Having one more party (the central bank) collect, store, and access data would not significantly worsen the privacy situation. This argument is partially right, especially when the central bank delegates all the commutations with end users to intermediaries and the central bank only holds a wholesale balance sheet.

This argument is inaccurate when the central bank has a copy of retail holdings. Having a copy of retail holdings means the central bank would have a complete set of data regarding end users' detailed account and transaction information across all intermediaries, whereas an intermediary would only have data when end users use its products or services or communicate with this intermediary directly or indirectly. In other words, it is impossible for an intermediary to have a complete set of CBDC-related financial data about an end user. The central bank will have enormous access to the data stored at the central bank, which again, brings back to the problem arose under the single tier model—mass surveillance and potential data abuse.

B. Infrastructure

Infrastructure refers to the ways of recording and sharing data. A central bank has two options, a centralized system (figure 4) and a DLT system (figure 5), for recording transactions and updating credit and debit information. It is important to note that a DLT is not decentralized. A decentralized system means there is no centralized authority that makes decisions; all parties share equal rights to make decisions. In the CBDC system, no matter what technology is used, it is always centralized. The central bank is the central authority that makes decisions on the amount of CBDC to issue, who can participate in the issuance process, who can update the ledger, who can see the identity and transaction information, and much more. It is distributed only because the central bank authorizes other entities to update the ledger. The rights to update the ledger are distributed among a few authorized entities. The authorization still comes from a centralized authority—the central bank. The central bank has the right to revoke its authorization or change the authorized entities.

FIGURE 4. CENTRALIZED SYSTEM

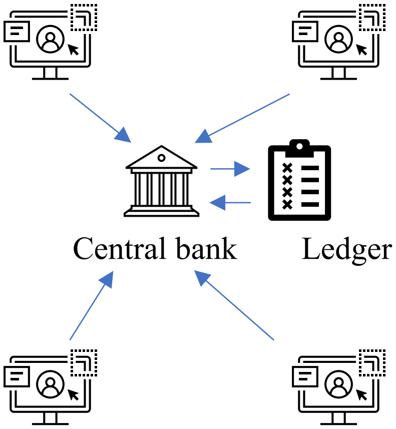
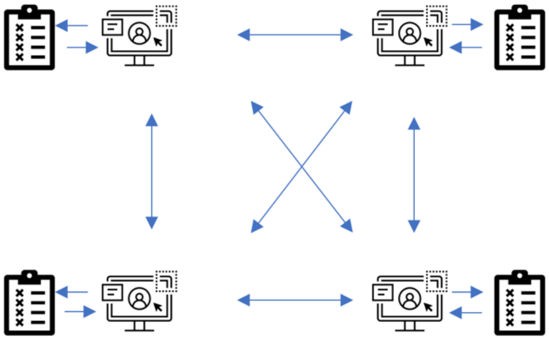


FIGURE 5. DLT SYSTEM



A centralized system is a collection of transactions managed by a single player, which is the central bank in this case. The central bank controls the system and its contents, that is, which transactions get posted to a central ledger. A ledger is a digital file containing accounts to which debits and credits are posted, just like a physical account book in which a company writes down the amounts of money it sends and receives. With a centralized system, other intermediaries such as banks cannot update the central ledger without going through the central bank, even if intermediaries handle retail transactions and directly communicate with end users. The central bank acts as a trusted party for managing the central ledger. To be clear, every intermediary can hold its own ledger that records debits and credits of its users and is different from ledgers held by other intermediaries. One intermediary has no access to a ledger held by other intermediaries. In other words, ledgers held by all intermediaries are not synchronized.

DLT refers to the processes and technologies that enable participants[94] in a network to securely propose, validate, and record state changes to a synchronized ledger that is distributed across the

[94] Technically speaking, participants refer to nodes. I user participants instead of nodes to avoid technical terms unfamiliar to readers. In computer science, a node is the basic computing unit of a network that updates the ledger. In the context of this paper, a participant refers to any authorized entity such as commercial banks and cashless payment systems (e.g., Apple Pay or Google Pay) in the CBDC network.

network's participants.[95] At its core, DLT is a decentralized way of recording and sharing data.[96] The distributed ledger is an agreed-upon record of digital data spread across multiple entities.[97] DLT uses a consensus mechanism[98] to ensure the accuracy of the data on the ledger. In the context of payment, clearing, and settlement, DLT enables multiple entities, through the consensus mechanism, to process transactions without necessarily relying on a central authority to maintain a single "golden copy" of the ledger. In the context of CBDC transactions, commercial banks, cashless payment systems, and other authorized entities can post transactions and add credits and debits to the CBDC ledger without relying on the central bank to maintain a single copy of the ledger.

There are two types of DLT: permissionless and permissioned.[99] Permissionless DLTs are open to every participant in the network.[100] Any participant can add an entry to the ledger through the consensus mechanism.[101] In contrast, permissioned DLTs are only open to a limited number of participants.[102] Only permitted and verified participants can control record keeping.[103] Therefore, permissioned DLTs share a limited consensus process.[104] Most likely, central banks would consider only permissioned DLTs, in which a network of preselected participants have power over recordkeeping.[105] It would be easier and faster for these preselected participants to reach consensus on the state of the ledger.[106] While it is technically possible to use permissionless DLTs, the economic cost is too high for a large group of participants to reach consensus.[107] In

[95] David Mills, et al., *Distributed Ledger Technology in Payment, Clearing and Settlement*, FINANCE AND ECONOMICS DISCUSSION SERIES DIVISIONS OF RESEARCH & STATISTICS AND MONETARY AFFAIRS: FEDERAL RESERVE BOARD, 29, 2, (Dec. 2016).
[96] Michael S. Barr et al., *Should Central Banks Use Distributed Ledger Technology and Digital Currencies to Advance Financial Inclusion?*, SSRN JOURNAL, 3 (2021), https://www.ssrn.com/abstract=3849051 (last visited Jul 30, 2021); *See also Distributed Ledger Technology (DLT) and Blockchain* (FinTech Note No. 1) World Bank Group, (2017) http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
[97] Barr et al., *supra* note 170; *see also* César A. Del Río *Use of Distributed Ledger Technology by Central Banks: A Review* (*Uso de la tecnología de contabilidad distribuida por los bancos centrales: Una revisión*), ENFOQUE UTE, 8(5), 1–13 (2017) http://scielo.senescyt.gob.ec/pdf/enfoqueute/v8n5/1390-6542-enfoqueute-8-05-00001.pdf
[98] A consensus mechanism is a method of authenticating and validating a value or transaction on the blockchain or a distributed ledger without the need to trust or rely on a centralized authority. Sigrid Seibold & George Samman, *Consensus: Immutable agreement for the Internet of value*, KPMG (2016) https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf. "Consensus Mechanism" has been described in a variety of ways. *See, e.g.,* Robby Houben & Alexander Snyders, Policy Department for Economic, Scientific and Quality of Life Policies, *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion* (July 2018) https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.
[99] Barr et al., *supra* note 170.
[100] *Id.*
[101] *Id.*; *see also* Leon Perlman, *Distributed Ledger Technologies and Financial Inclusion*, ITU-T Focus Group Digital Financial Services (Mar. 2017) https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf.
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] Auer and Boehme, *supra* note 1644, at 8.
[106] Mills, *supra* note 59, at 169.
[107] Auer and Boehme, *supra* note 1644, at 8.

addition, a permissionless DLT will raise questions related to governance and information security issues because a larger number of distributed participants are unknown to each other.[108]

In the centralized system, if it is a one-tier model, data flows mainly from end users to the central bank because end users need to rely on the central bank to update the balances to the ledger. Data related to the payer's identity and transaction amount will be sent to the central bank. To receive the money, the payee also needs to share its identity data with the central bank in order to have an account at the central bank. After the central bank verifies data from the payer and payee, the central bank will update the ledger with the correct amount. If it is a two-tier model where intermediaries handle retail payments, identity and transaction data first flows from end users to intermediaries, and intermediaries verify such data and update the ledger they hold but cannot update the single "golden copy" that the central bank holds. Depending on the design, if the central bank wants to hold a wholesale balance sheet of all intermediaries, very limited data regarding end users will be sent from intermediaries to the central bank. If the central bank wants to hold a retail copy that records every single transaction handled by every single intermediary, detailed data then again flows from intermediaries to the central bank.

The biggest privacy problem of the centralized system under the one-tier model is, again, that the central bank holds enormous quantities of end user data, which enables widespread surveillance. The centralized system could also make the central bank (or the government, in some cases) more enticing targets for hackers, leading to data leakage and the loss of privacy. The same issue applies to the two-tier model when the central bank decides to hold a copy of all retail transactions of all intermediaries. If the central bank decides to keep only a copy of the wholesale balance sheet under the two-tier model, then the privacy issue is limited to a smaller scale, and end users only need to worry about data leakage or abuse at the intermediary with which they hold an account or carry out transactions.

In a DLT (permissioned DLT in this case) system, data flows among participants in the network (intermediaries in the context of CBDCs). Assuming entity A wants to transfer $100 to entity B, the process involves three broad steps. First, to initiate a payment, entity A uses cryptographic tools to digitally sign a proposed update to the shared ledger that would transfer $100 from its account on the ledger to entity B's account. Data on this request flows from entity A to the network. Second, upon receiving the transfer request, other participants in the network need to authenticate entity A's identity (public key) and validate that entity A has sufficient funds to make the payment. Data on identity and funds flows from entity A to the network, and all network participants can see the data in order to take part in the consensus process. Third, after the consensus process where all participants agree on the transfer of funds, the ledger is updated and $100 is added to entity B's account. The data on the latest balance on the ledger is also shared by all participants.

The privacy issue in a DLT system is that a DLT system allows for broader access to information, which potentially compromises the integrity of data. Multiple intermediaries such as commercial banks and other payment services providers, as long as they are authorized to update the ledger, will have access to a complete set of CBDC data, including but not limited to transacting parties (shown in addresses/public keys), transaction amount, and transaction time.

[108] Mills, *supra* note 59 at 169.

Any intermediary in the network has a copy of the synchronized ledger and can disclose any information to others unless rigorous rules are in place. An attack on one intermediary is sufficient to get a complete set of CBDC data. Therefore, having more participants (intermediaries) in the network makes privacy protection harder.

Some might argue that, in the DLT system, participants in the network will not directly see the names of payers and payees but only addresses consisting of random numbers and letters. The pseudonymous nature of the address does not reveal the real identity of the payer or payee, which thus protects privacy. This is arguably true when there is only one transaction. Even if many parties can see the address and this transaction, it is probably difficult to cause real privacy harm to the transacting parties. However, when transaction volumes accumulate, it will be easier to identify the person behind the address, especially when the address is associated with some distinctive transaction activities (such as sending a certain amount at the same time for a period of time from the same address). When all participants in the network can see and analyze those data, privacy remains a huge problem, regardless of pseudonyms.

C. Verification Object?

Some literature argues that, once the operational model and infrastructure have been chosen, the question arises of how and to whom one should give access.[109] The verification object is about who should provide what information to authenticate themselves as the owner of the CBDC in order to gain access to the system.[110] Figures 6 and 7 below present two options: an account-based model and a token-based model. The key distinction lies in what to verify in order to process a payment: an account-based system requires verification of the identity of the payer, while a token-based system requires verification of the validity of the object used to pay.[111]

FIGURE 6. ACCOUNT-BASED MODEL[112]

[109] Auer & Boehme, *supra* note 164, at 9; see also *The Digital Dollar Project, Exploring a US CBDC*, *supra* note 123, at 17.

[110] Baer, *supra* note 1655, at 6.

[111] Charles M. Kahn & William Roberds, *Why pay? An introduction to payments economics*, 18 JOURNAL OF FINANCIAL INTERMEDIATION 1–23 (2009); The distinction between account-based and token-based model has also been discussed in the following reports and papers: Benoît Cœuré & Jacqueline Loh, *Central bank digital currencies*, BANK FOR INTERNATIONAL SETTLEMENTS 4 https://www.bis.org/cpmi/publ/d174.pdf; Charles M. Kahn, et al., *Should the Central Bank Issue E-money?* (Bank of Canada, Working Paper No. 58, 2018) https://www.bankofcanada.ca/wp-content/uploads/2018/12/swp2018-58.pdf; Auer & Boehme, *supra* note 164; *see also* Rod Garratt, et al., *supra* note 163.

[112] *The Digital Dollar Project: Exploring a US CBDC*, *supra* note 123, at 17.

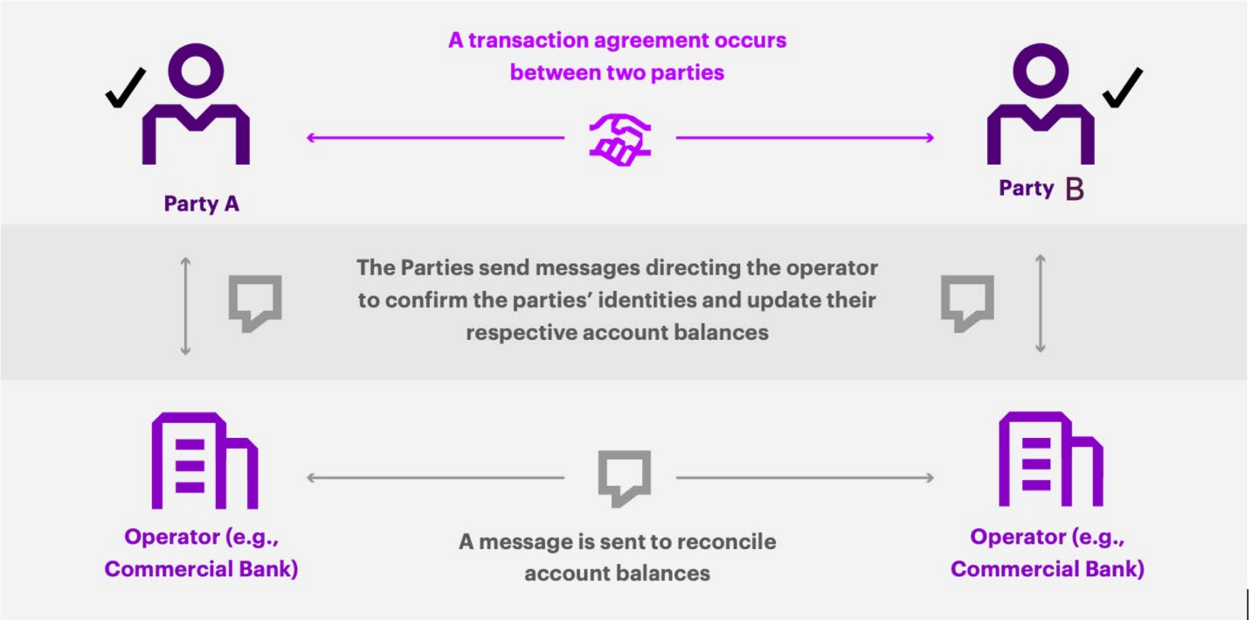
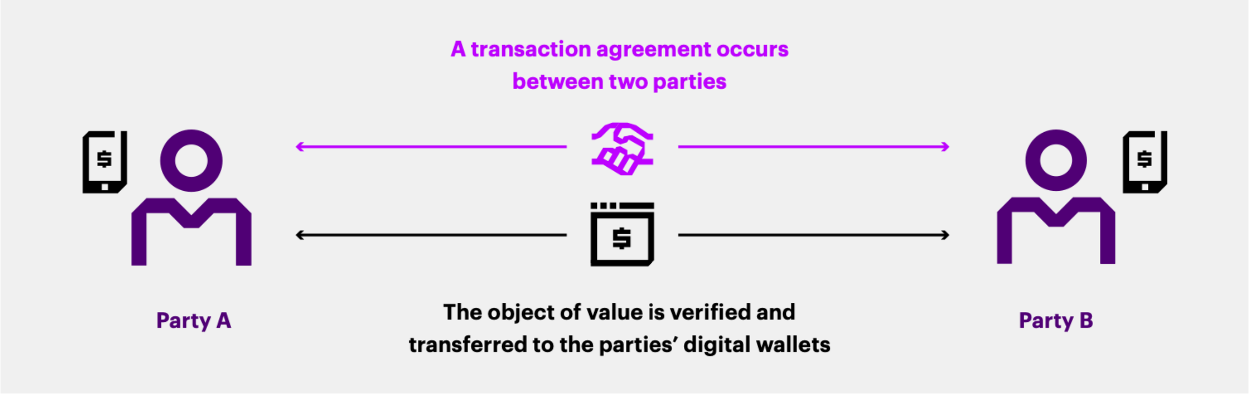

A transaction agreement occurs between two parties
Party A
Party B
The Parties send messages directing the operator to confirm the parties' identities and update their respective account balances
Operator (e.g., Commercial Bank)
A message is sent to reconcile account balances
Operator (e.g., Commercial Bank)

FIGURE 7. TOKEN-BASED MODEL[113]


A transaction agreement occurs between two parties
Party A
The object of value is verified and transferred to the parties' digital wallets
Party B

The account-based model fundamentally depends on the ability to verify the account holder's identity.[114] It follows the conventional account model and ties ownership to an identity.[115] Transactions are authorized via identification. Under this model, individuals hold their balances as accounts with the central bank and transactions are recorded as new entries on a centralized ledger.[116] The account owner can request a transfer of funds to another account owner.[117] The

[113] *Id.*
[114] Cœuré & Loh, *supra* note 185, at 34.
[115] Auer & Boehme, *supra* note 164, at 9.
[116] Barr et al., *supra* note 170, at 8.
[117] *Id.*

central bank would settle the transaction by updating its central ledger.[118] As shown in figure 6 (assuming it is a two-tier model), if Party A wants to transfer CBDC to Party B, Party A notifies the commercial bank where Party A holds an account. The bank verifies the identity of Party A and the account information and sends CBDC to its correspondent commercial bank where Party B holds an account and Party B's identity has been verified by its commercial bank.

In a token-based model, the token contains all information necessary for the recipient to verify the legitimacy of the transaction, and the recipient can verify the object transferred (i.e. the token).[119] Physical cash (i.e., banknotes) is a good example of a token-based model. As shown in figure 7, assuming Party A wants to pay Party B $100 cash, the only thing party B needs to worry about is that the $100 bill is not fake. If the bill is valid, then it can be used to make a purchase.

Similarly, in the context of CBDCs, if the token is an offline object (such as a physical card, as in the PBOC's design) that functions like traditional paper currency and can pass peer-to-peer without going through a central bank clearing system, Party B only needs to verify that this physical object is genuine and does not need to worry about the identity of Party A.

If the token is a digital currency, theoretically speaking, party B only needs to worry about whether the digital currency is genuine and whether it already been spent.[120] Party B does not need to know anything about Party A. The transaction happens between two wallets instead of two accounts. Wallets are not actually where the digital currencies are stored[121]. Instead, each wallet has a private key that corresponds to an address in the network, which, in turn, corresponds to the number of tokens held by the owner of the wallet.[122] These wallets could take the form of a website, a mobile app, or even a hardware wallet.[123]

While it is very common to make a distinction between account-based and token-based systems,[124] from a practical point of view, such a distinction is problematic and sometimes useless.[125] Many computer science professionals think the distinction is meaningless and irrelevant when it comes to cryptocurrencies and other revolutionary electronic payment methods.[126] One of the biggest issues with this distinction is that the use of the token-based and

[118] Barr et al., *supra* note 170.; *see also* Tommaso Mancini-Griffoli, et al., *Casting Light on Central Bank Digital Currencies*, INTERNATIONAL MONETARY FUND (Nov. 2018) https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-onCentral-Bank-Digital-Currencies-46233.

[119] *The Digital Dollar Project: Exploring a US CBDC*, *supra* note 123, at 17.

[120] Cœuré & Loh, *supra* note 185, at 4.

[121] Nikhil Sridhar & Patrick Horan, *Should Central Banks Offer the Public Token-Based Digital Currencies?*, DISCOURSE, https://www.discoursemagazine.com/economics/2021/06/08/should-central-banks-offer-the-public-token-based-digital-currencies/ (last visited Jun. 21, 2022).

[122] *Id.*

[123] *Id.*

[124] *See* Cœuré & Loh, *supra* note 185; Kahn, *supra* note 185; Mancini-Griffoli, et al*., supra* note 192, Auer & Boehme, *supra* note 164, Sridhar & Horan, *supra* note 195.

[125] Garratt, et al., *supra* note 163.

[126] Kahn, *supra* note 185.

account-based terminologies does not create mutually exclusive categories.[127] For example, Bitcoin and many other digital currencies can satisfy both categories.[128]

"Bitcoin fits the definition of an account-based system. The account is a Bitcoin address, and the private key is the proof of identity needed to transact from that account. Every time a Bitcoin user wants to spend Bitcoin, that user must verify their identity by using their private key. Bitcoin also fits the definition of a token-based system. When someone wants to spend a Bitcoin, the protocol verifies its validity by tracing its history. The current transaction history is used to verify the validity of the 'object' being transferred, as other token-based systems also do."[129]

Unless the CBDC is an offline physical object, a CBDC also fits the definitions of an account-based system and a token-based system. In a centralized system, a CBDC is account-based because the central bank or intermediaries, depending on whether it is a one-tier or two-tier design, need to verify the identities of the payer and payee before processing the transactions and updating the balance sheet. In a DLT system, a CBDC can be account-based because the public key is the account and the private key is the proof of identity. A CBDC arguably can also be token-based because participants in the network also need to verify the transaction history of the "object" being transferred. Therefore, at the deepest levels of computer architecture, the distinction makes no sense.[130] The distinction remains relevant probably only because it helps nonexperts to understand the revolutionary technology or product by referring to something that already exists or of which people have knowledge.[131]

That is also why I argue that the choice of the verification object is a very technical issue at the deepest levels of computer architecture rather than a structural and foundational design choice that central banks need to decide in the first place. Token-based architecture is just one feature associated with a DLT system. From a privacy point of view, the analysis of the DLT system has already covered the dataflow of the token-based feature and the scenarios of who has access to what data.

D. One Unique Scenario

In practice, most likely, central banks would consider a two-tier operational model rather than a one-tier model. Central banks would also prefer a centralized system rather than a DLT system.

A two-tier model outperforms a one-tier model for a few reasons: overwhelming consumer-facing tasks, innovation goals, and disintermediation concerns. First, central banks have already been tasked with so many responsibilities, additional consumer-facing responsibilities in the one-tier system would overwhelm central banks. Although central banks' responsibilities range widely in different jurisdictions, their duties usually fall into three areas. First, central banks' top priority is to control and manipulate the national money supply: issuing currency and setting

[127] Garratt, et al., *supra* note 163; *see also Bitcoin is an Account, Not a Token*, MONEYNESS (Aug. 18, 2020) http://jpkoning.blogspot.com/2020/08/bitcoin-is-account-not-token.html

[128] *Token- or Account-Based?*, *supra* note 163.

[129] *Id.* (arguing that Bitcoin is not a token).

[130] Kahn, *supra* note 185.

[131] *Id.*

interest rates on loans and bonds. In this way, they manage monetary policy to guide the country's economy and achieve economic goals, such as full employment. Second, they regulate member banks through capital requirements, reserve requirements, and deposit guarantees, among other tools. They also provide loans and services for a nation's banks and its government and mange foreign exchange reserves. Third, a central bank also acts as an emergency lender to distressed commercial banks and other institutions, and sometimes even the government. For instance, by purchasing government debt obligations, the central bank provides a politically attractive alternative to taxation when a government needs to increase revenue.

Thus, issuing currency is just one of many responsibilities central banks have to deal with. Issuing currency to control money supply is a very macro decision that central banks are well-equipped to make. If central banks had to handle many micro consumer-facing tasks that have long been the private sector's job, such as creating and managing accounts, handling retail transactions, and monitoring for money laundering and financing of terrorism, central banks would be overwhelmed. They may also lack the technical expertise and human resources to accomplish all these tasks.

In addition, from a broader policy perspective, the central bank taking on fewer consumer-facing responsibilities would give the private sector more room to innovate CBDC-related products and services. Finally, in a one-tier system, the CBDC is directly distributed by a central bank, which directly competes with the banking sector for deposits, causing disintermediation concerns. This would directly contradict central banks' goal of guiding the country's economy and achieving economic goals such as full employment.

Practically, central banks would adopt a centralized system over a DLT system. At the very outset, no central bank worldwide has an operational DLT-based system at this point, although two-thirds of central banks are directly experimenting with DLT protocols.[132] This is because some issues remain regarding the speed, processing cost, security, transparency and privacy, legal settlement finality, scalability, and network effects of the technology.[133] Some central banks, such as the European Central Bank and the Bank of Japan, have declared DLT not mature enough at this stage to power the world's biggest payment systems.[134] The Bank of Canada stated that, for critical financial market infrastructures such as wholesale payment systems, current versions of DLT may not provide an overall net benefit relative to current centralized systems.[135]

[132] Del Río, *supra* note 171; Garrick Hileman & Michel Rauchs, *Global Blockchain Benchmarking Study*, CAMBRIDGE CENTER FOR ALTERNATIVE FINANCE (2017) https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternativefinance/downloads/2017-09-27-ccaf-globalbchain.pdf

[133] César A. Del Río, *Use of Distributed Ledger Technology by Central Banks: A Review*, 8 ENFOQUE UTE 1 (Dec. 2017).

[134] Balazs Koranyi & Catherine Evans, *Blockchain Immature for Big Central Banks, ECB and BOJ Say*, REUTERS. (Sept. 6, 2017) https://www.reuters.com/article/usblockchain-ecb/blockchain-immature-for-big-central-banks-ecb-and-boj-sayidUSKCN1BH2DH.

[135] James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack, & Wade McMahon, *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?* (June 2017) http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.

In the context of CBDC, a few issues remain salient, and DLT might not be able to meet the needs of a large volume of transactions using CBDCs. First, the speed of transaction settlement within a DLT system is slower than that in existing centralized systems (e.g., real-time gross settlement systems) because the process for validating a transaction and reaching consensus in DLT is potentially more complex than with a central entity.[136] Second, DLT faces scalability challenges. Consensus algorithms and cryptographic verification introduce latency and limit the number of transfers that DLTs can process currently, whereas existing payment clearing and settlement systems can process hundreds of millions of transactions daily.[137] Additionally, ledgers that add transactional histories on top of one another, such as blockchains, may challenge storage capacity over time.[138] Third, it remains unclear whether the cost of a DLT system is lower than that of a centralized system. A distributed arrangement in which participants contribute to maintaining and updating a shared ledger could cause increased direct costs for contributing to the operation of the DLT.[139] The costs have been allocated to participants, and it is not clear if this is cost effective compared to a centralized system.

Therefore, at this moment, a two-tier and centralized CBDC is the most likely and most viable choice. From a privacy point of view, because of the two-tier design, intermediaries would have access to CBDC data, which therefore increases the risks of data leakage and abuse. Intermediaries would continue to see the same types of transaction data that they currently do.[140] The main difference is that some intermediaries such as banks might be forced to harvest and monetize that data in the way that some FinTech companies currently do, as they would not be earning net interest income on a CBDC in the way they do with a deposit (and associated loan).[141]

Because of a centralized system, the central bank would by default collect and store an enormous quantity of CBDC data related to the identity and transaction information of end users (individuals and businesses). Holding enormous quantities of data could potentially lead to mass surveillance and abuse, especially when the central bank opts to hold a copy of retail balance sheets.

This two-tier and centralized design could by default potentially bring about privacy violations in various forms, although it could effectively achieve other goals. The next question is whether central banks can come up with solutions to address privacy violations in this design. The section below proposes a few general principles to design a privacy preserving CBDC.

CONCLUSION

In this paper, I demystify CBDCs by comparing CBDCs with other digital currencies and explain what motivates central banks to issue a CBDC. I also adopt a pragmatic approach to

[136] Mills, *supra* note 169; *see also* Del Río, *supra* note 171, at 4; Baer, *supra* note 165, at 6.

[137] Del Río, *supra* note 171, at 8.

[138] Mills, *supra* note 169, at 36.

[139] Del Río, *supra* note 171 at 8.

[140] Baer, *supra* note 165 at 13.

[141] Baer, *supra* note 165.

understanding privacy contextually and investigate privacy problems that could occur in four structural CBDC designs.

Again, the scope of this study is still limited. Although I study four of the most foundational design options, CBDC designs are far more granular and nuanced. Many design options at the secondary levels also affect the privacy landscape. Future work can explore more design options and study their privacy implications. It is worth noting that, although critical, user privacy is not the only issue central banks must address when designing a CBDC. Central banks have other policy goals, such as improving financial inclusion, maintaining financial stability, and creating a competitive and resilient financial market. As a result, central banks may have to sacrifice user privacy to certain degrees when trying to meet other privacy goals. Moreover, the principles are neither comprehensive nor exhaustive and should serve as a starting point and reference framework. Hopefully, this paper can inspire more scholars to complete the framework by proposing more concrete principles for optional CBDC designs that meet users' privacy needs and achieve other policy goals.