Privacy Implications of Central Bank Digital Currencies

*Jiaying Jiang**

One hundred thirty-one countries, representing over 98 percent of the global gross domestic product (GDP), are currently 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, nongovernmental organizations (NGOs), think tanks, and even the general public have underscored the importance of privacy in CBDC systems. Moreover, a diverse group of economists, computer scientists, engineers, and legal scholars have embarked on crafting privacy-preserving CBDC designs.

But two fundamental questions appear to be overshadowed: (1) How is privacy defined in the context of CBDCs? and (2) What specific privacy challenges emerge from CBDCs? Prior to proposing solutions, a clear understanding of these concerns is crucial and necessary. This Article first adopts Daniel Solove's pragmatic approach and Helen Nissenbaum's theory of contextual integrity to conceptualize privacy within the CBDC context. Next, it examines the data flow inherent to four core CBDC designs. It concludes that the most significant privacy concern arises from central banks collecting

* Jiaying Jiang, Assistant Professor of Law, University of Florida Levin College of Law. I am grateful to many former colleagues at the Information Law Institute and Hauser Fellows Program at NYU Law, as well as to my current colleagues at UF Law, for their generous feedback. Special thanks to Joseph Weiler, Grainne de Burca, Katherine Strandburg, Alexandre de Streel, Francesca Episcopo, David Stein, Thomas Streinz, Aniket Kesari, Elettra Bietti, and Thomas Haley. I am also indebted to many central bank officials (whose names remain confidential) at the Federal Reserve, People's Bank of China, European Central Bank, Swiss National Bank, and Central Bank of the Bahamas. I also thank Herve Troupe (International Monetary Fund), Sonja Davidovic (Monetary Authority of Singapore), Jonas Gross (Digital Euro Association), Karl Wust (Swiss Federal Institute of Technology), Jamiel Sheikh (CBDC Think Tank), Henry Holden, Mike Alonso, Robert Oleschak (Bank for International Settlements), and participants at the 2022 Law and Society Annual Meeting for their generous time and valuable insights. I also greatly appreciate my research assistants, Aslesha Parchure and Hanley Gibbons, and editors at Seton Hall Law Review for their excellent work and edits on this project.

extensive end-user data. Such data aggregation raises alarms of mass surveillance, elevates cybersecurity risks, and poses potential data misuse or abuse by other government entities, especially in the absence of governing rules. The role of intermediaries also raises privacy concerns by creating additional data repositories, which increases risks of data misuse and cybersecurity attacks. This Article also argues that, for most central banks in democratic regimes, mass surveillance is not the objective when contemplating CBDCs. Mass surveillance concerns often arise from the general public's misunderstanding of the role of central banks and the ways central banks utilize data. For these central banks, detailed personal data (e.g., who purchases what, when, and where) holds limited relevance to their mandate. Instead, they rely on aggregate data, which do not need to be personally identifiable, to gain insights into the economy. In the end, this Article proposes three legal and technical principles as a guiding framework for designing a CBDC that prioritizes privacy protection.

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, [which] 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 means of payment that anyone could use in the euro area."[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 Article addresses only retail CBDCs because retail CBDCs directly involve individuals and raise the research questions of this Article.

---

[1] *Central Bank Digital Currency (CBDC)*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., https://www.federalreserve.gov/central-bank-digital-currency.htm (Apr. 20, 2023).

[2] TOMMASO MANCINI-GRIFFOLI ET AL., CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY 7 (2018), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233.

[3] BANK OF CAN. ET AL., CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES 3 (2020) (citation omitted), https://www.bis.org/publ/othp33.pdf.

[4] *Id.*

[5] *Digital Euro*, EUR. CENT. BANK, https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (last visited Sept. 20, 2023).

[6] Codruta Boar & Andreas Wehrli, *Ready, Steady, Go?—Results of the Third BIS Survey on Central Bank Digital Currency* 4 (Bank for Int'l Settlement, Working Paper No. 114, 2021), https://www.bis.org/publ/bppdf/bispap114.pdf.

[7] *Id.*

The Atlantic Council tracks the current state of CBDC development across the globe. One hundred thirty-one countries, representing over 98 percent of global gross domestic product (GDP), are exploring a CBDC.[8] Of the one hundred thirty-one countries tracked by the Atlantic Council, as of September 20, 2023, eleven countries launched CBDCs, twenty-one countries entered into the pilot stage, thirty-two countries are in the development stage, and forty-five countries remain in the research stage.[9] The Bahamas launched its Sand Dollar in October 2020, making it the first country to launch a CBDC.[10] The Eastern Caribbean Central Bank launched DCash in March 2021 in four member states and later expanded to three more.[11] Nigeria, Jamaica, and Anguilla feature a live retail CBDC.[12]

In addition, seventy-two central banks communicated publicly in positive tones about their CBDC work.[13] China's central bank is at a very advanced stage of experimenting with its CBDC, and it has run pilot programs in several cities.[14] The European Central Bank issued a report on a digital euro that examines the issuance of a CBDC "from the perspective of the Eurosystem."[15] The Federal Reserve of the United States still debates whether the United States needs a CBDC and fosters a broad and transparent public dialogue about the potential benefits and risks of a US CBDC.[16] The Federal Reserve Bank of Boston and Massachusetts Institute of Technology (MIT) tested the

---

[8] Ananya Kumar et al., *Central Bank Digital Currency Tracker*, ATL. COUNCIL, https://www.atlanticcouncil.org/cbdctracker (last visited Sept. 20, 2023).

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] Bank for International Settlements (@BIS_org), TWITTER (July 6, 2022, 7:10 AM), https://twitter.com/BIS_org/status/1544639801407709184?lang=en.

[14] PEOPLE'S BANK OF CHINA, PROGRESS OF RESEARCH AND DEVELOPMENT OF E-CNY IN CHINA 13 (2021), http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf; *see also* Joasia E. Popowicz, *China Expands E-yuan Pilot*, CENT. BANKING (Apr. 4, 2022), https://www.centralbanking.com/fintech/cbdc/7945516/china-expands-e-yuan-pilot.

[15] EUR. CENT. BANK, REPORT ON A DIGITAL EURO 3 (2020), https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

[16] BD. OF GOVERNORS OF THE FED. RSRV. SYS., MONEY AND PAYMENTS: THE U.S. DOLLAR IN THE AGE OF DIGITAL TRANSFORMATION 1 (2022) [hereinafter MONEY AND PAYMENTS], https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.

technology, publishing a report called Project Hamilton.[17] In March 2022, the White House published an executive order on digital assets and directed the Office of Science and Technology to study the technical possibilities of a US CBDC.[18] The Biden administration also urgently encouraged the Federal Reserve to continue its research and development efforts exploring the potential design and deployment options of a US CBDC.[19]

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 these banks must consider and address. Major central banks already addressed the importance of privacy. The European Central Bank conducted a public consultation on a digital euro.[20] Both citizens and professionals participating in the consultation considered privacy the most important feature of a digital euro.[21] The Federal Reserve emphasized that one key policy consideration when examining the pros and cons of a potential US CBDC centers on how to preserve the privacy of citizens and maintain the ability to combat illicit finance.[22] China's central bank, the People's Bank of China (PBOC), adopted strict compliance with regulations on data and privacy protection as a key principle of the institutional design of its CBDC system. In fact, the PBOC already moved forward with the design of "managed anonymity" to protect privacy and user information in its CBDC pilot program.[23] The Bank of Canada "outline[d] what is technologically feasible for

---

[17] *Project Hamilton—Building a Hypothetical Central Bank Digital Currency, Digit. Currency Initiative*, DIGIT. CURRENCY INITIATIVE, https://dci.mit.edu/project-hamilton-building-a-hypothetical-cbdc (last visited Sept. 20, 2023).

[18] OFF. OF SCI. & TECH. POL'Y, TECHNICAL EVALUATION FOR A U.S. CENTRAL BANK DIGITAL CURRENCY SYSTEM 5 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf.

[19] Exec. Order No. 14,067, 87 Fed. Reg. 14143, 14145 (Mar. 9, 2022).

[20] EUR. CENT. 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.

[21] *Id.* at 10–11. ("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.").

[22] MONEY AND PAYMENTS, *supra* note 16, at 2.

[23] PEOPLE'S BANK OF CHINA, *supra* note 14, at 5–6.

privacy in a [CBDC]" and suggested a design approach for CBDC privacy.[24]

Governments, nongovernmental organizations (NGOs), and think tanks 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.[25] 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 U.S CBDC.[26] The World Economic Forum studied privacy architecture examples in use today and particularly addressed the role of digital identity in privacy for CBDCs.[27] It suggested that central banks should balance privacy and financial crime management in a CBDC-world.[28] Scholars at the Bank for International Settlements repeatedly directed society's attention to the importance of privacy and the need to "strik[e] this balance between public privacy . . . and reduc[e] illegal activity."[29] Neha Narula, director of MIT Media Lab, said, "There [is] still a policy discussion happening around privacy, around how much data should be stored at

---

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

[25] Exec. Order No. 14,067, 87 Fed. Reg. 14143, 14145 (Mar. 9, 2022).

[26] THE DIGIT. DOLLAR PROJECT, PRIVACY PRINCIPLES FOR A DIGITAL DOLLAR 1–2 (2021), https://digitaldollarproject.org/wp-content/uploads/2021/10/DDP-Privacy-Principles-10.25.21_Final.pdf ("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.").

[27] WORLD ECON. F., PRIVACY AND CONFIDENTIALITY OPTIONS FOR CENTRAL BANK DIGITAL CURRENCY 17 (2021), https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf.

[28] *Id.*

[29] *See* BANK OF CAN. ET AL., *supra* note 3, at 6; *see also* Raphael Auer & Rainer Böhme, *The Technology of Retail Central Bank Digital Currency*, *in* BIS QUARTERLY REVIEW: INTERNATIONAL BANKING AND FINANCIAL MARKET DEVELOPMENTS 86 (2020), https://www.bis.org/publ/qtrpdf/r_qt2003.pdf ("[T]here is . . . [a] trade-off between privacy and ease of access on the one hand and ease of law enforcement on the other. The associated design choice . . . is whether access to the CBDC . . . [uses] account-based technology[] or . . . technology based on so-called digital tokens.").

the central bank, [and] how much should be stored in intermediaries[.]"[30]

Some economists, computer scientists, engineers, and legal scholars already moved forward to design a CBDC with privacy protection. For instance, Sarah Allen et al. discussed from whom a CBDC should "protect sensitive identity and/or transaction data[.]"[31] Jonas Gross et al. argued that a CBDC system should provide "at least[] the same privacy-preserving features as cash" in order "[t]o secure access to a fully private, regulatorily compliant form of money[.]"[32] They proposed a software-based CBDC that imposes limits on anonymous payments to support full privacy while addressing constraints related to anti-money laundering (AML) and countering the financing of terrorism (CFT), concluding that privacy and regulatory compliance can be provided by design.[33] More specifically, they proposed using zero-knowledge proof (ZKP) to enable users to reveal their payment history to provide evidence for integrity and completeness without revealing personal or identifiable information.[34] Nadia Pocher et al. proposed implementing privacy-enhancing technologies (PETs) to protect individual privacy by safeguarding data.[35]

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. But, 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?

---

[30] David Uberti, *Surveillance Risks Shape How Central Banks Test Digital Currencies*, WALL ST. J. (Mar. 22, 2022, 5:30 AM), https://www.wsj.com/articles/surveillance-risks-shape-how-central-banks-test-digital-currencies-11647941400.

[31] Sarah Allen et al., *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations* 44 (Nat'l Bureau of Econ. Rsch., Working Paper No. 27634, 2020), https://www.nber.org/system/files/working_papers/w27634/w27634.pdf.

[32] Jonas Gross et al., Designing a Central Bank Digital Currency with Support for Cash-Like Privacy 2 (Jan. 14, 2022) (unpublished manuscript) (on file at SSRN), http://ssrn.com/abstract=3891121.

[33] *Id.* at 8, 33.

[34] *Id.* at 33.

[35] Nadia Pocher & Andreas Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*, 19 IEEE TRANSACTIONS ON NETWORK & SERV. MGMT. 1776, 1776, 1782–1783 (2022).

This Article address these two critical issues. This Article adopts Daniel Solove's pragmatic approach and Helen Nissenbaum's contextual integrity theory to conceptualize 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 kind of information is being shared? What are the transmission principles? The next step explores 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.

This Article argues, 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 payor 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. So the payor, payee, entities processing the payment, and law enforcement agencies are the main actors in this context. Information being shared includes identity data, transaction data, bank affiliation, etc.

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 violates 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 possibly arise from various design choices, this Article first studies the dataflow of four structural and foundational design choices. Following the dataflow, it investigates 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 misuse and abuse of CBDC data by central banks, intermediaries, and cybercriminals.

Finally, this Article provides a few principles as a reference framework for designing a privacy-preserving CBDC for each jurisdiction to consider when designing a CBDC to meet its respective privacy needs. Central banks can view this framework as a starting

point to identify a range of privacy needs that are of interest to all stakeholders. The framework begins with an explicit recognition of the need for privacy protection in the CBDC system in central bank laws or regulations. Next, this Article presents privacy by design (PbD) as a key principle that each jurisdiction can follow. In the context of CBDCs, PbD first requires a clear design of the roles of central banks and intermediaries, which can directly affect the privacy landscape in the CBDC system. Maneuvering their roles in the design stage helps to anticipate and prevent privacy-invasive events. PbD also requires a robust technological design to embed privacy into the architecture of the CBDC system. Many privacy-preserving technologies are available to ensure privacy protection at the foundational level.[36] Finally, the CBDC system should follow a principle of user-centric design because individual users have the greatest vested interest in the management of their own personal data.

This Article makes four contributions at the theoretical and practical levels. First, at the theoretical level, this Article fills a gap in explaining privacy in the context of CBDCs. Most existing CBDC literature focuses on the differences between CBDCs and other forms of money (e.g., cryptocurrencies and commercial bank electronic money (e-money));[37] the relationship between central banks and other entities, especially commercial banks;[38] the ability of CBDCs to improve financial inclusion;[39] and cross-border applicability of CBDCs.[40]

---

[36] *See* Gross et al., *supra* note 32, at 2.

[37] Afzal Vafoiyon et al., The Regulation and Differences Between Cryptocurrency, Stablecoin, Central bank Digital Currency, e-Money, Virtual Currency and In-Game Currency 2 (Mar. 24, 2023) (unpublished manuscript) (on file at SSRN), https://ssrn.com/abstract=4391297.

[38] Darrell Duffie, *Interoperable Payment Systems and the Role of Central Bank Digital Currencies*, *in* FAIR ADVANCES REPORT 40, 40 (2021), https://www.institutlouisbachelier.org/wp-content/uploads/2021/02/ra-fair.pdf.

[39] Michael S. Barr et al., *Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion* 1 (Univ. of Mich. Ctr. on Fin., L. & Pol'y, Working Paper No. 3, 2020), https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf; David Murakami et al., CBDCs, Financial Inclusion, and Optimal Monetary Policy 2 (May 11, 2022) (unpublished manuscript) (on file at SSRN), https://ssrn.com/abstract=4102397.

[40] *See, e.g.*, Wei Shen & Heng Wang, *Global Stablecons and China's CBDC: New Moneys with New Impacts on the Final System?*, 41 REV. BANKING & FIN. L. 255, 259 (2021), https://www.bu.edu/rbfl/files/2023/03/RBFL-Fall-2021-Article-2-Shen-and-Wang-255.pdf; Cheng-Yun Tsang & Ping-Kuei Chein, *Policy Responses to Cross-Border Central Bank Digital Currencies—Assessing the Transborder Effects of Digital Yuan*, 17 CAP. MKTS. L.J.

Although central banks, government authorities, and some scholars recognized the importance of privacy and called for privacy protection, they fail to fully explain what privacy means and what privacy problems could occur in the CBDC context;[41] 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.

Second, at the practical level, this Article educates technological specialists, legal scholars, and policymakers, as well as bridging the gap between the tech, legal, and policy world. Miscommunication and ignorance of each other's fields remains one of the biggest challenges in advancing technological innovations that benefit society. This Article educates technology specialists (e.g., engineers and computer scientists) on legal and policy considerations (e.g., AML and combating the financing of terrorism) so they can factor these issues at the design stage and design a CBDC that meets policy needs as well as regulatory requirements. This Article 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. Additionally, 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[42] and the prevalence of privately issued digital currencies, such as cryptocurrencies and stablecoins, constantly challenges central bank authority.[43] In response, central banks can carefully design and issue a CBDC that not only ensures the general public's continuous access to central bank money but also furthers other policy objectives. A primary concern and a highly demanded feature among users in the

237, 237 (2022), http://dx.doi.org/10.2139/ssrn.3891208; Chusu He et al., *Central Bank Digital Currencies and International Payments* 3 (Swift Inst., Working Paper No. 2020-002, 2022), https://swiftinstitute.org/wp-content/uploads/2023/04/SWIFTInstitute_CBDCInternationalPayments_PublishedMay2022.pdf; BANK FOR INT'L SETTLEMENTS, PROJECT MBIDGE: CONNECTING ECONOMIES THROUGH CDBC 10 (2022), https://www.bis.org/publ/othp59.pdf.

[41] *See supra* notes 20–34 and accompanying text.

[42] Stephen Williamson, *Central Bank Digital Currency: Welfare and Policy Implications*, 130 J. POL. ECON. 2829, 2830 (2022).

[43] *See* Kumar et al., *supra* note 8.

design of a CBDC is privacy.[44] Inadequate addressal of privacy issues severely undermines the possibility of achieving widespread adoption of CBDCs.

Third, this Article enables intermediaries, especially commercial banks and other payment service providers, to navigate their roles amidst the rise of financial technology (fintech) innovations. Current fintech trends, promoting trustless infrastructure and peer-to-peer transactions, pose a threat to traditional financial institutions by eliminating intermediaries. CBDCs initiated by central banks, however, offer intermediaries a chance to bolster their roles in finance and payment sectors. Considering policy implications, central banks will likely collaborate with these intermediaries rather than bypassing them in issuing CBDCs. This Article also aids intermediaries in understanding privacy requirements and CBDC design. By actively engaging in CBDC design and providing customer-facing services, intermediaries can not only strengthen their role in fintech but also enhance their relationships with central banks and consumers.

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.[45] Through this Article, the unbanked population, which numbers 1.7 billion,[46] and the even greater underbanked population

---

[44] *See supra* notes 21–23.

[45] PEOPLE'S BANK OF CHINA, *supra* note 14, at 4; ALLAN WRIGHT ET AL., CENT. BANK OF BAH., RSCH. DEP'T, FINANCIAL INCLUSION AND CENTRAL BANK DIGITAL CURRENCY IN THE BAHAMAS 11 (2022), https://www.centralbankbahamas.com/viewPDF/documents/2022-09-23-13-49-13-CBDCupdated-paper.pdf; Fabio Panetta, Exec. Bd. Member, Eur. Cent. Bank, Introductory Statement at the Committee on Economic and Monetary Affairs of the European Parliament: A Digital Euro: Widely Available and Easy to Use (Apr. 24, 2023), https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230424_1~f44c7ac164.en.html.

[46] *Financial Inclusion*, THE WORLD BANK, https://www.worldbank.org/en/topic/financialinclusion/overview (Mar. 29, 2022).

can learn that access to easier payment systems and financial services is not free and sometimes comes with high privacy costs.

This Article consists of four parts. Part I demystifies CBDCs. This part explains the differences between CBDCs and other digital currencies such as commercial bank e-money, cryptocurrencies, and stablecoins. It also explains what motivates central banks to issue a CBDC, including external pressure and internal needs. Part II conceptualizes privacy in the context of CBDCs, using Daniel Solove's pragmatic approach and Helen Nissenbaum's contextual integrity theory. 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 III 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 could occur within various design options. Part IV proposes a few legal and technical principles for designing a privacy-preserving CBDC.

I. DEMYSTIFYING CBDCS

Many people may ask, "What's new about CBDCs?" After all, most entities digitize financial services, and consumers less frequently pay with cash.[47] Consumers now use credit cards, debit cards, Venmo, Apple Pay, PayPal, and many other tools to pay for products or services, thanks to vibrant innovations in the fintech space.[48] In some niche markets, consumers can also use cryptocurrencies and stablecoins for their payments. What is the difference between this new form of money and existing money? Why do consumers want to use CBDCs for payment while so many other payment tools are available? What motivates central banks to issue a CBDC? This Part answers these inquires below.

---

[47] MONEY AND PAYMENTS, *supra* note 16, at 16.

[48] Zachary Aron & Megan Scala, *Getting Ahead of the Curve: Reviving the Relevance of the Credit Card Business*, DELOITTE INSIGHTS (Feb. 26, 2020), https://www2.deloitte.com/xe/en/insights/industry/financial-services/consumer-payment-survey.html.

A. *Understanding CBDCs*

Many kinds of money or payment tools exist in the payment market, such as commercial bank money, e-money, and cryptocurrency.[49] Commercial bank money "is the digital form of money that is most commonly used by the public [and it] is held in accounts at commercial banks."[50] E-money is a digital store of a medium of exchange on a computerized device.[51] "E-money can be held on cards, devices, or on a server [including] pre-paid cards, electronic purses, such as M-PESA in Kenya, or web-based services, such as PayPal."[52] A cryptocurrency is a form of digital or virtual currency that is not denominated in fiat currency and uses cryptography to secure transactions.[53] Popular cryptocurrencies include Bitcoin (BTC), Ethereum (ETH), and so on.[54] A stablecoin is a type of cryptocurrency that attempts to peg its market value to some external reference, such as a reserve asset like the US dollar or gold, to reduce volatility.[55]

A CBDC is different from commercial bank money. The key difference is that a CBDC is a liability of the central bank, as opposed to a commercial bank.[56] Commercial bank money involves citizens having deposits in commercial banks, which then hold reserves in the central bank; meanwhile, in a CBDC system, citizens' direct deposits could lie in the central bank itself, depending on the design.[57] For instance, when one deposits money at the Bank of America (a commercial bank), one has a claim against the Bank of America, not

---

[49] MANCINI-GRIFFOLI ET AL., *supra* note 2, at 14.

[50] MONEY AND PAYMENTS, *supra* note 16, at 5.

[51] Janine Firpo, *E-Money—Mobile Money—Mobile Banking—What's the Difference?*, WORLD BANK BLOGS: PRIV. SECTOR DEV. BLOG (Jan. 21, 2009), https://blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference.

[52] *Id.*

[53] John Kiff et al., *A Survey of Research on Retail Central Bank Digital Currency* 9 n.5 (Int'l Monetary Fund, Working Paper No. 104, 2020).

[54] *Today's Crytocurrency Prices by Market Cap*, COINMARKETCAP, https://coinmarketcap.com (last visited Sept. 21, 2023).

[55] THE FED. DEPOSIT INS. CORP. & THE OFF. OF THE COMPTROLLER OF THE CURRENCY, REPORT ON STABLECOINS 4 (2021) [hereinafter REPORT ON STABLECOINS], https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

[56] *What is a Central Bank Digital Currency?*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., https://www.federalreserve.gov/faqs/what-is-a-central-bank-digital-currency.htm (Jan. 20, 2022).

[57] *Id.*

the Federal Reserve. If one loses money, one seeks remedies from the Bank of America. The contractual relationship lies between the individual and the Bank of America.

A CBDC is also different from e-money. The European Union (EU), in its directive, defines e-money as "electronically . . . stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions."[58] Also, e-money can have hybrid issuers—"[s]ervice providers who issue e-money as an accessory activity to their core business, i.e. mobile phone companies, public transport companies, etc."[59] In contrast, a CBDC represents a claim on the central bank and the central bank is the sole issuer of its CBDC.[60] Even if a central bank can authorize other entities to distribute CBDCs, these entities are distributors only, not issuers.[61]

A CBDC is significantly different from cryptocurrencies and stablecoins in nature, issuance, management, and value. Although CBDCs and cryptocurrencies are both electronic and could be universally accessible, a fundamental difference is that a CBDC is the liability of a central bank, whereas a cryptocurrency or stablecoin is not.[62] CBDCs serve as legal tender, the legal implication of which is that one cannot reject CBDCs as a means of payment; however, one can refuse to accept BTC, ETH, or other cryptocurrencies and stablecoins as a form of payment.[63]

A central bank with a centralized management system issues and guarantees a CBDC, whereas a distributed network without a centralized agency issues and manages cryptocurrencies and stablecoins. Some cryptocurrencies utilize blockchain technology, meaning that a group of unknown persons behind their computers across the globe manage them.[64]

---

[58] *Electronic Money*, EUR. CENT. BANK (emphasis omitted), https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html (last visited Sept. 21, 2022).

[59] Firpo, *supra* note 51.

[60] Press Release, Bank of Jam., BOJ Prepares for Central Bank Digital Currency (Mar. 22, 2021), https://boj.org.jm/cbdc-information-press-release-22-march-2021.

[61] *Id.*

[62] Martin Chorzempa, *How are Central Bank Digital Currencies Different from Other Payment Methods?*, PETERSON INST. FOR INT'L ECON. (Apr. 12, 2021), https://www.piie.com/research/piie-charts/how-are-central-bank-digital-currencies-different-other-payment-methods.

[63] Kiff, *supra* note 53, at 9–10.

[64] *See id.* at 63.

Furthermore, under the law, the issuing central bank usually decides the value of a CBDC. This is in contrast to cryptocurrencies like BTC and ETH, whose values are determined by the marketplace and are known to be highly volatile.[65] Stablecoins, as its name suggests, aim for stability with values backed by collaterals, fiat currencies, or sometimes algorithms.[66] But there is no guarantee that stablecoins remain stable.[67] The recent TerraUSD crash is a case in point.[68] CBDCs, recognized as legal tender, may be the preferred choice for consumers seeking reliable alternatives, given their systemic significance and the robust backing by the full faith and credit of the government. For many individuals, a CBDC represents a safer form of payment than private digital currencies.[69] The underlying theory is that "[c]entral banks can always print money" even when other financial institutions face bank runs in a financial crisis.[70] Consumers can still have a claim on the central bank and will never lose their money.

B. *Motivations for Issuing a CBDC*

External pressure and internal needs drive central banks' experimentation and potential issuance of CBDCs. External pressure comes from the prevalent use of cryptocurrencies and the adoption of stablecoins in the payment sector.[71] Internal needs come from the need to improve financial inclusion, reduce transaction costs in the payment system, prevent illegal use of money, facilitate cross-border payments, and improve payment diversity.[72] In addition to these

---

[65] MANCINI-GRIFFOLI ET AL., *supra* note 2, at 13.

[66] *Introduction to Stablecoins. Use Cases and Examples*, PIXELPLEX (Dec. 23, 2020), https://pixelplex.io/blog/what-are-stablecoins; *see also* Garth Baughman et al., *The Stable in Stablecoins*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (Dec. 16, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/the-stable-in-stablecoins-20221216.html.

[67] *See* REPORT ON STABLECOINS, *supra* note 55, at 4.

[68] *See generally* Farran Powell & Michael Adams, *The Crypto Market Crash Is Driving Stablecoin Regulations*, FORBES ADVISOR, https://www.forbes.com/advisor/investing/cryptocurrency/stablecoin-crypto-crash/ (Nov. 4, 2022, 9:19 AM).

[69] *See* Chorzempa, *supra* note 62.

[70] *Id.*

[71] *See* Jiaying Jiang & Karmen Lucero, *Background and Implications of China's Central Bank Digital Currency: E-CNY*, 33 U. FLA. J. L. & PUB. POL'Y 237, 252–53 (2023).

[72] BANK OF CAN. ET AL., *supra* note 3, at 5–6; Ananya Kumar et al., *supra* note 8; JIM HIMES, WINNING THE FUTURE OF MONEY: A PROPOSAL FOR A U.S. CENTRAL BANK DIGITAL

internal needs common to most central banks, some central banks must meet distinctive needs. For instance, China probably wants to use its digital yuan to address the duopoly of Alipay and WeChat Pay in the payment market.[73] The United States aims to maintain its leadership in the global financial system with a potential digital dollar. The EU attempts to explore the use of a digital euro to support the international role of the euro and stimulate its demand for the euro among foreign investors.

One must note that this Part discusses central banks' motivations to experiment with CBDCs. Motivations are the starting points where central banks see the potential of CBDCs and are eager to work on them with the hope that CBDCs can be used to achieve such goals. But motivations differ from real results. Aiming to improve financial inclusion with the use of CBDCs does not mean that they can in effect improve financial inclusion. Many benefits of CBDCs remain highly theoretical. The real results remain to be seen. Any single reason will not be sufficient in influencing a central bank to issue a CBDC. Some also argue that a CBDC is a solution in search of a problem.[74]

CURRENCY 13–14 (2022), https://himes.house.gov/_cache/files/3/d/3da9ff6d-4e8a-47b7-be28-ced21ecb5724/2F46398524B2AD91FD40BDC5263F4F23.himes-cbdc-white-paper.pdf.

[73] *See* Jiang & Lucero, *supra* note 71, at 241.

[74] Christopher J. Waller, Fed. Rsrv. Sys., Speech at the American Enterprise Institute: CBDC—A Solution in Search of a Problem? (Aug. 5, 2021), https://www.bis.org/review/r210806a.pdf. The Governor's statement has sparked debate. Opponents argue that the numerous ongoing CBDC projects globally have demonstrated that CBDCs represent a chance for every nation to modernize the technology their central bank employs to distribute sovereign currency, ensuring a more inclusive and robust financial market. *See CBDC: An Opportunity or a Solution in Search of a Problem?*, EMTECH (Mar. 27, 2023), https://emtech.com/cbdc-an-opportunity-or-a-solution-in-search-of-a-problem/#:~:text=This%20is%20a%20fundamental%20component,payments%20apps%20didn%27t%20exist ("This is a fundamental component of financial services for economies to grow and thrive. CBDC is therefore, not a solution in search of a problem, it is indeed the coming next generation of infrastructure needed to replace the systems that were installed over [fifty] years ago, when payments apps didn't exist.").

1. External Pressure

The emergence and prevalent use of cryptocurrencies "are raising pressures on central banks to develop their own digital [currency]."[75] "Cryptocurrencies, especially [BTC], [have] again triggered intense debate over who should control money in the future."[76] "The peer-to-peer payment system of [BTC] also urged the world to rethink the merits and drawbacks of existing centralized payment systems."[77] Central banks might find themselves compelled to rethink their role and the need to issue a CBDC in response to cryptocurrencies. Should commercial activity substantially transition towards adopting cryptocurrencies, governments face the risk of relinquishing control over their monetary policies—mechanisms utilized by central banks to monitor inflation and ensure financial stability.[78]

Cryptocurrencies like BTC and ETH, while popular, are not the main threat. Because the value is extremely volatile, many investors (or speculators) "sock it away rather than use it" for payments.[79] The underlying technology of BTC (i.e., public blockchain) faces scalability challenges; therefore, the blockchain network cannot complete large volumes of transactions to meet market needs. The governance structure is also problematic because a group of unknown miners manage the network. It also poses great environmental challenges because transactions on the network consume enormous amounts of electricity.[80] Additionally, since cryptocurrencies "are not centrally issued or controlled . . . . [they] pose regulatory and law-enforcement challenges."[81]

Compared to BTC and ETH, stablecoins could pose a greater threat to central banks.[82] As previously mentioned, "stable" fiat

---

[75] Daren Fonda, *Why Cryptocurrencies Are a Threat to Central Banks*, BARRON'S, https://www.barrons.com/articles/cryptocurrency-is-threatening-the-role-of-central-banks-why-governments-must-go-crypto-51619814196 (May 3, 2021).

[76] Jiang & Lucero, *supra* note 71, at 251.

[77] *Id.*

[78] Fonda, *supra* note 75.

[79] *Id.*

[80] *Cambridge Bitcoin Electricity Consumption Index*, UNIV. OF CAMBRIDGE, https://ccaf.io/cbnsi/cbeci (last visited Sept. 21, 2023); *see also* Alexander Neumueller, A Deep Dive into Bitcoin's Environmental Impact, UNIV. OF CAMBRIDGE: JUDGE BUS. SCH. (Sept. 27, 2022), https://www.jbs.cam.ac.uk/2022/a-deep-dive-into-bitcoins-environmental-impact.

[81] MARC LABONTE & REBECCA M. NELSON, CONG. RSCH. SERV., R46850, CENTRAL BANK DIGITAL CURRENCIES: POLICY ISSUES 16 (2022).

[82] *See* REPORT ON STABLECOINS, *supra* note 55, at 8.

currency or other reference assets peg the value of stablecoins, making stablecoins more suitable for a store of value and a medium of exchange.[83] Although today's stablecoins are primarily used to facilitate the trade of other crypto assets, stablecoins could be more widely used in the future as a means of payment by households and businesses.[84] If a country widely adopts a foreign-backed stablecoin, it restricts the local central bank's ability to implement its own monetary policy.[85] Additionally, the local central bank could encounter the threat of currency substitution, a situation potentially leading to "dollarization." Therefore, stablecoins pushed central banks to contemplate the introduction of their own CBDCs.

2. Internal Needs

There are many internal reasons to explore CBDCs, and the motivations of different countries for issuing CBDCs depend on their economic situations. Some common motivations include promoting financial inclusion, increasing efficiency in payment and reducing transaction costs, preventing illegal use of money, facilitating cross-border payments, and introducing competition and resilience in the payment market.

Financial inclusion is a major motivator for developing CBDCs, especially in emerging economies.[86] If designed properly, some CBDC features could help improve financial inclusion. For instance, unbanked populations can still use CBDCs for daily transactions because CBDCs do not need to be associated with a bank account. Those who live in geographically remote areas with limited internet access or those who do not have a high-end smartphone can still use CBDCs for retail payments because CBDCs allow for offline transactions and payments, which can occur by tapping two phones.

---

[83] *See* discussion *supra* Part.II.A.

[84] REPORT ON STABLECOINS, *supra* note 55, at 1.

[85] *See* Jiang & Lucero, *supra* note 71, at 252.

[86] *See* Christian Barontini & Henry Holden, *Proceeding with Caution—A Survey on Central Bank Digital Currency* 10 (Bank for Int'l Settlements Papers, Working Paper No. 101, 2019), https://www.bis.org/publ/bppdf/bispap101.pdf; *see also* Codruta Boar et al., *Impending Arrival—A Sequel to the Survey on Central Bank Digital Currency* 4 (Bank for Int'l Settlement Papers, Working Paper No. 107, 2020), https://www.bis.org/publ/bppdf/bispap107.pdf; Boar & Wehrli, *supra* note 6, at 7; Raphael Auer et al., *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies* 8 (Bank of Int'l Settlement Papers, Working Paper No. 880, 2020), https://www.bis.org/publ/work880.pdf; ASHLEY LANNQUIST & BRANDON TAN, CENTRAL BANK DIGITAL CURRENCY'S ROLE IN PROMOTING FINANCIAL INCLUSION 4 (2023).

The interoperability of CBDCs with other payment systems can also bring the unbanked or underbanked population to the existing financial system. The cross-border potential of CBDCs could also help immigrants send money from developed countries, where they work, to developing or underdeveloped countries, where their families are located, with very low transaction costs. In addition, CBDCs could provide public access to central bank money, especially "[i]n jurisdictions where access to cash is in decline."[87] Last but not least, CBDCs could be used to make stimulus and other government-to-peer payments to unbanked households—"a March 22, 2020 draft of a U.S. House emergency . . . stimulus bill referred to a . . . 'digital dollar' [as a way to transfer] stimulus payments to unbanked Americans[,]" implying a motivation for developing a CBDC to further financial inclusion.[88]

Reducing costs associated with physical cash is also a primary motivation to adopt CBDCs for both advanced and emerging market economies.[89] It is costly to issue, maintain, and recycle physical cash. The private costs associated with physical cash use ranged from 0.2 percent of the GDP (in Norway) to 2.5 percent of the GDP (in Guyana); and banks, firms, and households primarily bear these costs.[90] The 2019 US Federal Reserve Board currency budget was $955 million, which "covered currency printing by the Bureau of Engraving and Printing, maintaining currency fitness, vault costs, protection, transportation[,] . . . [and] counterfeit deterrence."[91] Additionally, a decline in cash use also leads to an increase in the cost of accepting cash.[92] A CBDC could potentially cut back on some costs because digitalization eliminates the needs to print, recycle, or transport physical cash.

Central banks consider a CBDC given its potential for discouraging illicit activities, such as money laundering, terrorism financing, and tax evasion. Anonymity of transactions, especially with respect to high denomination banknotes and cryptocurrencies, greatly

---

87 BANK OF CAN. ET AL., *supra* note 3, at 5.

88 Kiff et al., *supra* note 53, at 14–15.

89 *See* Barontini & Holden, *supra* note 86, at 10; Boar et al., *supra* note 86, at 4–5.

90 Kiff et al., *supra* note 53, at 12.

91 *Id.* at 34 n.41 (citing BD. OF GOVERNORS OF THE FED. RSRV. SYS., DIV. OF RSRV. BANK OPERATIONS & PAYMENT SYS., 2019 CURRENCY BUDGET (2019), https://www.federalreserve.gov/foia/files/2019currency.pdf).

92 Barontini & Holden, *supra* note 86, at 3 (citing SVERIGES RIKSBANK, THE RIKSBANK'S E-KRONA PROJECT—REPORT 2 (2018)).

exacerbate illicit activities because transactions are very difficult to trace. CBDCs with a clear record of transactions will deter such activities. Therefore, central banks could retain control and obtain oversight over payment systems that are at risk of being used for illicit purposes.[93] CBDCs would further increase the government's ability to collect tax revenues efficiently, as transactions that would have occurred through cash-in-the-shadow-economy would end up in the tax base with the rise of CBDCs.[94] CBDCs could theoretically reduce the risk of counterfeiting paper currency, but the risk of large-scale electronic counterfeiting could be a serious concern for governments as well.[95]

The ability of CBDCs to facilitate efficient cross-border payment also motivates central banks in both developing and developed economies.[96] While emerging markets and developing economies (EMDEs) are generally motivated by domestic payments efficiency as opposed to cross-border payments efficiency, larger EMDEs with ongoing pilots are more strongly motivated by cross-border payments efficiency.[97] These emerging economies believe CBDC can reduce long transaction chains in cross-border payments.[98] Advanced economies are motivated to issue CBDCs because CBDCs have the potential for faster clearing and settlement between central banks,[99] as well as the potential to address "limited operating hours of current payment systems."[100] Other cross-border problems that central banks want to address with CBDCs include fragmented data formats, complexity of compliance checks, unclear foreign exchange rates, legacy technologies, funding costs, and weak competition.[101]

---

93 *See* Barontini & Holden, *supra* note 86, at 14.

94 Allen et al., *supra* note 31, at 12.

95 *Id.*

96 *See* BANK FOR INT'L SETTLEMENTS, *supra* note 40, at 10–11; MORTEN BECH ET AL., USING CBDCS ACROSS BORDERS: LESSONS FROM PRACTICAL EXPERIMENTS 4 (2022), https://www.bis.org/publ/othp51.pdf.

97 Boar & Wehrli, *supra* note 6, at 7–9.

98 Anneke Kosse & Ilaria Mattei, *Gaining Momentum—Results of the 2021 BIS Survey on Central Bank Digital Currencies* 8 (Bank for Int'l Settlements Papers, Working Paper No. 125, 2022), https://www.bis.org/publ/bppdf/bispap125.htm.

99 *See* Barontini & Holden, *supra* note 86, at 10; Boar et al., *supra* note 86, at 5; Kosse & Mattei, *supra* note 98, at 8.

100 Kosse & Mattei, *supra* note 98, at 8.

101 *Id.* at 8 graph 5.

Central banks intend to use CBDCs to introduce competition and resilience in the domestic payment market. Introducing a CBDC can diversify domestic payment systems, which would address the potential issues associated with a concentrated market.[102] Many private payment systems benefit from strong network effects such as benefits of aggregating data to provide additional services,[103] which may result in monopolies, high barriers to entry, and high costs for merchants.[104] Central banks that introduce CBDCs could disrupt the monopolies by introducing more actors into the payment market. Nonetheless, fragmentation from many existing systems can increase "cost and complexity of interoperability[,]" which CBDCs could potentially address by transfers between fragmented payment systems.[105] Some private payment systems may not account for the societal cost of potential systemic operational failures, including cyberattacks, leading to a possible underinvestment in security measures.[106] Further, a concentrated payment system market could result in private issuers providing lower quality services and commercializing user data.[107] As a result, users are the ones bearing the costs. CBDCs backed by the full faith and credit of a government could internalize some of the social costs because a central bank with government support possess better resources than the private sector to address cyberattacks and other systemic operational failures.

3. Motivations Unique to Specific Countries

One of China's motivations to issue a CBDC is to respond to the Alipay and WeChat Pay duopoly. Alipay and WeChat Pay control 55.1 percent and 38.9 percent of the mobile payment market, respectively, giving them a "duopoly over trillions of dollars in mobile payments."[108] This duopoly could create risks, such as economic instability in the case of a disruption to the digital payment infrastructure or "the bankruptcy

---

[102] *See* BANK OF CAN. ET AL., *supra* note 3, at 5–6.

[103] Wilko Bolt & David Humphrey, *Public Good Issues in TARGET: Natural Monopoly, Scale Economies, Network Effects and Cost Allocation* 7 (Eur. Cent. Bank, Working Paper No. 505, 2005), https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp505.pdf.

[104] BANK OF CAN. ET AL., *supra* note 3, at 5–6.

[105] *Id.*

[106] Kiff et al., *supra* note 53, at 12.

[107] *Id.*

[108] *How Will a Central Bank Digital Currency Advance China's Interests?*, CHINAPOWER, https://chinapower.csis.org/china-digital-currency (Aug. 26, 2020).

of a private company."[109] By developing a CBDC, China's central bank, the PBOC, can centralize clearing mechanisms and "enhance its oversight over digital currency . . . [to] reduce the autonomy of these companies[,]" thus strengthening the PBOC's supremacy and financial stability.[110]

The United States continue to investigate whether a US CBDC, or a digital dollar, can improve the efficiency of domestic payment systems.[111] Internationally, the United States also tries to explore whether a digital dollar can promote "global financial stability and mitigate systemic risk[,]" especially from "digital asset trading platforms and service providers" that are not subject to or in compliance with regulations or supervision.[112] Maintaining its position as a leader "in the global financial system and in technological and economic competitiveness" motivates the United States to invest in "payment innovations and digital assets."[113] The United States is motivated to stay at the forefront of developing digital assets like CBDCs "in setting standards that promote: democratic values; the rule of law; privacy; the protection of consumers, investors, and businesses; and interoperability with digital platforms, legacy architecture, and international payment systems."[114] Additionally, the US dollar and financial institutions play a role in the global financial system and confer economic and national security benefits, which the United States hopes to maintain through digital asset development.[115]

In Europe, issuing a digital euro would support Europe's drive toward continued innovation and "support other strategic objectives of the Eurosystem . . . . [such as] increase[ing] choice, competition[,] and accessibility with regard to digital payments."[116] As major foreign central banks issue CBDCs, they "could enhance the status of other international currencies at the expense of the euro[,]" which may motivate the EU to issue a digital euro to support the currency's

---

[109] Jiang & Lucero, *supra* note 71, at 250–51.

[110] *Id.*

[111] MONEY AND PAYMENTS, *supra* note 16, at 1.

[112] Press Release, White House, Executive Order on Ensuring Responsible Development of Digital Assets (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] EUR. CENT. BANK, *supra* note 15, at 3.

international role and stimulate the its demand among foreign investors.[117] "[I]nteroperable designs of CBDCs across currencies could contribute to strengthening the international role of the euro and to improving cross-currency payments . . . without having to grant non-euro area residents access to the digital euro."[118] Further, the EU could be motivated to issue a digital euro to lead by example in reducing the costs and ecological footprint associated with payment systems and infrastructure, which may create incentives to provide payment services that also have reduced costs and ecological footprints.[119]

Other countries, including the Bahamas, Jamaica, Eastern Caribbean countries (Saint Kitts and Nevis, Montserrat, Antigua and Barbuda, Dominica, Saint Lucia, Saint Vincent and the Grenadines, and Grenada), and Nigeria, have launched CBDCs, each driven by various motivations.[120] In the Bahamas, an important incentive is the acceleration of recovery following natural disasters that cause physical damage to banks and ATMs.[121] Jamaica's primary motivation "was to reduce storage and handling costs of cash usage," with an expectation to save an estimated $7 million per year that is currently spent on replacing, storing, and handling cash.[122] "The Eastern Caribbean Central Bank (ECCB) launched its digital currency" aiming to improve financial inclusion and expand banking services across challenging terrains.[123] The e-Naira, Nigeria's digital currency, is also primarily motivated by the goal of increasing financial inclusion as well, but another motivator is the potential for a well-managed digital currency to increase the GDP by $29 billion over the next ten years.[124]

---

[117] *Id.* at 14.

[118] *Id.*

[119] *Id.* at 15.

[120] Kumar et al., *supra* note 8.

[121] Vicki Hyman, *The Bahamas Is 'Disaster-Proofing' Payments with Its First-Ever Digital Currency*, MASTERCARD (Feb. 18, 2021), https://www.mastercard.com/news/perspectives/2021/the-bahamas-is-disaster-proofing-payments-with-its-first-ever-digital-currency.

[122] Kumar et al., *supra* note 8.

[123] Pierrick Ribes, *Why Governments Around the World Are Going All in for Central Bank Digital Currencies*, ENTREPRENEUR: MIDDLE E. (Aug. 12, 2023), https://www.entrepreneur.com/en-ae/finance/why-governments-around-the-world-are-going-all-in-for/457269.

[124] Kumar et al., *supra* note 8.

II. 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. But, 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*

"[T]he notion of privacy is not consistent across the globe . . . ."[125] Defining privacy proves to be quite complicated, and many find it difficult to precisely define privacy.[126] According to Julie Inness, the legal and philosophical discourse of privacy is in a state of chaos.[127] Jurists, legal scholars, philosophers, psychologists, and sociologists appear to have a welter of different conceptions of privacy.[128] 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.[129] These headings are as follows:

> (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.[130]

But, many scholars have criticized that these "conceptions [and theories of privacy] are either too narrow or too broad."[131] Take the

---

[125] WORLD ECON. F., *supra* note 27, at 3; *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).

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

[127] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2002); *see also* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992).

[128] Solove, *supra* note 127, at 1092.

[129] SOLOVE & SCHWARTZ, *supra* note 126, at 43.

[130] Solove, *supra* note 127, at 1092.

[131] *Id.* at 1094 (critiquing all six categories of conceptions and explaining why each conception is either too broad or too narrow or both).

conception of the right to be let alone as an example, Samuel Warren and Louis Brandeis, in their famous article, *The Right to Privacy*,[132] inspired significant attention to privacy and framed the discussion of privacy in the United States throughout the twentieth century.[133] But 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 important values."[134] "Being let alone does not inform us about the matters in which we should be let alone."[135] Therefore, many commentators argue that "defining privacy as the right to be let alone is too broad."[136]

Additionally, "[p]rivacy 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."[137] While individuals seemingly hold differing views of what information they feel comfortable sharing, they exhibit similar changes in attitude regarding what information is considered private when the context in which the information is shared changes. For example, individuals demonstrated striking similarity in the degree to which they felt comfortable sharing personal information with different recipients such as a spouse, other family members, coworkers, lawyers, and

---

[132] 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. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890). 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. *See* ROBERT E. SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOUSITY FROM PLYMOUTH ROCK TO THE INTERNET 128 (2000).

[133] Solove, *supra* note 127, 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, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966) (hailing Warren & Brandeis' article as the "most influential law review article of all."); 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).

[134] Solove, *supra* note 127, at 1101.

[135] *Id.*

[136] *Id.* at 1102; *see also* DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 5, 16 (1979); Tom Gerety, *Redefining Privacy*, 12 HARV. CIV. RTS.-CIV. LIBERTIES L. REV. 233, 234–35, 263 (1977).

[137] DIGIT. DOLLAR FOUND., THE DIGITAL DOLLAR PROJECT: EXPLORING A U.S. CBDC 20 (2020), http://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf.

telemarketers.[138] In other words, people actually have largely matching concepts of privacy; it is the context in which the private information is transmitted to another that determines their barometer for privacy. It is difficult to have one conception that covers all scenarios a person might face and may therefore be more appropriate to use a framework that assesses the context in which a scenario occurs.

B. *Pragmatic Approach*

"[T]he existing method of conceptualizing privacy has thus far proven to be problematic and unsatisfying . . . ."[139] In response, Daniel Solove proposed a pragmatic approach that recognizes context and contingency, rejects a priori knowledge, and focuses on concrete practices.[140] According to pragmatists, knowledge originates through experience.[141]

Pragmatism has its philosophical grounds. Just as John Dewey suggests, "philosophical inquiry begins with problems in experience,

---

[138] HELEN NISSENBAUM, PRIVACY IN CONTEXT 151–52 (2010) ("Respondents were highly discriminating in their reports, and similar to one another in how their judgments were affected by circumstances, types of information, and recipients, affirming that the degree of comfort people experience when sharing information is a function of several factors and not simply one, such as control or sensitivity of information. Information types or attributes included age, marital status, health status, opinions, salary, Social Security numbers, religious affiliations, and phone number; and recipients included family members, telemarketers, and coworkers. Individual variability was overshadowed by striking similarities in the degree to which information types and recipient roles were predictive of the respondents' level of comfort in sharing information. This should put to rest the frequent insinuation that privacy preferences are personal and idiosyncratic.").

[139] Solove, *supra* note 127, at 1126.

[140] *Id.* at 1127.

[141] *Id.* at 1127 n.231 (citing PRAGMATISM AND CLASSICAL AMERICAN PHILOSOPHY: ESSENTIAL READINGS AND INTERPRETIVE ESSAYS 3 (John J. Stuhr ed., 2000)) ("Pragmatists reject the view of philosophy 'as a purely theoretical quest for eternal truths or knowledge of an ultimate and unchanging reality.'"); *see also* John Dewey, *Reconstruction in Philosophy*, *in* 12 THE MIDDLE WORKS OF JOHN DEWEY 92 (Jo Ann Boydston ed., 1982). Many pragmatists go beyond making the epistemological claim that an ultimate or transcendent reality is not knowable. John Dewey observes some philosophers "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." JOHN DEWEY, RECONSTRUCTION IN PHILOSOPHY 24 (1920). Dewey claims that philosophy is still possible by exploring knowledge gleaned from experience. *Id.* at 113–14.

not with abstract universal principles."[142] Pragmatism also shares much in common with Wittgenstein's idea of family resemblances.[143] This notion of family resemblances demonstrates that "universals are neither necessary nor even useful in explaining how words and concepts apply to different things."[144] "[A] new application of a word or concept will" need to be clarified in its specific context, and these clarifications will be adequate on their own.[145] This perspective liberates us from the need to argue about which conditions adequately fulfill the concept of privacy, or from trying to establish "[fixed] conceptual boundaries and common denominators."[146] Instead, it focuses on "mapping out the terrain of privacy by examining specific problematic situations."[147]

In line with this pragmatic philosophy, Solove's pragmatic approach emphasizes the contextual and dynamic nature of privacy.[148] It conceptualizes privacy in particular contexts rather than in the abstract.[149] It does not adhere to traditional frameworks that aim to define privacy in sweeping, general terms, requiring set conditions to be met.[150] Instead, conceptualizing privacy is more about identifying and trying to address specific issues.[151] Solove argues that privacy issues arise when there are "disruptions to certain practices."[152] By "practices," he means a range of "activities, customs, norms, and traditions."[153] "Examples of practices include writing letters, [speaking with a psychotherapist], engaging in sexual intercourse," and consulting a lawyer.[154] In this viewpoint, privacy is not an isolated or

---

142 Solove, *supra* note 127, at 1127; *see also* JOHN DEWEY, EXPERIENCE AND NATURE 3–4 (1925); MICHAEL ELDRIDGE, TRANSFORMING EXPERIENCE: JOHN DEWEY'S CULTURAL INSTRUMENTALISM 4 (1998) ("Thinking . . . is [thus] a tool for solving problems . . . .").

143 Solove, *supra* note 127, at 1126.

144 Stanley Cavell, *Excursus on Wittgenstein's Vision of Language*, *in* THE NEW WITTGENSTEIN 21, 35 (Alice Crary & Rupert Read eds., 2000).

145 *Id.*

146 Solove, *supra* note 127, at 1126.

147 *Id.*

148 *Id.* at 1127.

149 *Id.* at 1128.

150 *Id.* at 1092.

151 *Id.* at 1129.

152 Solove, *supra* note 127, at 1129.

153 *Id.*

154 *Id.*

abstract concept; "[p]rivacy is a dimension of these practices."[155] More specifically:

> 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.[156]

Addressing disruptions to practices is also indicative of the important values related to the fair and just treatment of individuals.[157] As Julie Cohen points out, autonomy in an unpredictable world necessitates a space relatively shielded from external examination and intrusion—a realm in which individuals can actively shape their identities.[158]

To understand practices and disruptions to practices properly, two additional concepts are particularly relevant—namely, private matters and the value of privacy. "Turning our focus from disruptions to the practices they disrupt, [people] often refer to aspects of these practices as 'private matters.'"[159] In simpler terms, individuals label particular things, locations, and activities as "private."[160] Traditionally, one considers one's house, diary, body, and sexual behavior private.[161] 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.[162] Instead, privacy is embedded in activities or norms that are naturally borderless.[163] 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 between

---

155 *Id.*

156 *Id.* at 1093.

157 Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000).

158 *Id.* at 1424.

159 Solove, *supra* note 127, at 1131.

160 *Id.*; *see also* ALAN F. WESTIN, PRIVACY AND FREEDOM 32–42, 57–60 (1967).

161 Solove, *supra* note 127, at 1132.

162 Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUT. & TECH. L.J. 1, 40 (1998).

163 *See id.*

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 or physical threat and harm to the person. But if these photos and text messages involve human trafficking, government (even general public) access to 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, violating or destroying one person's privacy. The law should evaluate these conflicting values to decide if certain matters should be private.

C. *Contextual Integrity*

Building upon this notion of contextually dependent concepts of privacy, Helen Nissenbaum developed a new theory of privacy known as contextual integrity, which holds that privacy is determined by the "*appropriate* flow of personal information" within informational norms or parameters.[164] These parameters are as follows: (1) the context in which a transmission occurs, (2) the actors involved, (3) the attributes of the conveyed information, and (4) the principle facilitating the transmission of the data.[165]

In the traditional "who, what, when, where, why" analysis, these different parameters each answer different questions. Context is the "when and where," actors are the "who," attributes are the "what," and transmission principles are the "why." Context refers to the situation in which information is transmitted and provides the means to determine the informational norms associated with the activity evaluated. Actors are the parties involved in an information exchange and fall into three categories, although an actor may fill multiple roles simultaneously: the sender, the receiver, and the subject of the information.[166] Attributes are the characteristics and content of the information being transmitted.[167]

---

[164] NISSENBAUM, *supra* note 138, at 127–28.

[165] *Id.* at 140–47.

[166] *Id.* at 141.

[167] *Id.* at 143–44.

A transmission principle is a norm that governs the flow of information from one actor to another within a specific context.[168] It defines what is considered appropriate or acceptable in terms of information sharing within that context. It is best understood as the expected characteristic of the underlying reason for transmission: the sender's goal in the transmission, whether the information transmission was voluntary or compelled, whether the transmission is unidirectional or bidirectional, whether the transmission is necessary or optional to achieve a desired outcome, whether the transmitted information is confidential or may be shared, etc. For example, in both a healthcare and friendship context, confidentiality is an expected transmission principle. But in the healthcare context, the flow of information is unidirectional from patient to physician, whereas friends are expected to reciprocally exchange confidential information.[169]

A variance in any of these parameters might alter the subject's perception of privacy, leading to a different response about whether their privacy maintains. This concept is more readily applicable to privacy in a digital world because it does not rely on the territorial view of privacy referenced above.

The contextual integrity framework helps explain why an Amazon customer may only feel moderately uneasy about Amazon recommending books or products based on their prior Amazon purchases, while simultaneously harboring outright resentment toward targeted third-party advertisements on a different website facilitated by cross-site tracking of the same purchase.[170] In the first scenario, the customer is both the subject and initial sender of the purchase data being sent to Amazon, the recipient, under transmission principles of completing a transaction and reciprocity (the user expects Amazon to become a sender of information back to them, making users a recipient). The subsequent Amazon recommendations manifest internally and do not imply that Amazon violated the contextual integrity of the information flow by sharing any of the data with other parties.[171]

---

168 *Id.* at 145–47.

169 *Id.* at 146.

170 NISSENBAUM, *supra* note 138, at 195.

171 For purposes of this hypothetical, the customer is unaware that Amazon is selling their purchase data to third parties even though Amazon openly acknowledges that their customer data is sold to partners. *See Amazon.com Privacy Notice*, AMAZON,

In the latter scenario, however, the customer can infer that Amazon violated contextual integrity because even though they remain the data subject and the recipient, the sender is now a third party with which the subject has not previously interacted. This implies that, at some point, Amazon, the recipient that the customer trusted with purchase data in one privacy context, later became a sender of that data to another recipient that the customer (the original sender) did not intend to include, thus violating the integrity of the context and transmission principles of the original informational transmission. The attributes of the data might even be the same in both scenarios, but the change in actors and transmission principle alters the context in which it was provided and leads to a radically different attitude in the customer.

This demonstrates how contextual integrity offers an understanding of privacy that is better suited to the increasingly digital world. Every digital interaction generates data, so evaluating privacy by identifying the parties and their contextual intentions for transmitting that data provides an effective method of evaluating whether privacy has been sufficiently preserved.

D. *Pragmatic Approach and Contextual Integrity in the Context of CBDCs*

The pragmatic approach and contextual integrity are 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 example, Samuel Warren and Louis Brandeis' famous formulation of privacy as one's right to be let alone is also relevant in the context of CBDCs. One has the right to live one's life as one chooses, including one's financial life, such as deciding with whom one wants to transact and where and when one makes a payment, free from intrusion or invasion. But 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

---

https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (Aug. 11, 2023).

security and the challenge of terrorism."[172] "The stakes are considerably higher today than in Brandeis' time" in the 1890s.[173]

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 prefer to take some measures to shield themselves from unwanted access. But, "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, must receive 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 too abstract to capture all aspects of privacy in the context of CBDCs. Therefore, an alternative to understand privacy is necessary.

The second reason the pragmatic approach and the theory of contextual integrity are well suited to the discussion of CBDCs is that they are flexible enough to capture many practical and nuanced questions. Various CBDC designs can raise very different privacy questions. One-tier and two-tier designs will allow for different parties to collect, access, and store CBDC data, which will raise different privacy questions.[174] Centralized and DLT designs will expose very different CBDC information to different parties involved.[175] Various parties, such as the payor, 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

---

[172] Leah Burrows, *To be Let Alone: Brandeis Foresaw Privacy Problems*, BRANDEISNOW (July 24, 2013), https://www.brandeis.edu/now/2013/july/privacy.html.

[173] *Id.*; *see also* NISSENBAUM, *supra* note 138, at 145.

[174] *See* discussion *infra* Part III.A.

[175] *See* discussion *infra* Part III.B.

address. Privacy thus means different sets of rights and obligations to each of the parties. No one single conception of privacy captures all problems arising from different settings and for all parties. The pragmatic approach and contextual integrity theory are more suitable because they address privacy contextually in different scenarios and focus on 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, this Article adopts Daniel Solove's pragmatic approach and Helen Nissenbaum's contextual integrity theory to conceptualize privacy in the context of CBDCs. This Article focuses on understanding privacy in specific contextual situations rather than seeking to illustrate an abstract conception of privacy. To have a more nuanced understanding of privacy in the CBDC context, one must ask five questions: What are the contexts? Who are the actors? What are the attributes of the information? What are the transmission principles facilitating the exchange of the information? The last question explores what aspects of information sharing practice should be considered private and what values to balance when recognizing and protecting the value of privacy in CBDCs.

The specific contextual situation related to CBDCs centers on the practice of payment, or to be more precise, making payments with CBDCs.[176] Four actors are involved in processing a payment: the payor, 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 attributes of the information include payors and payees' names, phones, addresses, and the balances on their accounts, where and when they made the payment, and which entities processed the payment.

Transmission principles are one of the parameters embedded in an informational norm, in this payment context, covarying with actors and attributes. A single payment may involve multiple transmission principles between different actors. For instance, when a payor makes a CBDC payment to a payee, the transmission principle is buying a good or service, which necessitates conveying data about monetary amount, the payor's account or wallet address, the payee's account or wallet address, etc., to the payment processors. The payment processor, however, may transmit the data to others under a different

---

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

transmission principle such as forwarding the information to law enforcement under a national security principle. Whether or not the payor and payee reasonably understood and knowingly consented to this subsequent transmission principle is determined by the societal informational norms associated with CBDC payments, which in turn determines their view of whether their privacy has been adequately preserved. If society is widely aware of and accepts the sharing of CBDC payment data with law enforcement agencies, then contextual integrity is preserved. A lack of societal understanding and approval of this sharing of information with law enforcement agencies violates contextual integrity, and the parties will rescind the transmission as a breach of their privacy, undermining their faith in the privacy of a CBDC payment.

Privacy is one dimension of CBDC payments. It refers to the degree to which attributes of CBDC data such as identity and transaction data are hidden from others, including the payee, participating entities, and 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 or to preserve contextual integrity. 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.

Assessing which aspects of a CBDC payment should remain private, and from whom, requires a normative analysis. One can argue that identity and transaction information, for the purpose of CBDC payments, are private matters. Such information should be kept private from the government, the public, or any third parties unrelated to the transaction. "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."[177] Similarly, CBDCs as a new form of retail payment method share the same characteristics. Account, identity, and transaction data, separately or collectively, can be used to construct a detailed picture of an individual's personal life. Revealing such information to the government, public, or unrelated third parties in the transactions could jeopardize an individual's personal life, dignity,

[177] Geoffrey Goodell et al., *A Digital Currency Architecture for Privacy and Owner-Custodianship*, FUTURE INTERNET, May 14, 2021, at 3.

and freedom. Therefore, maintaining the confidentiality of such information from these entities is crucial.

The degree of privacy also varies and relies on a normative assessment. One can consider their identity and transaction information private, but one does 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) [,]"[178] or vise versa. 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."[179] Central banks should conduct cost-benefit analyses or use other mechanisms to decide the extent to which CBDC data should be hidden from which entity.

When conducting this normative analysis, it is necessary to balance various conflicting values. On one hand, people recognize the value of keeping some CBDC data private because they cherish the freedom to make payments whenever, wherever, and with whomever they desire without intrusion. On the other hand, individuals 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 private after balancing all conflicting values.

The law is usually the result of balancing all these values. Take the Financial Services Modernization Act of 1999, more commonly known as the Gramm-Leach-Bliley Act (GLBA), as an example;[180] the GLBA "enables the creation of financial conglomerates that provide a host of different forms of financial services."[181] It "authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies."[182] The GLBA recognizes the social and economic value of providing broader financial services to ordinary Americans. Financial institutions sharing

---

178 Darbha & Arora, *supra* note 24.

179 *Id.*

180 Financial Services Modernization Act of 1999, 15 U.S.C. §§ 6801–6809.

181 SOLOVE & SCHWARTZ, *supra* note 126, at 575.

182 *Id.*

financial data with affiliated entities "was seen as helping them target their customers to better meet their needs."[183]

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."[184] 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."[185] The law also requires financial institutions to give notice to customers when financial institutions share customer information with affiliated entities.[186] If financial institutions share customer information with nonaffiliated entities, they should first provide customers with the ability to opt out of the disclosure.[187] 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 rather a dimension of the practice of CBDC payments. Privacy is a part of payment practices. Payment practices include a payor sending money to a payee (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 ensure the payment is both legitimate and legal. Because privacy is part of the payment practices, certain elements of CBDC payments should be considered private as well. Any deviation from the informational norms involving the private information would be considered a violation of privacy. Arguments about what should be considered private and from whom are normative and could vary between various jurisdictions, cultures, and times. When conducting normative analysis, it is necessary to balance the value of CBDC data privacy with other conflicting values.

---

[183] *Id.*

[184] *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act (last visited Sept. 22, 2023).

[185] Financial Services Modernization Act of 1999 § 6809(4).

[186] *Id.* § 6802(a).

[187] *Id.* § 6802(b).

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 must be solved. This Part 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 distinct features and capabilities.[188] Different design choices will lead to unique privacy concerns. This Article agrees with MIT and the Federal Reserve Bank of Boston's view that design options for CBDCs are more nuanced than generally perceived.[189] Many commonly assumed categories are still very limited; those categories are insufficient to capture the intricate decisions involved in aspects like access, the role of intermediaries, institutional functions, and data storage policies with regard to CBDC design.[190]

This Article does not aim to cover all design choices, a task that would be practically unfeasible, and explore their respective privacy implications. Instead, it investigates two structural and foundational design choices as examples. All central banks will encounter and must decide on these two design choices before they move on to others. Figure 1 shows these two design choices cover the operational model and infrastructure. 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 (also

---

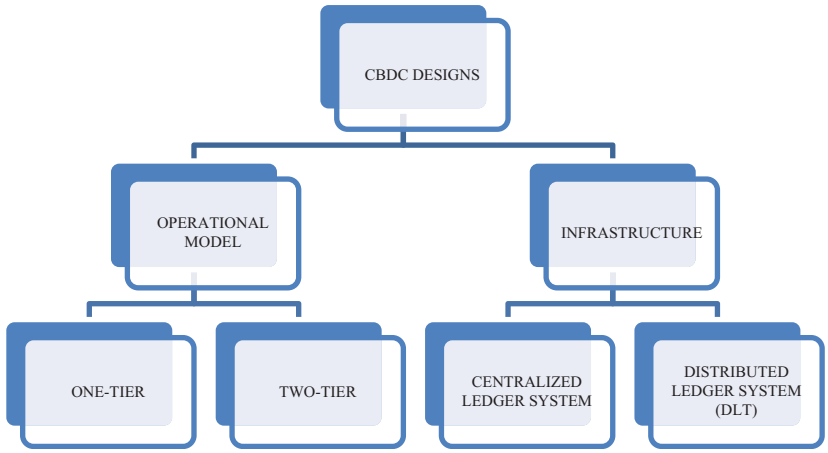
[188] GABRIEL SODERBERG ET AL., BEHIND THE SCENES OF CENTRAL BANK DIGITAL CURRENCY: EMERGING TRENDS, INSIGHTS, AND POLICY LESSONS 12 (2022), https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174.

[189] FED. RSRV. BANK OF BOS. & MASS. INST. OF TECH. DIGIT. CURRENCY INITIATIVE, PROJECT HAMILTON PHASE 1: A HIGH PERFORMANCE PAYMENT PROCESSING SYSTEM DESIGNED FOR CENTRAL BANK DIGITAL CURRENCIES 30 (2022), https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx. This Article agrees with the analysis in Project Hamilton that existing categorizations of design choices are insufficient to reveal the complexity of choices in access, intermediation, institutional roles, and data retention in CBDC design. This Article does not intend to come up with new or better categories. Instead, this Article picks two existing design choices, meaningful and foundational although imperfect, to address their privacy issues.

[190] *Id.*; *see also* Rod Garratt et al., *Token- or Account-Based? A Digital Currency Can Be Both*, LIBERTY ST. ECON. (Aug. 12, 2020), https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both.

known as a layered intermediary model). Infrastructure refers to the ways of recording transactions or updating credit and debit information. Two design choices are available: a centralized (conventional) ledger system and a distributed ledger technology (DLT) system.

Figure 1: CBDC Design Choices



To understand the privacy issues that could emerge from various design choices, methodologically, this Article first examines the dataflow of each design choice. Following the dataflow, it delves deeper into identifying 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 and transaction data. Some data are encrypted while others 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., 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.[191] This Article argues that the verification object is not a structural and foundational question like the choice of operational model and infrastructure. This Part concludes by

[191] *See* Auer & Böhme, *supra* note 29, at 88, 93; *see also* DIGIT. DOLLAR FOUND., *supra* note 137, at 17.

critiquing the inconsistent use of terminologies and the purported need to distinguish between account-based and token-based systems. It further elaborates on why this design element is not considered a foundational and structural choice for the central bank to decide at the outset.[192]

A. *Operational Model*

The operational model determines how CBDCs are distributed and who performs end-user facing tasks. Figure 2 shows a one-tier operational model, also called a direct distribution model, which means the central bank directly issues CBDCs to end users, such as individuals, corporations, and merchants. The central bank communicates 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.

Figure 3 displays a two-tier operational model, which means the central bank first issues CBDCs to intermediaries, such as commercial banks, cashless payment services providers, and other authorized institutions, and the intermediaries then issue CBDCs to end users. In other words, "[t]he obligation to provide CBDCs on demand would fall to the intermediar[ies] rather than the central bank."[193] "To guarantee that in all cases the customer's CBDC[s] would be honored . . . the intermediary would have to hold an equal amount of [reserve] at the central bank."[194] Additionally, the central bank also delegates most of the consumer-facing work and banking services to intermediaries. End "[u]sers 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.[195] Depending on the design, the central bank can retain a copy of all retail CBDC holdings or wholesale CBDC holdings of the intermediaries.

---

[192] *See* discussion *infra* Part III.C.

[193] Gregory Baer, Central Bank Digital Currencies: Costs, Benefits and Major Implications for the U.S. Economic System 5 (Apr. 7, 2021) (unpublished working paper) (on file with Bank Policy Institute).

[194] *Id.*

[195] Agustín Carstens, Gen. Manager, Bank for Int'l Settlements, Remarks at Hoover Institution Policy Seminar: Digital Currencies and the Future of the Monetary System (Jan. 27, 2021), https://www.bis.org/speeches/sp210127.pdf*; see also* Fabio Panetta, Member of the Exec. Bd., Eur. Cent. Bank, Speech at a Bruegel Online Seminar: Evolution or Revolution? The Impact of a Digital Euro on the Financial System (Feb. 10, 2021), https://www.bis.org/review/r210211d.pdf.

Figure 2: One-Tier Operational Model

Central bank End users

Figure 3: Two-Tier Operational Model

Issuance of CBDC:
Consumer facing tasks:

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 the CBDC in the account, balance, etc. (note: by default, this Article uses an account-based model here). When the central bank handles 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, know your customer (KYC) and AML, transaction risk assessment, clearing, settlement, and many more.[196] 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 communications with end users, including collecting and managing end users' account information. Intermediaries can also clear and settle transactions and, therefore, will have a copy of transaction details, unless the system is designed to intentionally obfuscate information through privacy enhancing mechanisms such as ZKP.[197] 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.

---

[196] *KYC (Know Your Customer) vs AML (Anti-Money Laundering)*, DOW JONES, https://www.dowjones.com/professional/risk/glossary/anti-money-laundering/kyc-vs-aml (last visited Oct. 12, 2023) (explaining KYC and AML).

[197] *See* OFF. OF SCI. & TECH. POL'Y, *supra* note 18, at 29.

From a privacy point of view, the one-tier operational model, which enables central banks to collect and store an enormous amount of end-user data, raises three privacy concerns: (1) mass surveillance, (2) cybersecurity risks, and (3) potential data misuse and abuse by other government authorities.

Mass surveillance refers to the deployment of "systems or technologies that collect, analyze, and/or generate data" on either the whole population or a large fraction of it, "rather than limiting surveillance to individuals [for whom] there is a reasonable suspicion of wrongdoing."[198] Mass surveillance is a concern because it "enables significant power imbalances and hinders people's autonomy."[199] Power imbalance occurs when a government or an entity gains access to a vast amount of data and retains exclusive control over how that data is used, while those being monitored generally lack similar access to data and are, therefore, unable to influence how their data is being used.[200] This concentrates power in the hands of those who control the data, creating an unequal dynamic. Mass surveillance hinders people's autonomy because "[i]t creates an environment of suspicion and threat, [leading even those who have not committed] any wrongdoing to change . . . the way they act, speak[,] and communicate."[201] This behavioral shift is often referred to as the *chilling effect* of mass surveillance, which restricts the lawful exercise of individuals' rights including the freedom to express yourself and to protest.[202]

The one-tier operational model could trigger mass surveillance concerns because central banks inherently occupy a dominant position in the power dynamic. Central banks not only by default collect and store a vast majority of end-users' CBDC data but also hold the authority to decide how this data is used. Citizens may change their spending behaviors due to the concern that they are being closely monitored, invoking the "Big Brother is watching" sentiment. As a result, their freedom to make spending choices is compromised.

---

198 *Mass Surveillance*, PRIVACY INT'L, https://privacyinternational.org/learn/mass-surveillance (last visited Sept. 22, 2023).

199 *Id.*

200 *Id.*

201 *Id*

202 *Id.*

But, this Article does not agree with the statement that central banks create CBDCs in order to monitor or control their citizens.[203] People with such view misunderstand the role of central banks, as well as the ways central banks utilize data. Generally speaking, mass surveillance is not the intended purpose of launching a CBDC, at least not for most of the central banks, for two reasons below.

First, in democratic countries, central banks, such as the Federal Reserve or European Central Bank, do not equal to government. Central banks operate independently and make independent decisions without needing approval from the their governments, such as the White House or government bodies of European member countries. Assuming central banks operate within their constitutional mandates, the individuals' CBDC data (who pays whom, when, and where) is of limited value to a central bank. The aggregated data, which need not be personally identifiable, offers insight into the economy. One or some individuals' spending habits or financial transactions are not representative of larger economic trends or conditions. They are anecdotal at best and not useful for policy decisions that affect an entire economy. Additionally, individual financial behaviors can vary widely due to numerous factors such as age, income, location, and personal preferences. This high variability makes individual data points less useful for macroeconomic analysis.

In contrast, only aggregated data provides valuable insights into various economic indicators such as consumer spending, savings rate, and investment flows. These are essential metrics for central banks to monitor and influence through policy measures. But, the data set must be large enough to be meaningful; if only a small segment of the population within a jurisdiction uses CBDCs, the collected data may not be sufficient to identify trends and patters for informed policymaking. It is unlikely that CBDC data, assuming one is issued by a central bank, would be large enough to yield meaningful insights to economic trends and patterns. This is because, in a practical setting, a CBDC is likely to coexist with other existing payment instruments such as cash, card payments, and mobile payments. More importantly, central banks do not need personally identifiable data to gain these insights; anonymized data suffices.

---

[203] *But see* Aditi Kumar & Eric Rosenbach, *Could China's Digital Currency Unseat the Dollar?*, FOREIGN AFFS. (May 20, 2020), https://www.foreignaffairs.com/articles/china/2020-05-20/could-chinas-digital-currency-unseat-dollar.

Second, even in authoritarian countries, the government likely possesses a variety of tools to monitor or control their citizens.[204] States own many financial institutions, providing direct government access to that data. For those institutions that are not state owned, the government can often mandate the submission of financial data. Consequently, creating and maintaining a CBDC system would not be the most economically and operational efficient approach for government-led mass surveillance. Therefore, the primary motive behind most central banks issuing a CBDC is unlikely to be mass surveillance. In democratic countries, central banks generally do not have the incentive to closely monitor everyone's personalized data.[205] Furthermore, central banks in authoritarian regimes do not require CBDCs as a tool for mass surveillance, as they already have other methods at their disposal for that purpose.

When it comes to the question of whether mass surveillance, arising from a central bank holding vast amounts of end-user data, directly equates to an invasion of privacy, the answer differs depending on the jurisdiction. Each jurisdiction has its own set of societal norms on what is considered permissible for central banks to do with end-user data and such society norms are influenced by unique values, cultures, and times.[206] In the United States, "Americans' concerns about privacy arose from fears of government access to personal information."[207] There might be society agreement that allows the Federal Reserve to examine end-user personal data for AML and CFT compliance. But, continuous surveillance of such data without a reasonable justification is likely to be deemed unacceptable as it hinders people's autonomy over their financial activities and curtails civil rights and freedoms.[208] If the Federal Reserve were to engage in such practices, it would violate

---

[204] *Surveillance Technologies*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/mass-surveillance-technologies (last visited Sept. 22, 2023).

[205] RODNEY JOHN GARRATT & MICHAEL JUNHO LEE, FED. RSRV. BANK OF N.Y., MONETIZING PRIVACY 5 & n.7 (2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr958.pdf .

[206] *See* discussion *supra* Part II.

[207] JOHN STEPHENSON, AM. LEGIS. EXCH. COUNCIL, ABUSE AND MISUSE OF PERSONAL INFORMATION: A REPORT ON ISSUES AND TRENDS IN PRIVACY 3 (2013), https://alec.org/wp-content/uploads/2015/11/Abuse-and-Misuse-of-Personal-Info-Final-03202013.pdf.

[208] *End Mass Surveillance Under the Patriot Act*, AM. C.L. UNION, https://www.aclu.org/issues/national-security/privacy-and-surveillance/end-mass-surveillance-under-patriot-act (last visited Sept. 22, 2023).

data integrity (in Helen Nisenbaum's term) or an infringement of end-user privacy.

In addition to mass surveillance concerns, cybersecurity risks also pose significant threats to individual and collective privacy. Weak cybersecurity measures lead to unauthorized access to CBDC database, exposing details about end users' spending habits. This kind of information could be highly valuable to commercial entities, thereby creating a strong incentive for hackers to attack the CBDC system, extract data, and sell data to interested parties. The one-tier model worsens the situation by centralizing such data within a single entity, i.e., the central bank. It becomes easier for attackers to breach the system and gain access to individual and collective data.

The third privacy concern under the one-tier operational model is the possibility of data misuse or abuse by other branches of the government. Data misuse typically refers to the use of data contrary to the agreed-upon rules.[209] Data abuse is a type of data misuse, "normally with malicious intention, causing harm or unfair gain."[210] Given that CBDCs are a new experiment in many jurisdictions, crafting robust rules on data management proves to be a challenging task for many central banks. In the absence of agreed-upon rules, sharing CBDC data with other government agencies could risk exposing sensitive end-user data to unintended recipients. These recipients might then use the data for unintended purposes, recklessly or maliciously, thereby breaching privacy norms and potentially crossing legal boundaries. Even if rules are in place, the central bank and other involved entities often do not clearly define the mechanisms for overseeing and ensuring compliance, let alone their actual enforcement.

The two-tier model presents two privacy concerns: (1) an increased number of data collection points, heightening the risk of data misuse or abuse, and (2) increased cybersecurity risks at each of these collection points.

In a two-tier system, end-user data is stored across multiple authorized intermediaries, inherently multiplying the places where data could be compromised. These intermediaries may combine CBDC data with other types of financial and personal data, generating comprehensive user profiles. Unlike central banks, these authorized

---

[209] Swaroop Sham, *What Is Data Misuse?*, OKTA (June 25, 2020), https://www.okta.com/blog/2020/06/data-misuse.

[210] Sue Milton, *Data Privacy vs. Data Security*, *in* GLOBAL BUSINESS LEADERSHIP DEVELOPMENT FOR THE FOURTH INDUSTRIAL REVOLUTION 209, 234 (Peter Smith & Tom Cockburn eds., 2021).

entities—often commercial banks, payment companies, and other financial institutions—have a financial incentive to monetize user data.[211] The more complete the user profile, the higher the potential for harm if the data is misused or abused. Moreover, these intermediaries may share this data with third parties, either intentionally for business reasons or unintentionally due to security lapses, thus heightening the risk of data misuse or abuse. Tracing the source of such misuse becomes increasingly complicated as more entities are involved in handling the data.

The increased cybersecurity risks result from the fact that each intermediary employs its own cybersecurity measures, which may vary in different levels of robustness. Entities with weaker security protocols become potential vulnerabilities, more susceptible to cyberattacks. While the two-tier model expands the number of potential targets for attack, the scope of damage may be comparatively limited, as attackers can typically only access the data stored by one specific intermediary. In contrast, the one-tier model centralizes all data within the central bank, making it a potentially more lucrative target for attackers as they can obtain a larger set of data in a single breach.

Some might argue that the two-tier model is similar to the existing payment systems,[212] where commercial banks, other financial institutions, and technology providers collect end users' data as long as end users use their products or services. Having one more party, i.e., 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 consumer-facing tasks 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 utilize its products or services or communicate with it. 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 holding a copy of retail holdings reintroduces the problem that arose under the one-tier

---

[211] OLIVER WYMAN, WORLD ECON. F., THE APPROPRIATE USE OF CUSTOMER DATA IN FINANCIAL SERVICES 9 (2018), https://www.dowjones.com/professional/risk/glossary/anti-money-laundering/kyc-vs-aml.

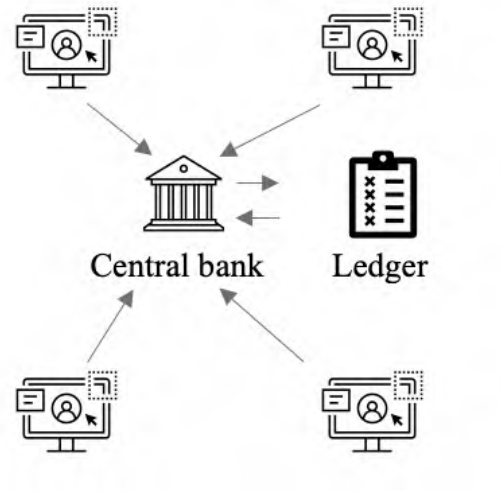
[212] Auer & Böhme, *supra* note 29, at 88.

model—mass surveillance, cybersecurity risks, and potential data misuse and abuse.

B. *Infrastructure*

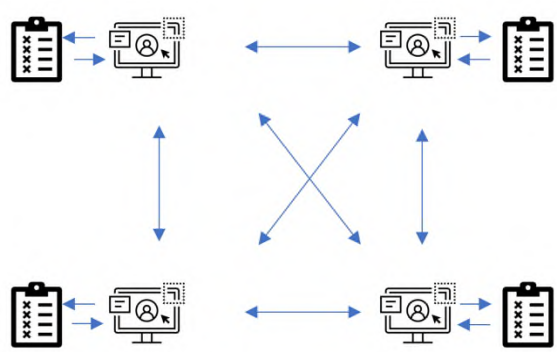
Infrastructure refers to the ways of recording and sharing data. A central bank has two options for recording transactions and updating credit and debit information: a centralized ledger system (Figure 4) and a DLT system (Figure 5).[213] It is important to note that a DLT is still not a wholly decentralized system. 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 partially centralized because the central bank makes the 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 Ledger System



[213] *Id.* at 91–92.

Figure 5: DLT System



A centralized system refers to transactions managed by a single player, which is the central bank in this case.[214] The central bank controls the system and its contents, that is, which transactions get posted to a central ledger.[215] 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.[216] 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.[217] 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.[218] One intermediary does not have access to a ledger held by other intermediaries.[219] In other words, ledgers held by all intermediaries are not synchronized.[220]

DLT refers to the processes and technologies that enable participants[221] in a network "to securely propose, validate[,] and record

---

214 *See id.* at 91–92.

215 *See id.* at 92.

216 *See id.*

217 *See id.*

218 Auer & Böhme, *supra* note 29, at 92.

219 *See id.*

220 *See id.*

221 Technically speaking, "participants" refers to nodes. This Article uses 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. Ayushi Abrol, *What Are Blockchain Guides?*, BLOCKCAIN COUNCIL (Sept. 27,

state changes . . . to a synchronized ledger that is distributed across the network's [participants]."[222] Essentially, DLT is a distributed method for documenting and disseminating information, and a distributed ledger represents a digital data log that is shared among several participants.[223] DLT uses a consensus mechanism[224] to ensure the accuracy of the data on the ledger. In the context of payment, 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."[225] 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.

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

---

2023), https://www.blockchain-council.org/blockchain/blockchain-nodes/#:~:text=Blockchain%20nodes%20are%20network%20stakeholders,network%20transactions%2C%20known%20as%20blocks. 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.

[222] COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENT, CLEARING AND SETTLEMENT: AN ANALYTICAL FRAMEWORK 2 (2017) (emphasis removed), https://www.bis.org/cpmi/publ/d157.pdf.

[223] Barr et al., *supra* note 39, at 1–2; *see also* César A. Del Río, *Uso de la tecnología de contabilidad distribuida por los bancos centrales: Una revisión* [*Use of Distributed Ledger Technology by Central Banks*], ENFOQUE UTE, Dec. 17, 2017, at 1–13, http://scielo.senescyt.gob.ec/pdf/enfoqueute/v8n5/1390-6542-enfoqueute-8-05-00001.pdf.

[224] SIGRID SEIBOLD & GEORGE SAMMAN, CONSENSUS: IMMUTABLE AGREEMENT FOR THE INTERNET OF VALUE 1 (2016), https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf ("Consensus mechanism: [a] method of authenticating and validating a value or transaction on a [b]lockchain or a distributed ledger without the need to trust or rely on a centralized authority."); *see, e.g.*, ROBBY HOUBEN & ALEXANDER SNYERS, CRYPTOCURRENCIES AND BLOCKCHAIN: LEGAL CONTEXT AND IMPLICATIONS FOR FINANCIAL CRIME, MONEY LAUNDERING AND TAX EVASION 18 (2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (describing "consensus mechanism" in a variety of ways).

[225] COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, *supra* note 222, at 2; Auer & Böhme, *supra* note 29, at 92; *see also* Mohammad Jabed Morshed Chowdhury et al., *A Comparative Analysis of Distributed Ledger Technology Platforms*, 7 IEE ACCESS 167930, 167934 (2019), 10.1109/ACCESS.2019.2953729.

related to the payor'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 payor 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 flow from end users to intermediaries, and intermediaries verify such data and update the ledger they hold, but they 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 inherent to the centralized system under the one-tier model is, again, that the central bank possesses an enormous amount of end-user data as it has to update every single transaction made by the end users. This recalls the concerns discussed above: mass surveillance, cybersecurity risks, and data misuse and abuse.[226] The centralized system under the two-tier model introduces an additional layer of privacy concerns. Because intermediaries must update transactions of their respective end users, the potential for data misuse or abuse by these intermediaries heightens. While cybersecurity threats leading to data breaches or privacy loss exist for the intermediaries, these threats may not necessarily affect end users associated with other intermediaries. Thus the privacy concerns and potential harms could be limited to a smaller scale.

In a DLT 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 must authenticate Entity A's identity 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 see the data in order to take part in the consensus process. Third, after the consensus process

---

[226] *See* discussion *supra* Part III.A.

where all participants agree on the transfer of funds, the ledger updates, and $100 is added to Entity B's account. All participants share the data on the ledger's latest balance.

The privacy concern with a DLT system centers on its ability to grant extensive access to data, subsequently amplifying the potential for compromising data integrity. Intermediaries, such as commercial banks and various payment service providers, can access a complete set of CBDC data if they have the central bank's authorization to update the ledger. Every intermediary in this network possesses a copy of the synchronized ledger, which escalates the threats of data misuse or abuse. A breach at a single intermediary's end can expose the entire CBDC dataset. This contrasts with the centralized system in the two-tier model, where intermediaries only hold data specific to their users. In such a setup, an attack's impact would be limited to those users. But, in a DLT system, a breach affects all end users. Therefore, having more participants (intermediaries) in the DLT network makes privacy protection harder.

It is often asserted that in the DLT system, the actual identities of transacting parties could be concealed, with network participants only viewing addresses comprised of a list of random numbers and letters.[227] Indeed, this pseudonymous approach obscures the direct identities of both payor and payee, thus preserving privacy. This is arguably true when considering isolated or infrequent transactions. In such cases, even if a lot of network participants view a transaction associated with a given address, it might be challenging to infer concrete details about the involved parties. But, as transactional activity amplifies, discerning the individual behind a given address becomes more feasible. This is particularly true when an address consistently exhibits unique transactional patterns, such as consistently sending a specific amount at regular intervals. Companies, like Chainalysis, carved a niche in de-anonymizing transactions within the DLT ecosystem.[228] With universal access and scrutiny of transactional data by network participants, pseudonymity alone cannot fully mitigate privacy concerns.

---

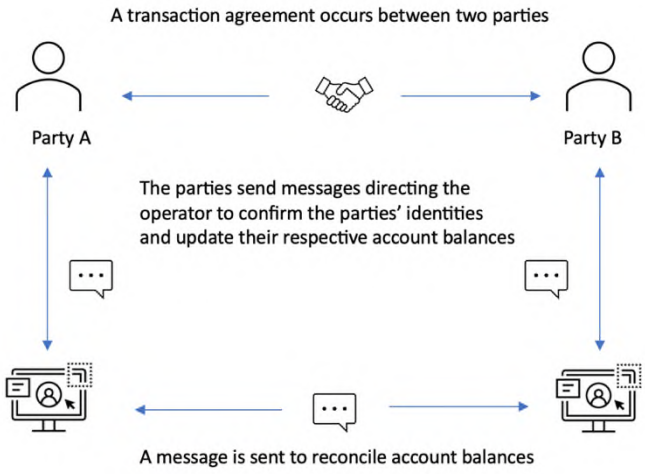
[227] WORLD BANK GRP., DISTRIBUTED LEDGER TECHNOLOGY (DLT) AND BLOCKCHAIN 8 (2017), 10.1109/ACCESS.2019.2953729.

[228] *Is Bitcoin Traceable?*, CHAINALYSIS (Apr. 11, 2022), https://www.chainalysis.com/blog/is-bitcoin-traceable.

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."[229] 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.[230] 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 verifying the identity of the payer, while a token-based system requires verifying the validity of the object used to pay."[231]

Figure 6: Account-Based Model[232]



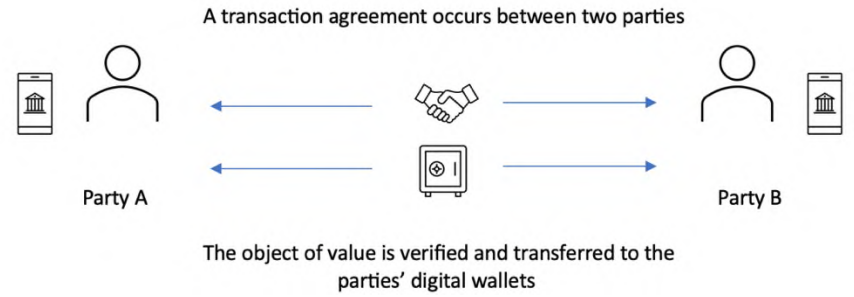
[229] Auer & Böhme, *supra* note 29, at 93; *see also* DIGIT. DOLLAR FOUND., *supra* note 137, at 20.

[230] *See* Baer, *supra* note 193, at 6.

[231] Garratt et al., *supra* note 190; *see also* Charles M. Kahn & William Roberds, *Why Pay? An Introduction to Payments Economics*, 18 J. FIN. INTERMEDIATION 1, 6 (2009). For a distinction between account-based and token-based model, see Charles M. Kahn et al., *Should the Central Bank Issue E-money?* 8 (Bank of Can., Working Paper No. 58, 2018), https://www.bankofcanada.ca/wp-content/uploads/2018/12/swp2018-58.pdf; Auer & Böhme, *supra* note 29, at 86; BENOÎT CŒURÉ & JACQUELINE LOH, BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES 4 (2018), https://www.bis.org/cpmi/publ/d174.pdf.

[232] DIGIT. DOLLAR FOUND., *supra* note 137, at 17.

Figure 7: Token-Based Model[233]



The account-based model fundamentally depends on the ability to verify the account holder's identity.[234] It "follow[s] the conventional account model and tie[s] ownership to an identity."[235] Transactions are authorized via identification. Under this model, individuals hold accounts with the central bank, and "transactions are recorded as new entries on a centralized ledger."[236] The holder of an account can ask to move funds to another account holder, and in response, the central bank would update its central ledger as a settlement.[237] 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)."[238] 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, Party B only needs to worry about whether the $100 bill is 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

---

233 *Id.*

234 CŒURÉ & LOH, *supra* note 231, at 4.

235 Auer & Böhme, *supra* note 29, at 93.

236 Barr et al., *supra* note 39, at 3.

237 *Id.*; *see also* MANCINI-GRIFFOLI ET AL., *supra* note 2, at 8.

238 DIGIT. DOLLAR FOUND., *supra* note 137, at 17.

through a central bank clearing system, Party B must verify that this physical object is genuine and Party A's identity is not Party B's concern.

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.[239] Party B does not need to know anything about Party A. The transaction happens between two wallets instead of two accounts. Wallets do not physically store digital currencies.[240] Rather, each wallet possesses a private key linked to an address within the network, representing the amount of tokens the wallet owner holds.[241] These wallets can be in the form of websites, mobile applications, or dedicated hardware devices.[242]

While it is very common to make a distinction between account-based and token-based systems,[243] from a practical point of view, such a distinction is problematic and sometimes inconsistent.[244] Many computer science professionals think the distinction is meaningless and irrelevant when it comes to cryptocurrencies and other revolutionary electronic payment methods.[245] One of the biggest issues with this distinction explains the "[u]se of the token-based and account-based terminologies . . . does not create mutually exclusive categories."[246] For example, BTC and many other digital currencies can satisfy both categories:

> [BTC] fits the definition of an account-based system. The account is a [BTC] address, and the private key is the proof of identity needed to transact from that account. Every time a [BTC] user wants to spend [BTC], that user must verify their identity by using their private key. . . . [BTC] also fits the definition of a token-based system. When someone wants

---

239 CŒURÉ & LOH, *supra* note 231, at 4.

240 Nikhil Sridhar & Patrick Horan, *Should Central Banks Offer the Public Token-Based Digital Currencies?*, DISCOURSE (June 8, 2021), https://www.discoursemagazine.com/economics/2021/06/08/should-central-banks-offer-the-public-token-based-digital-currencies.

241 *Id.*

242 *Id.*

243 *See* CŒURÉ & LOH, *supra* note 231, at 4; Kahn & Roberds, *supra* note 231, at 6; MANCINI-GRIFFOLI ET AL., *supra* note 2, at 8; Auer & Böhme, *supra* note 29, at 88; Sridhar & Horan, *supra* note 240.

244 Garratt et al., *supra* note 190.

245 *Id.*

246 Garratt et al., *supra* note 190; *see also Bitcoin is an Account, Not a Token*, THE BLOG OF JP KONING (Aug. 18, 2020), http://jpkoning.blogspot.com/2020/08/bitcoin-is-account-not-token.html.

> to spend a [BTC], 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.[247]

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 payor and payee's identities 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 must verify the transaction history of the "object" being transferred.[248] Therefore, at the deepest levels of computer architecture, the distinction makes no sense.[249] The distinction remains relevant probably because it helps nonexperts to understand the revolutionary technology or product by referring to something that already exists or of which people have knowledge.[250]

That is also why this Article argues 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.

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. 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 the national money supply: issuing

---

247 Garratt et al., *supra* note 190 (arguing BTC is not a token).

248 *See* CŒURÉ & LOH, *supra* note 231, at 4.

249 *See* Kahn & Roberds, *supra* note 231, at 11.

250 *See id.*

currency and setting interest rates on loans and bonds.[251] In this way, they manage monetary policy to guide the country's economy and achieve economic goals, such as full employment.[252] Second, they regulate member banks through capital requirements, reserve requirements, and deposit guarantees, among other tools.[253] They also provide loans and services for a nation's banks and its government and manage foreign exchange reserves.[254] Third, a central bank also acts as an emergency lender to distressed commercial banks and other institutions, and sometimes even the government.[255] For instance, by purchasing government debt obligations, the central bank provides a politically attractive alternative to taxation when a government needs to increase revenue.[256]

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.

---

[251] *What Is a Central Bank?*, EUR. CENT. BANK (July 10, 2015), https://www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/what-is-a-central-bank.en.html.

[252] *Id.*

[253] Simon Gray, *Central Bank Balances and Reserve Requirements* 9 (Int'l Monetary Fund, Working Paper No. 11/36, 2011), https://www.imf.org/external/pubs/ft/wp/2011/wp1136.pdf.

[254] *Id.* at 8.

[255] Andrew Sheng, *Role of the Central Bank in Banking Crisis*, *in* THE EVOLVING ROLE OF CENTRAL BANKS 193, 198 (Patrick Downes & Reza Vaez-Zadeh eds., 1991), https://doi.org/10.5089/9781557751850.071.

[256] *See id.* at 211.

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.[257] "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."[258] 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."[259] The Bank of Canada stated that "[f]or 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."[260]

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.[261] Second, DLT faces scalability challenges.[262] Consensus algorithms and cryptographic verification introduce latency and limit the number of transfers that DLTs can process currently, whereas existing payment clearing and settlement

---

[257] Del Río, *supra* note 223, at 2; GARRICK HILEMAN & MICHEL RAUCHS, CAMBRIDGE CTR. FOR ALT. FIN., GLOBAL BLOCKCHAIN BENCHMARKING STUDY 92 (2017), https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternativefinance/downloads/2017-09-27-ccaf-globalbchain.pdf.

[258] Del Río, *supra* note 223, at 1.

[259] Balazs Koranyi & Catherine Evans, *Blockchain Immature for Big Central Banks, ECB and BOJ Say*, REUTERS (Sept. 6, 2017, 12:47 PM), https://www.reuters.com/article/usblockchain-ecb/blockchain-immature-for-big-central-banks-ecb-and-boj-sayidUSKCN1BH2DH.

[260] JAMES CHAPMAN ET AL., BANK OF CAN. FIN. SYS. REV., PROJECT JASPER: ARE DISTRIBUTED WHOLESALE PAYMENT SYSTEMS FEASIBLE YET? 1 (2017), http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.

[261] David Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement* 23 (Fed. Rsrv. Bd. Fin. & Econ. Discussion Series, Working Paper No. 2016-095, 2016), https://doi.org/10.17016/FEDS.2016.095; *see also* Del Río, *supra* note 223, at 8; Baer, *supra* note 193, at 6.

[262] Jonathan Clark, Understanding Scalability in Distributed Ledger Technology 3 (2019) (Ph.D. dissertation, University of Cape Town), https://open.uct.ac.za/server/api/core/bitstreams/ad7ff1bb-99ab-4b28-9e9d-085e0ebfc619/content.

systems can process "hundreds of millions of transactions daily."[263] "Additionally, ledgers that add transactional histories on top of one another, such as blockchains, may challenge storage capacity over time."[264] 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.]"[265]

Therefore, a two-tier, centralized CBDC currently appears to be the most feasible and realistic option. But, from a privacy standpoint, the two-tier setup allows intermediaries to access a subset of the CBDC data, amplifying concerns about data exploitation, misuse, and vulnerability to cyberattacks. If the central bank retains a copy of retail balance sheets without clear rules on data sharing with other governmental bodies or third parties, it increases concerns about mass surveillance and potential data misuse by the central bank and associated government agencies. Additionally, the centralized nature of the system, housing vast amounts of high-value financial data, further magnifies its susceptibility to cyberattacks.

The next question is whether central banks can come up with solutions to mitigate these privacy concerns within this design. Part IV proposes a series of fundamental principles for the creation of a privacy-preserving CBDC.

IV. PRIVACY PRINCIPLES FOR A CBDC

Part III argues that what is considered private in the CBDC context is a normative assessment and should account for the values and cultures of each jurisdiction. As a result, privacy rules could vary by jurisdiction. Instead of suggesting a set of universal privacy rules for CBDCs for all jurisdictions to adopt, this Part will provide a few privacy-preserving principles for jurisdictions to consider when designing CBDCs to meet their respective privacy needs.

These guiding principles can serve as a reference framework and starting point from which central banks could identify a range of privacy needs of interest to all stakeholders. The principles are neither comprehensive nor exhaustive, nor do they address every possible privacy-related need. Some jurisdictions may want to adopt more detailed criteria or additional principles that meet the unique privacy

---

263 Del Río, *supra* note 223, at 9.

264 Mills et al., *supra* note 261, at 22.

265 Del Río, *supra* note 223, at 8–9 (citation omitted).

needs of their stakeholders. It is also worth noting that the scope of these principles only focuses on creating a privacy-preserving CBDC but does not address other policy goals such as improving financial inclusion, reducing transaction costs, and enabling frictionless cross-border payments.

As elaborated below, the framework begins by explicitly recognizing the need for privacy protection in a CBDC system. Next, it introduces PbD, a key principle that each jurisdiction can follow. In the context of CBDCs, PbD first requires a clear design of the roles of key players in CBDC systems: central banks and intermediaries that can directly affect the privacy landscape. Properly designing their roles helps anticipate and prevent privacy-invasive events. To embed privacy into the architecture of CBDC systems, PbD requires a suitable technological design using technology that can provide privacy protection at the foundational level. Finally, the CBDC system should follow the user-centered principle because individual users have the greatest vested interest in the management of their personal data.

A. *Legal and Regulatory Recognition of Privacy*

At the outset, it is crucial to underline the importance of privacy in every CBDC system. Whichever design choices a central bank may adopt, privacy must always be at the forefront of considerations. Academic studies extensively highlighted the significance of privacy. Numerous policymakers and central banks acknowledged the crucial role of privacy and called for privacy protection in CBDC systems.[266]

Even so, this Article continues to stress the importance of privacy from the very beginning, as it serves as the bedrock upon which other principles are built. Recognizing the centrality and significance of privacy in a CBDC system is a prerequisite for the successful implementation of other privacy-centric principles, like PbD. While jurisdictions might differ on specific privacy nuances in CBDC practices and the optimal degree of privacy, there should be unanimous agreement that privacy acts as a foundational principle in the CBDC system.

Highlighting the significance and necessity of privacy can be effectively achieved through its acknowledgement in policy, legal, and regulatory frameworks. While policymakers in many jurisdictions have done an excellent job in recognizing the need for privacy,[267] there remains a gap in its legal and regulatory recognition.

---

[266] *See* discussion *supra* Part III.

[267] *See* discussion *supra* Part I.

The three most relevant bodies of law are central bank laws, monetary laws, and privacy and data protection laws. Central bank laws decide if a central bank has the authority to issue a digital currency.[268] If so, central bank laws can, for example, require that the currency in digital form should be privacy preserving when authorizing the creation of central bank liabilities and the issuance of the currency in digital form. Monetary laws decide if a CBDC could be a currency (a means of payment, a medium of exchange, and a unit of account) in a jurisdiction.[269] If so, monetary law can further require that to qualify as currency, a CBDC design should adopt measures to ensure user privacy. Finally, privacy and data protection laws, which directly address privacy-related issues, would be the easiest ones to provide legal recognition. In many jurisdictions, the laws already provide legal and regulatory recognition by applying privacy and data protection laws to regulating digital transactions and payments.

B. *PbD*

The second principle to design a privacy-preserving CBDC is to follow the PbD approach. Dr. Ann Cavoukian developed the PbD concept in the 1990s, aiming to "address the ever-growing and systemic effects of [i]nformation and [c]ommunication [t]echnologies, and of large-scale networked data systems."[270] In the PbD perspective, the "future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."[271] Cavoukian defines PbD:

> [C]haracterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to prevent them from occurring. In short, [PbD] comes before-the-fact, not after.[272]

---

[268] Wouter Bossu et al., *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations* 13–14 (Int'l Monetary Fund, Working Paper No. 20/254, 2020), https://www.imf.org/en/Publications/WP/Issues/ 2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827.

[269] *See id.* at 5.

[270] ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 1 (2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[271] *Id.*

[272] *Id.* at 2 (emphasis omitted).

Another key element of PbD is that privacy should be "approached from a 'design-thinking' perspective—namely, a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, innovative, and inspiring."[273] Privacy must be incorporated into networked data systems and technologies by default.[274] Privacy must become integral to the design process and it should be embedded into every standard, protocol, and process that touches our lives.[275]

This Article applies Cavoukian's theory of PbD to the design of privacy practices in the CBDC system. Contextually, PbD in the CBDC system requires two critical actions: (1) a clear design of the roles of central banks and intermediaries in the CBDC system and (2) a definitive technology plan to facilitate a privacy-preserving CBDC.

1. Roles of Central Banks and Intermediaries

Clear articulation of the roles of central banks and intermediaries can help anticipate privacy-invasive events. Design options related to the roles of central banks and intermediaries significantly affect the privacy landscape and create various privacy issues.[276] For instance, the one-tier operational design and the centralized system both place the central bank at "the center of the universe." These two designs share the same privacy issue—mass surveillance and data misuse or abuse—because the central bank by default collects, stores, processes, and potentially uses all CBDC data. The two-tier operational design increases the chance of data leakage and data abuse and weakens end users' ability to control their data. The DLT design provides better privacy protection to some extent, but it also compromises data integrity. In summary, the involvement of central banks and intermediaries in the CBDC system directly influences the types of information these entities receive and further effectuates the privacy landscape.

A design in accordance with the discrete roles of these entities helps prevent privacy-invasive events from happening. With a clear understanding of the fact that various actors can pose different privacy issues, CBDC designers (or policymakers) can clearly articulate the roles of these entities in their designs to avoid certain disruptions to privacy. Providing privacy protection from the outset is a proactive and

---

[273] *Id.*

[274] *Id.*

[275] *See id.* at 3.

[276] *See* discussion *supra* Part III.

preventative measure. For instance, a one-tier operational design could result in mass surveillance and data abuse.[277] If a jurisdiction wants to avoid this risk, CBDC designers can either place intermediaries in the CBDC system and have the central bank keep a wholesale copy (which becomes a two-tier system) or adopt certain privacy-preserving technologies that allow the central bank to see only limited data while maintaining functionality—this way privacy disruptions can be addressed at the design stage.

In designing the roles of these entities, each jurisdiction can have criteria based on its values, culture, and needs. The question of design is part of a bigger question: What information should be considered private? Again, the answer also relies on a normative assessment. This Article does not intend to define which roles central banks or entities should play, and it argues this is a decision CBDC designers should make in the first place to avoid privacy disruptions.

2. Technological Design

In the context of CBDCs, PbD also requires a deliberate technological design. Privacy-preserving technologies should be intentionally embedded into the architecture of the CBDC system, not bolted on as an extra layer. Privacy should be an essential component of the core design and the functionality that CBDCs deliver.

Privacy embedded into the CBDC system can provide the foundational layer of privacy protection. Some may argue that existing privacy laws, such as the EU's General Data Protection Regulation,[278] provide various levels of privacy protection.[279] In the United States, some states have enacted privacy laws to provide certain degrees of privacy protection, California's Consumer Privacy Act[280] and Virginia's Consumer Data Protection Act;[281] sectoral laws such as the Gramm-

---

277 *See* discussion *supra* Part III.

278 *The General Data Protection Regulation*, EUR. COUNCIL: COUNCIL OF THE EUR. UNION, https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=The%20GDPR%20establishes%20the%20general,data%20processing%20operations%20they%20perform (Sept. 1, 2022).

279 GIULIA FANTI & NADIA POCHER, ATL. COUNCIL, PRIVACY IN CROSS-BORDER DIGITAL CURRENCY: A TRANSATLANTIC APPROACH 2 (2022), https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf.

280 CAL. CIV. CODE §§ 1798.100–.199 (West 2018).

281 VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2021).

Leach-Bliley Act[282] in the financial sector; and the Health Insurance Portability and Accountability Act[283] in the healthcare sector. It is true that privacy protection in some form exists within various legal and regulatory frameworks, but these laws and regulations offer secondary protection rather than protection at the foundational level.

A foundational layer of protection (i.e., privacy embedded directly into the CBDC system) can protect privacy more efficiently than secondary protection (ex post legal and regulatory protection) can. This is because privacy protection through design identifies and addresses privacy issues before the system begins to run and can potentially mitigate or avoid loss of privacy. Although some legal or regulatory requirements, such as notice requirements and "opt-in" options, are also ex ante mechanisms to prevent privacy violations, these requirements still lag behind the first layer of protection present when privacy has been a part of a system's design from its inception.

Ex post mechanisms such as punitive damages or injunctions are not ineffective; they are certainly helpful because punishment and deterrence can reduce future privacy violations. Instead, this Article argues that ex post and ex ante mechanisms are two sides of the same coin—both are very necessary and important. Among the ex ante mechanisms, spotting and addressing potential privacy issues as early as possible can reduce privacy violations more effectively in the first place. In that sense PbD offers better privacy protection than other legal or regulatory ex ante mechanisms do. In addition, by addressing potential privacy violations in a system's design, PbD can reduce the burden on ex post remedies and save victims the time and expense of going to court.

Many privacy-preserving technologies specifically protect privacy in the payment area. For instance, David Chaum founded a research stream on e-cash that aims to develop cryptography-based payment systems that are private by design and make payments untraceable.[284] He proposed a design in which users exchange their received digital banknotes for new ones in a compulsory interaction with a trusted payment service provider.[285] Chaum used blind signatures to unlink

---

[282] *Gramm-Leach-Bliley Act*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act (last visited Sept. 23, 2023).

[283] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL AND PREVENTION (June 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html.

[284] *See* David Chaum, *Blind Signatures for Untraceable Payments*, *in* ADVANCES IN CRYPTOLOGY: PROCEEDINGS OF CRYPTO 82, at 199, 199 (David Chaum et al. eds., 1983).

[285] *Id.* at 202.

the spending and receiving of a specific banknote.[286] Although blind-signature technology is not perfect (e.g., although the sender remains anonymous, the receiver is identified by their bank), it is a good experiment on integrating privacy design into the system and prioritizing privacy as an essential component of a system's core design and functionality.

Another technology that could be helpful in delivering privacy protection in the CBDC system is ZKP. The ZKP approach enables "one party (the prover) to prove to another (the verifier) that a [given] statement is true, without revealing any [additional] information" apart from the fact that the statement is indeed true.[287] "For [instance], given the hash of a random number, the prover could convince the verifier that . . . a number with this hash value [indeed exists], without revealing what [the number] is."[288]

Bontekoe proposed the use of ZKP to allow fully private transactions with the possibility of person-related monthly turnover or transaction limits.[289] But, this approach contradicts AML and CFT regulations.[290] In the context of CBDCs, AML and CFT are still very necessary. Regulators and central banks have repeatedly claimed that reconciling full privacy with regulatory constraints is not possible.[291]

To that end, Gross et al. presented a "holistic approach for a privacy/compliance-by-design CBDC" with ZKP.[292] Simply put, they use commitments and nullifiers to obfuscate transfers so transfers are not linkable.[293] "[A]ll end users [can] privately register and maintain their . . . private CBDC account[s]."[294] End users "only send

---

[286] *Id.* at 202–03.

[287] *What Are Zk-SNARKs?*, ZCASH, https://z.cash/technology/zksnarks (last visited Sept. 23, 2023).

[288] *Id.*

[289] Tariq Bontekoe, Balancing Privacy and Accountability in Digital Payment Methods Using zk-SNARKs 5 (Oct. 2020) (MSc thesis, University of Twente), http://essay.utwente.nl/83617/1/Bontekoe MA EEMCS.pdf.

[290] Gross et al., *supra* note 32, at 14.

[291] HANNA ARMELIUS ET AL., SVERIGES RIKSBANK, ON THE POSSIBILITY OF A CASH-LIKE CBDC 4 (2021), https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf; Raphael Auer & Rainer Böhme, *Central Bank Digital Currency: The Quest for Minimally Invasive Technology* (Bank for Int'l Settlements, Working Paper No. 948, 2021), https://www.bis.org/publ/work948.pdf.

[292] Gross et al., *supra* note 32, at 14 (emphasis omitted).

[293] *Id.* at iii.

[294] *Id.*

cryptographic proofs of the correct local accounting and compliance with the imposed limits [of] the ledger that . . . the central bank [maintains]."[295] The central bank only accepts a transfer proposal "if the ZKP rightfully proves" it complies with the imposed limits.[296]

Similarly, Karl Wüst et al. also designed a CBDC system called Platypus to provide strong privacy protection using Zerocash, a novel form of ZKP.[297] The system "assume[s] an authority that is trusted for the integrity of the currency (e.g., double-spending protection) but is not trusted for privacy."[298] Platypus uses Zerocash to "provide[] anonymity for the sender and recipient as well as secrecy of the transaction amounts."[299]

But not all PETs are mature, and ZKP has its drawbacks. The purpose of this Article is not to propose the perfect technological design offering flawless privacy protection in the context of CBDCs; instead, this Article argues that certain technologies (although imperfect and occasionally in need of further improvement) can be an essential component of a system's core design and functionality and that privacy should be embedded into the CBDC design and architecture to protect privacy at the foundational level.

C. *User-Centered Design*

The last principle by which to design a privacy-preserving CBDC is that the design process should center on the user. "User-centered design (UCD) is an iterative design process in which designers focus on the users and their needs in each phase of the design process."[300]

---

[295] *Id.*

[296] *Id.*

[297] Karl Wüst et al., *Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy-Preserving Regulation*, *in* CS '22: PROCEEDINGS OF THE 2022 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 2947, 2947–2948 (2022), https://doi.org/10.1145/3548606.3560617.

[298] *Id.*

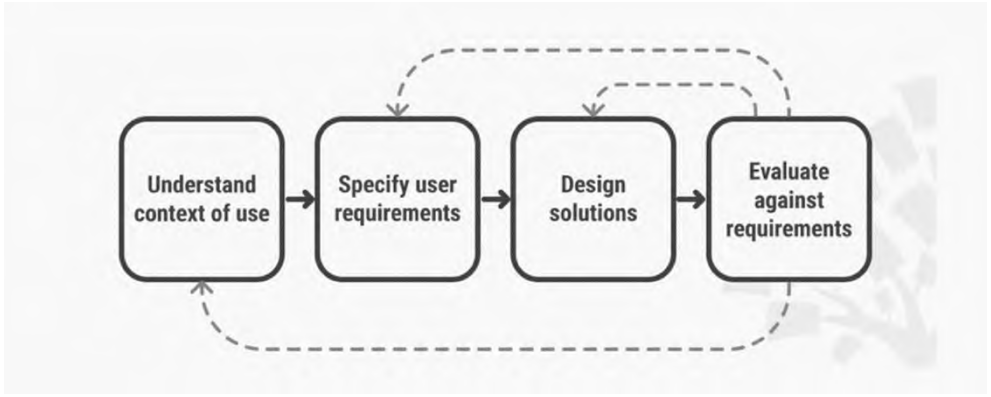
[299] *Id.*

[300] *User Centered Design*, INTERACTION DESIGN FOUND., https://www.interaction-design.org/literature/topics/user-centered-design (last visited Sept. 23, 2023). The term was coined in the 1970s and later Donald Norman (a cognitive science and usability engineering expert) adopted the term in his extensive work on improving what people experience in their use of items. The term rose in prominence thanks to works such as *User Centered System Design: New Perspectives on Human-Computer Interaction* (which Norman co-authored with Stephen W. Draper) and Norman's *The Design of Everyday Things* (originally titled *The Psychology of Everyday Things*). DONALD A. NORMAN & STEPHEN W. DRAPER, USER CENTERED DESIGN: NEW PERSPECTIVES ON HUMAN-

"In user-centered design, designers use a mixture of *investigative* methods and tools (e.g., surveys and interviews) as well as *generative* ones (e.g., brainstorming) to develop an understanding of user needs."[301] Generally, user-centered design involves four distinct phases:

> First, as designers [work] in teams, [they] try to understand the context in which users may use a system. Then [they] identify and specify the users' requirements. A design phase follows, in which the design team develops solutions. The team then proceeds to an evaluation phase. Here, [they] assess the outcomes of the evaluation against the users' context and requirements, to check how well a design is performing. . . . From here, [the] team makes further iterations of these four phases, and [they] continue until the evaluation results are satisfactory.[302]

Figure 8[303]



In the context of CBDCs and privacy, a user-centered design requires CBDC designers (i.e., central banks and other relevant authorities) to understand users' privacy needs before the design process. Designers can conduct public consultations, as the European Central Bank and the Federal Reserve have done, and interviews, in addition to using many other tools, to understand users' privacy needs and concerns if they have to use a CBDC.[304] If users require that their data not be shared with other entities except for entities directly

---

COMPUTER INTERACTION 15–16 (1986); DONALD A. NORMAN, THE DESIGN OF EVERYDAY THINGS (1990).

301 INTERACTION DESIGN FOUND., *supra* note 300.

302 *Id.*

303 *Id.*

304 MONEY AND PAYMENTS, *supra* note 16, at 2; *Digital Euro*, *supra* note 5.

handling the payments, then designers should accommodate this requirement by providing institutional and technological solutions in the design. If users are particularly concerned about state surveillance, designers may want to adopt a two-tier operational model instead of a one-tier model. Next, CBDC designers need to evaluate the CBDC design to see how closely the CBDC system matches the users' specific contexts and satisfies their needs. The process can repeat until the evaluation results are satisfactory. For instance, under the Biden Administration, the United States adopted a user-centered approach and is currently finalizing its first iteration of evaluation.[305]

The user-centered design approach is particularly important in designing a privacy-preserving CBDC. With close user involvement, a CBDC in a particular jurisdiction is more likely to meet users' privacy expectations and requirements, which fosters widespread adoption. Allowing users to play an active role before and during the CBDC design process is an effective check against abuses and misuses of their CBDC data and privacy. User participation also guarantees that informed privacy decisions may be reliably exercised.[306] In addition, "[p]utting designers in close contact with users [could foster] a deeper sense of empathy . . . . [which] is essential in creating ethical designs that respect privacy and the quality of life."[307]

CONCLUSION

This Article demystifies CBDCs by comparing CBDCs with other digital currencies and explain what motivates central banks to issue a CBDC. This Article adopts Daniel Solove's pragmatic approach and Helen Nissenbaum's contextual integrity theory to conceptualize privacy and investigate privacy problems that could occur in four CBDC designs. Finally, this Article proposes three legal and technical principles that central banks can follow if they decide to design a privacy-preserving CBDC: (1) legal and regulatory recognition of privacy, (2) privacy by design, and (3) user-centered design.

Again, the scope of this study is still limited. Although this Article discusses four of the most foundational design options, CBDC designs are far more granular and nuanced. Many design options at the

---

[305] *See* Exec. Order No. 14,067, 87 Fed. Reg. 14143 (Mar. 9, 2022); *see generally* OFF. OF SCI. & TECH. POL'Y, *supra* note 18.

[306] Awanthika Senarath et al., *Designing Privacy for You: A User Centric Approach for Privacy*, *in* HUMAN ASPECTS OF INFORMATION SECURITY, PRIVACY AND TRUST 739, 743 (Theo Tryfonas ed., 2017), https://doi.org/10.1007/978-3-319-58460-7_50.

[307] INTERACTION DESIGN FOUND., *supra* note 300.

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, 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. This Article intends to 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.


SETON HALL UNIVERSITY
HAZARD YET FORWARD
1856