Privacy Implications of Central Bank Digital Currency

Jiaying Jiang

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

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

Part of the Law Commons

Recommended Citation

54 Seton Hall L. Rev. (forthcoming)

This Article is brought to you for free and open access by the Faculty Scholarship at UF Law Scholarship Repository. It has been accepted for inclusion in UF Law Faculty Publications by an authorized administrator of UF Law Scholarship Repository. For more information, please contact jessicaejoseph@law.ufl.edu.
PRIVACY IMPLICATIONS OF CENTRAL BANK DIGITAL CURRENCIES

Jiaying Jiang

Table of Contents

INTRODUCTION .......................................................................................................................... 3

I. DEMYSTIFYING CBDCS ........................................................................................................ 9
   A. Understanding CBDCs ....................................................................................................... 9
   B. Motivations for issuing a CBDC ...................................................................................... 11
      1. External Pressure ......................................................................................................... 12
      2. Internal needs ............................................................................................................. 13
      3. Motivations unique to specific countries ................................................................... 15

II. CONCEPTUALIZING PRIVACY IN THE CONTEXT OF CBDCS ........................................ 17
    A. Existing Conceptions of Privacy .................................................................................... 17
    B. Pragmatic Approach ...................................................................................................... 19
    C. Contextual Integrity ...................................................................................................... 21
    D. Pragmatic Approach and Contextual Integrity in the Context of CBDCs .................... 22

III. PRIVACY ISSUES ARISING FROM VARIOUS CBDC DESIGNS .................................... 26
    A. Operational Model ......................................................................................................... 28
    B. Infrastructure ................................................................................................................ 30
    C. Verification Object? ....................................................................................................... 34
    D. One Unique Scenario .................................................................................................... 37

IV. PRIVACY PRINCIPLES FOR A CBDC ............................................................................. 40
    A. Legal and Regulatory Recognition of Privacy ............................................................... 40
    B. Privacy by Design ......................................................................................................... 41
       1. Roles of Central Banks and Intermediaries ................................................................. 42
       2. Technological Design ............................................................................................... 43
    C. User-Centered Design ................................................................................................ 45

CONCLUSION .............................................................................................................................. 46

Electronic copy available at: https://ssrn.com/abstract=4399409
PRIVACY IMPLICATIONS OF CENTRAL BANK DIGITAL CURRENCIES

Jiaying Jiang*

Abstract

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

However, when addressing the importance and preservation of privacy, all parties seem to overlook two very important issues: (1) What does privacy mean here? and (2) What privacy problems do CBDCs create? Before proposing solutions, one must understand which problems must be solved. In this article, I explore these two critical issues. I first adopt Daniel Solove’s pragmatic approach and Helen Nissenbaum’s contextual integrity theory to conceptualize privacy in the context of CBDCs. Next, I investigate the dataflow of four structural and foundational CBDC designs and conclude that each design will result in various potential privacy issues, including mass surveillance, misuse and abuse of CBDC data by central banks and intermediaries, and more. In the end, I propose three legal and technical principles as a reference framework for designing a privacy-preserving CBDC.

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

*Jiaying Jiang, Assistant Professor of Law, University of Florida Levin College of Law. I started this project when I was a Hauser Global Fellow at New York University School of Law, so I am grateful to many NYU Law colleagues for their early-stage feedback. Special thanks to Joseph Weiler, Grainne de Burca, Katherine Strandburg, Alexandre de Streel, Francesca Episcopo, David Stein, Thomas Streinz, Aniket Kesari, and Elettra Bietti. 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, for their excellent work on this project.
INTRODUCTION

Institutions around the globe define central bank digital currencies (CBDCs) differently. The Federal Reserve Bank defines a CBDC as “a digital liability of a central bank that is widely available to the general public.” The International Monetary Fund defines a CBDC as “a new form of money, issued digitally by the central bank and intended to serve as legal tender.” The Bank for International Settlements considers a CBDC “a digital form of central bank money that is different from balances in traditional reserve or settlement accounts” and that works as “a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank.” The European Central Bank envisions that CBDC could be an alternative to euro banknotes and could complement cash by serving as “an electronic form of money, issued by the Eurosystem, [that] would be accessible to all citizens and firms.”

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. 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. This paper will address only retail CBDCs because retail CBDCs directly involve individuals and raise the research questions of this paper.

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

---

4 Central Bank Digital Currencies: Foundational Principles and Core Features, supra note 3, at 3.
7 Id.
9 Id.
10 Id.
11 Id.
2021 in four member states and later expanded to three more. Nigeria also has a live retail CBDC.

In addition, 72 central banks have communicated publicly in positive tones about their CBDC work. China’s central bank is at a very advanced stage of experimenting with its CBDC, and it has run pilot programs in ten cities. The European Central Bank has issued a report on a digital euro that examines the issuance of a CBDC from the perspective of the Eurosystem. The Federal Reserve of the United States is still debating whether the United States needs a CBDC and has fostered a broad and transparent public dialogue about the potential benefits and risks of a US CBDC. The Federal Reserve Bank of Boston and MIT have tested the technology, publishing a report called Project Hamilton. 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. 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.

As central banks experiment with CBDCs and grapple with the ideal design of a CBDC, privacy has become one of the most prominent aspects of this development and a great concern they must consider and address. Major central banks have already addressed the importance of privacy. The European Central Bank conducted a public consultation on a digital euro. Both citizens and professionals participating in the consultation considered privacy the most important feature of a digital euro. The Federal Reserve emphasized that one key policy consideration when examining the pros and cons of a potential US CBDC is how to preserve the privacy of

---

12 Id.
14 Id.
21 Id. at 10. What the respondents want most from a digital euro is privacy (43%), security (18%), usability across the euro area (11%), the absence of additional costs (9%) and offline use (8%). The preference for privacy is also high among citizens of all ages but increases mildly with age: 39% of respondents under 35 years, 45% between 35 and 55 years and 46% of respondents aged 55 and over give the highest prominence to privacy.
citizens and maintain the ability to combat illicit finance. China’s central bank, the People’s Bank of China, has adopted strict compliance with regulations on data and privacy protection as a key principle of the institutional design of its CBDC system and has already moved forward with the design of “managed anonymity” to protect privacy and user information in its CBDC pilot program. The Bank of Canada has outlined what is technologically feasible for privacy in a CBDC and suggested a design approach for CBDC privacy.

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

Some economists, computer scientists, engineers, and legal scholars have already moved forward to design a CBDC with privacy protection. For instance, Sarah Allen et al. discussed from whom the CBDC should protect sensitive identity and/or transaction data. Jonas Gross et al. argued that a CBDC system should provide at least the same privacy-preserving features as cash in order

22 Board of Governors of the Federal Reserve System, supra note 17.
26 People should be able to use a U.S. CBDC without making themselves subject to undue corporate tracking or government surveillance. People may benefit from above-board, contractual sharing of information with financial services providers, or they may refuse it. Law enforcement access to CBDC usage data should be strictly controlled by due process, and other applicable U.S. law, including the Fourth Amendment. The Digital Dollar Project Privacy Sub-Committee, Privacy Principles for a Digital Dollar, Digital Dollar Project (Oct. 2021) https://digitaldollarproject.org/wp-content/uploads/2021/10/DDP-Privacy-Principles-10.25.21_Final.pdf.
28 Id.
29 Central Bank Digital Currencies: Foundational Principles and Core Features, supra note 3, at 6; see also Raphael Auer & Rainer Böhme, The Technology of Retail Central Bank Digital Currency, BIS Quarterly Review, 86 (Mar. 2020), http://ssrn.com/abstract_id=3561198 (They discuss different technical designs satisfy the criteria of safeguarding user privacy and allowing for effective law enforcement to varying degrees due to trade-offs associated with design choices. There is a trade-off between privacy and ease of access on one hand and ease of law enforcement on the other, with the associated design choice being whether access to the CBDC uses account-based technology or token-based technology.).
to secure access to a fully private, regulation-compliant form of money. They proposed a software-based CBDC that imposes limits on anonymous payments in order to support full privacy while addressing constraints related to anti-money laundering and countering the financing of terrorism; privacy and regulatory compliance can be provided by design. More specifically, they proposed using zero-knowledge proof to enable users to reveal their payment history to provide evidence for integrity and completeness without revealing personal or identifiable information. Nadia Pocher et al. proposed implementing privacy-enhancing technologies (PETs) to protect individual privacy by protecting data.

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

In this article, I address these two critical issues. I adopt Daniel Solove’s pragmatic approach 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 is to explore which aspects of these practices should be considered private and what other values to balance when recognizing and protecting the value of privacy in CBDC practices.

I argue, in the context of CBDCs, that privacy is not a separate abstract conception but a dimension of the practice of CBDC payments. Privacy is a part of payment practices. Payment practices include a 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 would be a violation of privacy. What should be considered private is a normative argument and may vary across jurisdictions, cultures, and times. When conducting normative analysis, it is necessary to balance the value of CBDC data privacy with other conflicting values.

32 Id. at 33.
33 Id.
Next, as a methodology for understanding what privacy problems would arise from various design choices, I first study the dataflow of four structural and foundational design choices. Following the dataflow, I investigate who could get access to what data. Each design varies in who can see, store, collect, and share CBDC-related data, which includes but is not limited to identity data and transaction data. Some data are encrypted, but some are not. All these factors contribute to potential disruptions in the practice of CBDC payment (i.e., privacy problems), including but not limited to state surveillance and the abuse and misuse of CBDC data by central banks and intermediaries.

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

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

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

Third, this paper enables intermediaries, especially commercial banks and other payment service providers, to navigate their roles in a world full of financial technology (fintech) innovations. Some ongoing fintech movements have been touting trustless infrastructure and peer-to-peer transactions with the goal of removing intermediaries. Such movements directly threaten commercial banks and other traditional financial institutions. CBDCs led by central banks present intermediaries with a new opportunity to strengthen their roles in the financial and payment markets. Due to policy considerations, central banks are highly unlikely to disintermediate these intermediaries but rather will likely work with them to issue CBDCs. This paper will also help intermediaries understand users’ privacy needs and choose a suitable CBDC design that meets those needs. By actively participating in CBDC designs and offering consumer-facing services, intermediaries will not only reinforce their roles and abilities in fintech movements but also improve their relationships with central banks and individuals.

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

---

36 Kumar et al., supra note 8.
instance, financial entities could constantly monitor and monetize users’ CBDC data, and the worst-case scenario is state surveillance.

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—such as mass surveillance or misuse and abuse of CBDC data by the central bank and intermediaries—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 of the financial services have been digitized, and consumers have less frequently used cash for payments. Consumers can use credit cards, debit cards, Venmo, Apply Pay, PayPal, and many other tools to pay for products or services, thanks to vibrant innovations in the FinTech space. 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? The section below answers these enquires.

A. Understanding CBDCs

Many kinds of money or payment tools exist in the payment market, such as commercial bank money, electronic money (e-money), and cryptocurrency.38 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.39 E-money is a digital store of a medium of exchange on a computerized device.40 E-money can be held on cards, devices, or on a server.41 Examples include prepaid cards, electronic purses such as M-PESA in Kenya, and web-based services such as PayPal.42 A

38 MANCINI-GRIFFOLI, ET AL., supra note 2.
39 Board of Governors of the Federal Reserve System, supra note 17.
41 Id.
42 Id.
cryptocurrency is a form of digital or virtual currency that is not denominated in fiat currency and uses cryptography to secure transactions. Popular cryptocurrencies include Bitcoins, Ethereum, and so on. A stablecoin is a type of cryptocurrency that attempts to peg their market value to some external reference, such as a reserve asset like the US dollar or gold, to reduce volatility.

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. 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. For instance, when one deposits money at the Bank of America (a commercial bank), one has a claim on the Bank of America, not the Federal Reserve. If one loses money, one can seek 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, 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. . . .” Also, e-money can have hybrid issuers—“service providers who issue e-money as an accessory activity to their core business, i.e., mobile phone companies, public transport companies, etc.” In contrast, a CBDC represents a claim on the central bank and the central bank is the sole issuer of its CBDC. Even if a central bank can authorize other entities to distribute CBDCs, these entities are distributors only, not an issuer.

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,

46 Id.
50 Id.
whereas a cryptocurrency or stablecoin is not.\textsuperscript{51} CBDCs serve as a legal tender, the legal implication of which is that one cannot reject CBDCs as a means of payment; however, one can refuse to accept Bitcoin, Tether, or other cryptocurrencies and stablecoins as a form of payment.\textsuperscript{52}

A CBDC is issued and guaranteed by a central bank with a centralized management system, whereas cryptocurrencies and stablecoins are issued and managed by a distributed network without a centralized agency. Some cryptocurrencies are run on blockchain, meaning they are managed by a group of unknown persons behind the computers across the globe.\textsuperscript{53}

Furthermore, the value of a CBDC is usually decided by the issuing central bank under the law. The value of cryptocurrencies such as Bitcoin and Ethereum is decided by the market, and the value is highly volatile.\textsuperscript{54} The value of stablecoins is designed to be more stable, as its name suggests, and is backed by collaterals, fiat currencies, or sometimes algorithms. However, there is no guarantee that stablecoins can remain stable.\textsuperscript{55} The recent Tether crash is a case in point.\textsuperscript{56}

Consumers may want to use CBDCs instead of other forms of money is because of the systemic importance of CBDCs. CBDC is a legal tender and backed by the full faith and credit of the government. A CBDC could be a safer form of payment than private digital currencies.\textsuperscript{57} The underlying theory is that central banks can always print money even when other financial institutions face bank runs in a financial crisis.\textsuperscript{58} Consumers can still have a claim on the central bank and will never lose their money.

\textbf{B. Motivations for issuing a CBDC}

Central banks’ experimentation and potential issuance of CBDCs are driven by both external pressure and internal needs. External pressure comes from the prevalent use of cryptocurrencies and the adoption of stablecoins in the payment sector.\textsuperscript{59} 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.\textsuperscript{60} In addition to these internal needs common to most central banks, some central banks have distinctive needs to meet. For instance, China probably wants to use its digital yuan to address the duopoly of Alipay and

\begin{footnotesize}

\textsuperscript{52} Kiff, \textit{supra} note 43, at 9.

\textsuperscript{53} Id.

\textsuperscript{54} MANCINI-GRIFFOLI, ET AL., \textit{supra} 2, at 13.


\textsuperscript{57} Chorzempa, \textit{supra} note 51.

\textsuperscript{58} Id.


\textsuperscript{60} CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, \textit{supra} note 3.
\end{footnotesize}
WeChat Pay in the payment market. The United States aims to maintain its leadership in the global financial system with a potential digital dollar. The European Union 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.

It is important to note that the session 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. However, 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. Instead, all of these reasons as a whole motivate central banks to consider issuing a CBDC.

1. External Pressure

The emergence and prevalent use of cryptocurrencies are raising pressures on central banks to develop their own digital currency. Cryptocurrencies, especially Bitcoin, have again triggered intense debate over who should control money in the future. The peer-to-peer payment system of Bitcoin has also urged the world to rethink the merits and drawbacks of existing centralized payment systems. Reformers have criticized the model of central bank authority in money issuance. Central banks have felt forced to rethink their role and the need to issue a CBDC to compete with cryptocurrencies. If commerce greatly shifts to the use of cryptocurrencies, governments risk losing control of their monetary policies, which are tools that the central bank uses to keep tabs on inflation and financial stability. Central banks need to create their own digital currency to maintain monetary inflation.

Cryptocurrencies like Bitcoin and Ethereum, while popular, are not the main threat. Because the value is extremely volatile, many investors (or speculators) stock it away rather than use it for payments. The underlying technology of Bitcoin (i.e., blockchain) faces scalability challenges; therefore, the blockchain network cannot complete large volumes of transactions that 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 electricity. Additionally, since cryptocurrencies are not centrally issued or controlled, it poses regulatory and law-enforcement challenges.
Compared to Bitcoin and Ethereum, stablecoins could pose a greater threat to central banks.\textsuperscript{70} As previously mentioned, the value of stablecoins is pegged into “stable” fiat currency or other reference assets, making it more suitable for a store of value and a medium of exchange. Although today’s stablecoins are primarily used to facilitate the trade of other assets, stablecoins could be more widely used in the future as a means of payment by households and businesses.\textsuperscript{71} In 2019, Meta’s (then Facebook’s) publication of the whitepaper on its stablecoin, Libra (whose name was changed to Diem in 2020),\textsuperscript{72} directly sped up central banks’ research and experiments in the CBDC space. With Diem’s 1.8 billion active daily users and its ability to provide payment services to 1.7 billion unbanked and underbanked populations, if Diem is widely adopted in a jurisdiction, especially in those developing economies, central banks would be at risk of losing authority on monetary matters. Therefore, stablecoin developments have pushed central banks to create their CBDCs as a response.

2. Internal needs

There are many internal reasons to explore CBDCs, and the motivations of different countries for issuing CBDCs depends on their economic situations. Some common motivations are: 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, specially in emerging economies.\textsuperscript{73} If designed properly, some of the CBDC features could help to improve financial inclusion. For instance, unbanked populations can still use CBDCs for daily transactions because CBDCs don’t 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. CBDCs interoperability with other payment systems can also bring the unbanked or underbanked population to the existing financial system. CBDCs’ cross-border potential could also help immigrants to send money from developed countries where they work to developing or underdeveloped countries where their families are located with very low transaction costs. CBDCs could also provide public access to central bank money, especially in jurisdictions where access to cash is in decline.\textsuperscript{74} CBDC could also be used for

\textsuperscript{70} President’s Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, supra note 44, at 8.

\textsuperscript{71} Id. at 1.


\textsuperscript{74} Central Bank Digital Currencies: Foundational Principles and Core Features, supra note 3, at 5.
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.75

Reducing costs associated with physical cash is also a primary motivation to adopt CBDCs for
both advanced and emerging market economies.76 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.77 The 2021 U.S. 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.78
Additionally, a decline in cash use also leads to an increase in the cost of accepting cash.79 A
CBDC could potentially cut back on some costs because digitalization eliminates the needs to
print, recycle or transport physical cash.

CBDC’s potential for discouraging illicit activities such as money laundering, terrorism
financing, and tax evasion also explains why central banks consider a CBDC. Anonymity of
transactions, especially with respect to high-denomination banknotes and cryptocurrencies,
greatly exacerbate illicit activities because transactions are untraceable. 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.80
CBDCs would also 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.81 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.82

CBDCs’ ability to facilitate efficient cross-border payment also motivates central banks in both
developing and developed economies. While emerging markets and developing economies
(EMDEs) generally are 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.83 These emerging economics believe CBDC can reduce long

75 Kiff et al., supra note 43, at 12.
76 Barontini & Holden, supra note 73, at 10; Boar, Holden & Wadsworth, supra note 73, at 4-5.
77 Kiff et al., supra note 43, at 12.
78 Id. at 34 (citing Currency and Bank Budgets, Federal Reserve, https://www.federalreserve.gov/foia/budgets.htm (last updated: May 6, 2022)).
79 Barontini & Holden, supra note 72, at 3 (citing SVERIGES RIKSBANK, THE RIKSBANK’S E-KRONA PROJECT –
REPORT 2 (Oct. 2018)).
80 Id. at 12.
Considerations, BROOKINGS 12 (2020), https://www.brookings.edu/research/design-choices-for-central-bank-digital-
currency-policy-and-technical-considerations/.
82 Id. at 12.
83 Boar & Wehrli, supra note 73, at 7.
transaction chains in cross-border payments. Advanced economies are heavily motivated to issue CBDCs because of the potential to allow for faster clearing and settlement between central banks and the potential to address limited operating hours of current payment systems. 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.

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. Many private payment systems benefit from strong network effects (benefits of aggregating data to provide additional services), which could result in monopolies, high barriers to entry, and high costs for merchants. CBDCs introduced by central banks could break the monopolies by introducing more actors into the payment market. On the other hand, fragmentation from many existing systems can increase cost and complexity of interoperability, so CBDCs could potentially address this issue by facilitating transfers between fragmented payment systems. These private payment systems do not internalize social costs of potential systemic operational failures, such as cyberattacks, leading them to underinvest in security. Further, a concentrated payment system market could result in private issuers providing lower quality services and commercializing user data. 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 the support of a government could have 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 duopoly of Alipay and WeChat Pay. Alipay and WeChat Pay control 55.1% and 38.9% of the mobile payment market, respectively, giving them a duopoly over trillions of dollars in mobile payments. This duopoly could create risks such as economic instability in the case of a disruption to the digital payment infrastructure or the bankruptcy of a private company. When citizens place large amounts of their money and financial assets in these services, there is a higher risk of disruption in the payment system.

---

85 Barontini & Holden, supra note 72, at 12; Boar, Holden & Wadsworth, supra note 72, at 5; Kosse & Mattei, supra note 84, at 8.
86 Kosse & Mattei, supra note 84, at 8.
87 Id. at 8.
88 CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, supra note 3, at 5.
90 CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES, supra note 3, at 5-6.
91 Id. at 5-6.
92 Kiff et al., supra note 43, at 12.
93 Id.
95 Jiang & Lucero, supra note 59, at 10.
money in Alipay or WeChat Pay wallets, commercial bank deposits get strained as money is drained out of the traditional banking system.\textsuperscript{96} By developing a CBDC, China’s central bank, People’s Bank of China (PBOC), can centralize clearing mechanisms and enhance its own control over digital currency to reduce autonomy of these companies, thus strengthening the PBOC’s supremacy and financial stability.\textsuperscript{97}

The United States is motivated to develop a US CBDC, or a digital dollar, to improve the safe and efficient domestic payment systems.\textsuperscript{98} Internationally, the United States also tried to explore if 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.\textsuperscript{99} Maintaining the United States’ position as a leader in the global financial system and in technological and economic competitiveness is also a key motivator for the United States to invest in payment innovations and digital assets.\textsuperscript{100} The United States is also motivated to stay at the forefront of developing digital assets such as CBDCs to set standards that promote democratic values, the rule of law, the protection of consumers, investors, and businesses, and interoperability with digital platforms, legacy architecture, and international payment systems.\textsuperscript{101} Additionally, the U.S. dollar and financial institutions play a role in the global financial system that confers economic and national security benefits, which the United States hopes to maintain through digital asset development.\textsuperscript{102}

In Europe, issuing a digital euro would support Europe’s drive toward continued innovation and support strategic objectives of the Euro system such as increasing choice, competition, and accessibility with regard to digital payments.\textsuperscript{103} As major foreign central banks issue CBDCs, the status of other international currencies could be enhanced at the expense of the Euro, which could motivate the European Union to issue a digital euro to support the international role of the euro and stimulate demand for the euro among foreign investors.\textsuperscript{104} An interoperable design of CBDCs across currencies would strengthen the euro’s international role and improve cross-currency payments without having to grant non-euro area residents access to the digital euro.\textsuperscript{105} 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.\textsuperscript{106}

Other countries, including The Bahamas, Jamaica, Eastern Caribbean (Saint Kitts and Nevis, Montserrat, Antigua and Barbuda, Dominica, Saint Lucia, Saint Vincent and the Grenadines, and...
Grenada) and Nigeria have launched CBDCs. In the Bahamas, an important motivator is the potential for faster recovery when natural disasters physically damage banks and ATMs. 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. While the Eastern Caribbean Central Bank (ECCB) launched its digital currency with the primary motivation of promoting financial inclusion, a country-specific concern that also motivated the development of digital currency is the need to expand banking across difficult terrains. 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 10 years.

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. However, before discussing how important privacy is and how to preserve privacy, the first question to ask should be: What does privacy mean here?

A. Existing Conceptions of Privacy

The notion of privacy is not consistent across the globe. Defining privacy has proven to be quite complicated, and many find it difficult to precisely define privacy. According to Julie Inness, the legal and philosophical discourse of privacy is in a state of chaos. Jurists, legal scholars, philosophers, psychologists, and sociologists appear to have a welter of different conceptions of privacy. 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. These headings include:

107 Kumar, et al., supra note 8.
109 Kumar, et al., supra note 8.
110 Id.
111 Id.
115 Solove, supra note 114, at 1092.
116 Solove & Schwartz, supra note 113, at 43.
“(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.”

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

Additionally, privacy is a deeply personal concept; individuals have their own barometer of what they consider private, including when and with whom their personal information can be shared. 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 telemarketers. In other words, people actually have largely matching

117 Solove, *supra* note 114, at 1087.
118 Solove, *supra* note 114, at 1094 (In Solove’s paper, he critiqued all six categories of conceptions and explained why each conception is either too broad or too narrow or both.).
119 Warren and Brandeis defined privacy as the “right to be let alone,” a phrase adopted from Judge Thomas Cooley’s treatises on torts in 1880. Cooley’s right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defining a right to privacy. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); See Robert E. Smith, BEN FRANKLIN’S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 128 (Chisheng Li ed. 2000).
121 Solove, *supra* note 114, at 1101.
124 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’
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

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

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

In line with this pragmatic philosophy, Solove’s pragmatic approach emphasizes the contextual and dynamic nature of privacy. It conceptualizes privacy in particular contexts rather than level of comfort in sharing information. This should put to rest the frequent insinuation that privacy preferences are personal and idiosyncratic.

---

126 Solove, supra note 114, at 1126.
127 Id. at 1127.
128 Id. at 1127. Pragmatists reject the view of philosophy “as a purely theoretical quest for eternal truths or knowledge of an ultimate and unchanging reality.” PRAGMATISM AND CLASSICAL AMERICAN PHILOSOPHY: ESSENTIAL READINGS AND INTERPRETIVE ESSAYS 3 (John J. Stuhr ed., 2000); see also John Dewey, Reconstruction in Philosophy, in 12 THE MIDDLE WORKS OF JOHN DEWEY 72 (Jo Ann Boydston ed., 1982); Many pragmatists go beyond making the epistemological claim that an ultimate or transcendent reality is not knowable. Some philosophers, observes John Dewey, “have not ventured to deny that [an ultimate reality] would be the appropriate sphere for the exercise of philosophic knowledge provided only it were within the reach of human intelligence.” Dewey, supra at 72. Dewey claims that philosophy is still possible by exploring knowledge gleaned from experience.
130 Solove, supra note 114, at 1126.
132 Id.
133 Solove, supra note 114 at 1126.
134 Id.
135 Id. at 1127.
privacy in the abstract. And it does not follow traditional accounts of privacy that seek to conceptualize privacy in general terms as an overarching category with necessary and sufficient conditions. Conceptualizing privacy is about understanding and attempting to solve certain problems. Solove contends that privacy problems involve disruptions to certain practices. By “practices,” he refers broadly to various activities, customs, norms, and traditions. Examples of practices include writing letters, talking to one’s psychotherapist, talking to one’s lawyer, engaging in sexual intercourse, and so on. Privacy is a dimension of these practices, and under this approach, privacy should be understood as part of these practices rather than a separate abstract conception.

“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.”

To understand practices and disruptions to practices properly, two additional concepts are particularly relevant: private matters and the value of privacy. Turning our focus from disruptions to the practices they disrupt, we often refer to aspects of these practices as “private matters.” In other words, we say that certain things, places, and affairs are “private.” Traditionally, one considers one’s house, one’s diary, one’s body, and one’s sexual behavior private. 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. Instead, privacy is embedded in activities or norms that are naturally borderless. In the digital world, one can consider one’s online photos, text messages, voice messages, emails, and investment portfolios private.

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

\[^{136}I d.\]
\[^{137}I d.\]
\[^{138}I d. \text{ at } 1129.\]
\[^{139}I d.\]
\[^{140}I d.\]
\[^{141}I d.\]
\[^{142}I d.\]
\[^{143}I d. \text{ at } 1127.\]
\[^{144}I d. \text{ at } 1131.\]
\[^{145}I d.\]
\[^{146}I d. \text{ at } 1132.\]
\[^{147}\text{Katrin Schatz Byford, } \text{Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment, } 24 \text{ Rutgers Computer & Tech. L.J. 1, 40 (1998).}\]
photos and messages would benefit many families suffering from losing their children or other loved ones. Society would be better off if such information were public (in other words, one person’s state of being private is violated or destroyed). The law should evaluate these conflicting values to decide if certain matters should be private.

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 information within informational norms or parameters.\(^{148}\) These parameters include: 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.\(^{149}\)

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, which provide the means to determine the informational norms associated with the activity being evaluated. Actors are the parties involved in an information exchange and are divided into three categories, although an actor may fill multiple roles simultaneously: the sender, the receiver, and the subject of the information.\(^{150}\) Attributes are the characteristics and content of the information being transmitted.\(^{151}\)

A transmission principle is a constraint on the flow of information from one actor to another within a specific context.\(^{152}\) Transmission principles are best understood as the expected characteristics 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. However, in the healthcare context the flow of information is unidirectional from patient to physician, whereas friends are expected to reciprocally exchange confidential information.\(^{153}\)

A variance in any of these parameters might alter the subject’s perception of privacy, leading to a different response about whether their privacy has been maintained. 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.

---

\(^{148}\) Nissenbaum, supra note 125, at 127-28.
\(^{149}\) Id. at 140-47.
\(^{150}\) Id. at 141.
\(^{151}\) Id. at 143-44.
\(^{152}\) Id. at 144.
\(^{153}\) Id. at 144-45.
The contextual integrity framework helps explain why an Amazon.com customer may only feel moderately uneasy about Amazon recommending books or products based on their prior Amazon.com purchases, while simultaneously harboring outright resentment toward targeted third-party advertisements on a different website facilitated by cross-site tracking of the same purchase.\footnote{Id. at 195.} 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 them a recipient). The subsequent Amazon.com recommendations are manifested internally and do not imply that Amazon has violated the contextual integrity of the information flow by sharing any of the data with other parties.\footnote{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 (Jun. 29, 2022), https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4Z8MHFRNJ.}

In the latter scenario, however, the customer can infer that contextual integrity has been violated because even though they remain the data subject and the recipient, the sender of the data is now a third party that the subject has not previously interacted with. 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 under which the information was originally transmitted. 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 can offer 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.

\textit{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 instance, under Samuel Warren and Louis Brandeis’ famous formulation for the right to privacy, yes, privacy in the context of CBDCs is also about one’s right to be let alone. One has the right to live one’s life as one chooses, including one’s financial life, such as whom one wants to transact with, where and when one makes a payment, free from intrusion or invasion. Government cannot conduct surveillance of the financial records of millions of Americans under the Fourth Amendment. However, this interpretation ignores the practice that a CBDC system should allow for limited government access to CBDC data to prevent money laundering and financing of terrorism. Brandeis could not have anticipated that the right to
privacy would be pitted against national security and the challenge of terrorism. The stakes are considerably higher today than in Brandeis’ time in the 1890s.

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

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

The second reason is that the pragmatic approach and contextual integrity theory are flexible enough to capture many practical and nuanced questions. CBDC-related privacy questions are particularly practical and nuanced. Various designs can raise very different privacy questions. As elaborated in Section B below, one-tier and two-tier designs will allow for different parties to obtain access and collect and store CBDC data, which will raise different privacy questions. Centralized and DLT designs will expose very different CBDC information to different parties involved. Various parties, such as the 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 address. Privacy thus means different sets of rights and obligations to each of the parties. No one single conception of privacy can capture all problems arising from different settings and for all parties. The pragmatic approach and contextual integrity theory are more suitable because they address privacy contextually in different scenarios and addresses different problems that each party is facing. It ties in with particular problems in the given context, which allows for a better understanding of privacy in all dimensions.

Therefore, in this article, I adopt Daniel Solove’s pragmatic approach and Helen Nissenbaum’s contextual integrity theory to conceptualize privacy in the context of CBDCs. I focus on understanding privacy in specific contextual situations rather than seeking to illustrate an abstract conception of privacy. The first step is to understand CBDC practices—what are the contexts? Who are the actors? What are the attributes of the information? What are the transmission principles facilitating the exchange of the information? The second step is to explore what

---

157 Id. Nissenbaum, supra note 125, at 145.
aspects of these practices should be considered private and what other values to balance when recognizing and protecting the value of privacy in the CBDC practices.

Step 1: understanding CBDC practices. The specific contextual situation related to CBDCs centers on the practice of payment or, to be more precise, making payments with CBDCs. 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. The simplified norm or activity of payment is that the payor initiates the process by asking relevant entities to send money (CBDCs) to the payee. The entities verify the payee (or the CBDC, depending on the design) and record debits and credits of the payor’s and payee’s accounts (I am not considering offline token-based systems here). Law enforcement agencies, as gatekeepers, make sure the payments comply with the law.

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 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, then contextual integrity is preserved. If there is a lack of societal understanding and or approval of this sharing of information with law enforcement, then contextual integrity is violated and the parties will resent the transmission as a breach of their privacy, undermining their faith in the privacy of a CBDC payment.

Step 2: normative assessment. 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 the general public. In other words, each party is provided with a varying degree of visibility to CBDC data. When one states that one protects privacy in the context of making payments using CBDCs, one is claiming to guard against certain disruptions to this practice or to preserve contextual integrity. The disruptions

---

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

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

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

The degree of privacy also varies and relies on a normative assessment. We can consider our identity and transaction information private, but we do not consider them private in the same way. A CBDC system may be more private with respect to one entity (e.g., merchant) and less so for another (e.g., government). 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. Central banks should conduct cost and benefit analysis or use other mechanisms to decide to what extent CBDC data should be hidden from which entity.

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

The law is usually the result of balancing all these values. Take the Gramm-Leach-Bliley Act (GLBA) as an example, the GLBA was designed to enable the creation of financial conglomerates that provide a host of different forms of financial services. It authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies. The GLBA recognized the social and economic value of providing broader financial services to ordinary Americans. Financial institutions sharing financial data

---

163 Id.
165 Solove, supra note 113, at 792.
166 Id.
with affiliated entities was seen as helping them target their customers to better meet their needs.\textsuperscript{167}

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.\textsuperscript{168} 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.”\textsuperscript{169} The law also requires financial institutions to give notice to customers when they share customer information with affiliated entities.\textsuperscript{170} If they share customer information with nonaffiliated entities, they should first provide customers with the ability to opt out of the disclosure.\textsuperscript{171} 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 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. What should be considered private is a normative argument and could vary in various jurisdictions, cultures, and times. When conducting normative analysis, it is necessary to balance the value of CBDC data privacy with other conflicting values.

III. Privacy Issues Arising from Various CBDC Designs

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

CBDCs can be designed in different ways with different characteristics and functions.\textsuperscript{172} Different design choices will create different privacy issues (disruptions to CBDC practices). I agree with MIT and the Federal Reserve Bank of Boston’s view that CBDC design choices are

\textsuperscript{167} Id.

\textsuperscript{168} https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

\textsuperscript{169} Gramm-Leach-Bliley Act, 15 U.S.C. §6809(4)

\textsuperscript{170} Gramm-Leach-Bliley Act, 15 U.S.C. §6802(a)

\textsuperscript{171} Gramm-Leach-Bliley Act, 15 U.S.C. §6802(b)

more granular than commonly assumed.\textsuperscript{173} Many commonly assumed categories are still very limited; those categories are insufficient to bring to the surface the complexity of choices in access, intermediation, institutional roles, and data retention with regard to CBDC design.\textsuperscript{174}

In this paper, I do not intend to go through all design choices (which is impossible, practically speaking) and explore their privacy implications. CBDC design choices are more granular than commonly assumed.\textsuperscript{175} Instead, I investigate two structural and foundational design choices that all central banks will encounter and must decide on before they move on to other design choices. These two design choices cover the operational model and infrastructure (figure 1). The operational model deals with how CBDCs are distributed and who performs consumer-facing tasks. Two design choices are available: a one-tier model and a two-tier model (also known as a layered intermediary model). Infrastructure refers to the ways of recording transactions or updating credit and debit information. Three design choices are available: a centralized ledger system, a distributed ledger technology (DLT) system, or no ledger system.

\textbf{Figure 1. CBDC Design Choices}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure1.png}
\end{figure}

\textsuperscript{173} Project Hamilton Phase 1 A High Performance Payment Processing System Designed for Central Bank Digital Currencies, FEDERAL RESERVE BANK OF BOSTON & MASSACHUSETTS INSTITUTE OF TECHNOLOGY DIGITAL CURRENCY INITIATIVE (Feb. 3, 2022) at 39.


\textsuperscript{175} Project Hamilton Phase 1 A High Performance Payment Processing System Designed for Central Bank Digital Currencies, FEDERAL RESERVE BANK OF BOSTON & MASSACHUSETTS INSTITUTE OF TECHNOLOGY DIGITAL CURRENCY INITIATIVE (Feb. 3, 2022) at 5. I agree 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. In this paper, I do not intend to come up with new or better categories. Instead, I pick two existing design choices, meaningful and foundational although imperfect, to address their privacy issues.
To understand what privacy problems would arise from these design choices, methodologically, I first studied the dataflow of each design choice. Following the dataflow, I further investigated who can get access to what data. Each design varies in who can see, store, collect, and share CBDC-related data, including but not limited to identity data and transaction data. Some data are encrypted whereas some are not. All these factors contribute to what kind of disruptions could occur in the practice of CBDC payment (i.e., privacy problems).

The operational model and infrastructure are structural and foundational because they both deal with a key issue: the trust model, which decides what roles central banks and intermediaries (i.e., 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. I argue that the verification object is a very technical choice at the micro level, not a structural and foundational question like the choice of operational model and infrastructure. The section at the end will critique the need to distinguish between account-based and token-based systems and further elaborate why this design element is not considered a foundational and structural choice for the central bank to decide at the outset.

A. Operational Model

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

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

---

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

Data flow under the two-tier operational model is more complex. Data mainly flows between intermediaries and end users because intermediaries handle all communication with end users, including collecting and managing end users’ account information and clearing transactions. Intermediaries also clear transactions in real time and, therefore, will have a copy of transaction details, unless the system is designed to intentionally obfuscate information through privacy enhancing mechanisms such as zero-knowledge proof (ZKP). In terms of the record at the central bank, depending on the design, the central bank can have a copy of retail holdings or the wholesale balance sheet. If the former, then the central bank will also have at least the account and balance information of the end users; if the latter, the central bank will not have such information of an end user.

The biggest problem with the one-tier operational model, from a privacy point of view, is that the central bank by default will collect and store an enormous amount of end user data, which could enable mass surveillance, leading to abuse. Central banks are a government agency in many jurisdictions, for example, China’s central bank (the People’s Bank of China). A government agency having enormous financial information about users might have different implications in

---

180 Off. of Sci. and Tech. Pol’y, supra note 18, at 29.
different countries. In some authoritarian countries, without checks and balances, a government agency, i.e., the central bank, can easily obtain access to its citizens’ financial data stored at the central bank and share this information with other government agencies. Citizens are vulnerable to such intrusion to their financial data. Even in some democratic countries that have checks and balances, it is still unclear how central banks would protect users’ privacy under this new system in which central banks would have unprecedented access to financial data about its citizens that are usually stored and handled by banks and other intermediaries. Unless rigorous rules are put in place and executed properly, protection of users’ privacy remains unclear.

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

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

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

B. Infrastructure
Infrastructure refers to the ways of recording and sharing data. A central bank has three options for recording transactions and updating credit and debit information: a centralized ledger system (figure 4), a DLT system (figure 5), or no ledger system at all.\textsuperscript{181} 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.

\textbf{FIGURE 4. CENTRALIZED LEDGER SYSTEM}

\textbf{FIGURE 5. DLT SYSTEM}

A centralized system is a collection of transactions managed by a single player, which is the central bank in this case. The central bank controls the system and its contents, that is, which

\textsuperscript{181} \textit{Id.} at 34-36.
transactions get posted to a central ledger. A ledger is a digital file containing accounts to which debits and credits are posted, just like a physical account book in which a company writes down the amounts of money it sends and receives. With a centralized system, other intermediaries such as banks cannot update the central ledger without going through the central bank, even if intermediaries handle retail transactions and directly communicate with end users. The central bank acts as a trusted party for managing the central ledger. To be clear, every intermediary can hold its own ledger that records debits and credits of its users and is different from ledgers held by other intermediaries. One intermediary has no access to a ledger held by other intermediaries. In other words, ledgers held by all intermediaries are not synchronized.

DLT refers to the processes and technologies that enable participants in a network to securely propose, validate, and record state changes to a synchronized ledger that is distributed across the network’s participants. At its core, DLT is a decentralized way of recording and sharing data. The distributed ledger is an agreed-upon record of digital data spread across multiple entities. DLT uses a consensus mechanism to ensure the accuracy of the data on the ledger. In the context of payment, clearing, and settlement, DLT enables multiple entities, through the consensus mechanism, to process transactions without necessarily relying on a central authority to maintain a single “golden copy” of the ledger. In the context of CBDC transactions, commercial banks, cashless payment systems, and other authorized entities can post transactions and add credits and debits to the CBDC ledger without relying on the central bank to maintain a single copy of the ledger.

There are two types of DLT: permissionless and permissioned. Permissionless DLTs are open to every participant in the network. Any participant can add an entry to the ledger through the

---

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


187 Barr et al., * supra note 184*.

188 *Id.*
In contrast, permissioned DLTs are only open to a limited number of participants. Only permitted and verified participants can control record keeping. Therefore, permissioned DLTs share a limited consensus process. Most likely, central banks would consider only permissioned DLTs, in which a network of preselected participants have power over recordkeeping. It would be easier and faster for these preselected participants to reach consensus on the state of the ledger. While it is technically possible to use permissionless DLTs, the economic cost is too high for a large group of participants to reach consensus. In addition, a permissionless DLT will raise questions related to governance and information security issues because a larger number of distributed participants are unknown to each other.

In the centralized system, if it is a one-tier model, data flows mainly from end users to the central bank because end users need to rely on the central bank to update the balances to the ledger. Data related to the 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 flows from end users to intermediaries, and intermediaries verify such data and update the ledger they hold but cannot update the single “golden copy” that the central bank holds. Depending on the design, if the central bank wants to hold a wholesale balance sheet of all intermediaries, very limited data regarding end users will be sent from intermediaries to the central bank. If the central bank wants to hold a retail copy that records every single transaction handled by every single intermediary, detailed data then again flows from intermediaries to the central bank.

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

In a DLT (permissioned DLT in this case) system, data flows among participants in the network (intermediaries in the context of CBDCs). Assuming entity A wants to transfer $100 to entity B, the process involves three broad steps. First, to initiate a payment, entity A uses cryptographic

---

189 Id.
190 Id.
191 Id.
192 Id.
193 Auer and Boehme, supra note 176, at 8.
194 Mills, supra note 183, at 59.
195 Auer and Boehme, supra note 176, at 8.
196 Mills, supra note 183 at 59.
tools to digitally sign a proposed update to the shared ledger that would transfer $100 from its account on the ledger to entity B’s account. Data on this request flows from entity A to the network. Second, upon receiving the transfer request, other participants in the network need to authenticate entity A’s identity (public key) and validate that entity A has sufficient funds to make the payment. Data on identity and funds flows from entity A to the network, and all network participants can see the data in order to take part in the consensus process. Third, after the consensus process where all participants agree on the transfer of funds, the ledger is updated and $100 is added to entity B’s account. The data on the latest balance on the ledger is also shared by all participants.

The privacy issue in a DLT system is that a DLT system allows for broader access to information, which potentially compromises the integrity of data. Multiple intermediaries such as commercial banks and other payment services providers, as long as they are authorized to update the ledger, will have access to a complete set of CBDC data, including but not limited to transacting parties (shown in addresses/public keys), transaction amount, and transaction time. Any intermediary in the network has a copy of the synchronized ledger and can disclose any information to others unless rigorous rules are in place. An attack on one intermediary is sufficient to get a complete set of CBDC data. Therefore, having more participants (intermediaries) in the network makes privacy protection harder.

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

C. Verification Object?

Some literature argues that, once the operational model and infrastructure have been chosen, the question arises of how and to whom one should give access. 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. Figures 6 and 7 below present two options: an account-based model and a token-based model. The key distinction lies in what to verify in order to process a payment: an account-based system requires verification of the identity of the payor, while a token-based system requires verification of the validity of the object used to pay.

---

197 Auer & Boehme, supra note 176, at 9; see also The Digital Dollar Project, Exploring a US CBDC, supra note 123, at 17.
198 Baer, supra note 177, at 6.
199 Charles M. Kahn & William Roberds, Why pay? An introduction to payments economics, 18 JOURNAL OF FINANCIAL INTERMEDIATION 1–23 (2009); The distinction between account-based and token-based model has also been discussed in the following reports and papers: Benoît Cœuré & Jacqueline Loh, Central bank digital
Figure 6. Account-based Model

Figure 7. Token-based Model


201 Id.
The account-based model fundamentally depends on the ability to verify the account holder’s identity. It follows the conventional account model and ties ownership to an identity. Transactions are authorized via identification. Under this model, individuals hold their balances as accounts with the central bank and transactions are recorded as new entries on a centralized ledger. The account owner can request a transfer of funds to another account owner. The central bank would settle the transaction by updating its central ledger. 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). Physical cash (i.e., banknotes) is a good example of a token-based model. As shown in figure 7, assuming Party A wants to pay Party B $100 cash, the only thing party B needs to worry about is that the $100 bill is not fake. If the bill is valid, then it can be used to make a purchase.

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

If the token is a digital currency, theoretically speaking, party B only needs to worry about whether the digital currency is genuine and whether it already been spent. Party B does not need to know anything about Party A. The transaction happens between two wallets instead of two accounts. Wallets are not actually where the digital currencies are stored. Instead, each wallet has a private key that corresponds to an address in the network, which, in turn, corresponds to the number of tokens held by the owner of the wallet. These wallets could take the form of a website, a mobile app, or even a hardware wallet.
While it is very common to make a distinction between account-based and token-based systems,\(^{212}\) from a practical point of view, such a distinction is problematic and sometimes useless.\(^{213}\) Many computer science professionals think the distinction is meaningless and irrelevant when it comes to cryptocurrencies and other revolutionary electronic payment methods.\(^{214}\) One of the biggest issues with this distinction is that the use of the token-based and account-based terminologies does not create mutually exclusive categories.\(^{215}\) For example, Bitcoin and many other digital currencies can satisfy both categories.\(^{216}\)

“Bitcoin fits the definition of an account-based system. The account is a Bitcoin address, and the private key is the proof of identity needed to transact from that account. Every time a Bitcoin user wants to spend Bitcoin, that user must verify their identity by using their private key. Bitcoin also fits the definition of a token-based system. When someone wants to spend a Bitcoin, the protocol verifies its validity by tracing its history. The current transaction history is used to verify the validity of the ‘object’ being transferred, as other token-based systems also do.”\(^{217}\)

Unless the CBDC is an offline physical object, a CBDC also fits the definitions of an account-based system and a token-based system. In a centralized system, a CBDC is account-based because the central bank or intermediaries, depending on whether it is a one-tier or two-tier design, need to verify the identities of the payor and payee before processing the transactions and updating the balance sheet. In a DLT system, a CBDC can be account-based because the public key is the account and the private key is the proof of identity. A CBDC arguably can also be token-based because participants in the network also need to verify the transaction history of the “object” being transferred. Therefore, at the deepest levels of computer architecture, the distinction makes no sense.\(^{218}\) The distinction remains relevant probably only because it helps nonexperts to understand the revolutionary technology or product by referring to something that already exists or of which people have knowledge.\(^{219}\)

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

D. One Unique Scenario

\(^{212}\) See Cœuré & Loh, \textit{supra} note 199; Kahn, \textit{supra} note 199; Mancini-Griffoli, et al., \textit{supra} note 206, Auer & Boehme, \textit{supra} note 176, Sridhar & Horan, \textit{supra} note 209.

\(^{213}\) Garratt, et al., \textit{supra} note 174.

\(^{214}\) Kahn, \textit{supra} note 199.

\(^{215}\) Garratt, et al., \textit{supra} note 174; \textit{see also} Bitcoin is an Account, Not a Token, \textit{MONEYNESS} (Aug. 18, 2020) http://jpkoning.blogspot.com/2020/08/bitcoin-is-account-not-token.html

\(^{216}\) Garratt, et al., \textit{supra} note 174.

\(^{217}\) \textit{Id.} (arguing that Bitcoin is not a token).

\(^{218}\) Kahn, \textit{supra} note 199.

\(^{219}\) \textit{Id.}
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 and manipulate the national money supply: issuing currency and setting interest rates on loans and bonds. In this way, they manage monetary policy to guide the country’s economy and achieve economic goals, such as full employment. Second, they regulate member banks through capital requirements, reserve requirements, and deposit guarantees, among other tools. They also provide loans and services for a nation’s banks and its government and manage foreign exchange reserves. Third, a central bank also acts as an emergency lender to distressed commercial banks and other institutions, and sometimes even the government. For instance, by purchasing government debt obligations, the central bank provides a politically attractive alternative to taxation when a government needs to increase revenue.

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

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

Practically, central banks would adopt a centralized system over a DLT system. At the very outset, no central bank worldwide has an operational DLT-based system at this point, although two-thirds of central banks are directly experimenting with DLT protocols. 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. Some central banks, such as the European Central Bank and the Bank of Japan, have declared DLT not mature.

---

221 Del Rio, supra note 185.
enough at this stage to power the world’s biggest payment systems. The Bank of Canada stated that, for critical financial market infrastructures such as wholesale payment systems, current versions of DLT may not provide an overall net benefit relative to current centralized systems.

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. Second, DLT faces scalability challenges. Consensus algorithms and cryptographic verification introduce latency and limit the number of transfers that DLTs can process currently, whereas existing payment clearing and settlement systems can process hundreds of millions of transactions daily. Additionally, ledgers that add transactional histories on top of one another, such as blockchains, may challenge storage capacity over time. 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. The costs have been allocated to participants, and it is not clear if this is cost effective compared to a centralized system.

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

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

---

224 Mills, supra note 183; see also Del Rio, supra note 185, at 4; Baer, supra note 165, at 6.
225 Del Rio, supra note 185, at 8.
226 Mills, supra note 183, at 36.
227 Del Rio, supra note 185 at 8.
228 Baer, supra note 184 at 13.
229 Baer, supra note 184.
This two-tier and centralized design could by default potentially bring about privacy violations in various forms, although it could effectively achieve other goals. The next question is whether central banks can come up with solutions to address privacy violations in this design. The section below proposes a few general principles to design a privacy preserving CBDC.

IV. PRIVACY PRINCIPLES FOR A CBDC

In the previous section, I argued 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. In this section, instead suggesting a set of universal privacy rules for CBDCs for all jurisdictions to adopt, I 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 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, I introduce privacy by design (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 can help 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, I must stress that privacy is necessary and that every CBDC system should protect it. Whichever design choices a central bank may adopt, privacy should be a critical consideration. Scholarly literature on privacy has amply justified its importance. Many policymakers and central banks have already successfully identified the importance of privacy and called for privacy protection in CBDC systems, as previously mentioned in Section III.

Nevertheless, I still emphasize the need for privacy at the outset because it is the foundational principle that sets the tone for other principles. Only if we assume the importance and need for privacy in a CBDC system will other privacy principles, such as PbD, be sound and logical.
Although each jurisdiction might vary on which aspects of CBDC practices should be considered private and the ideal degree of privacy, all should come to an agreement that we need privacy in the CBDC system as an underlying principle.

One way to emphasize the importance and the need for privacy is through policy, legal, and regulatory recognition. Therefore, policymakers, legislatures, and regulators should recognize it in official policy documents, laws, and regulations. As previously mentioned, policymakers in many jurisdictions have done an excellent job in recognizing the need for privacy. But legal and regulatory recognition is still lacking.

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. 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. 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 cases, the laws have already provided legal and regulatory recognition by applying privacy and data protection laws to regulating digital transactions and payments.

B. Privacy by Design

The second principle by which to design a privacy-preserving CBDC is to follow the PbD approach. Developed by Dr. Ann Cavoukian in the 1990s, the PbD concept aims to “address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.” 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. Cavoukian defines PbD as characterized 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.

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

231 Id. at 5.
233 Id.
holistic, interdisciplinary, integrative, innovative, and inspiring.” Privacy must be incorporated into networked data systems and technologies by default. Privacy must become integral to the design process and it should be embedded into every standard, protocol, and process that touches our lives.

In this paper, I apply 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. The investigation in Section III makes evident that design options related to the roles of central banks and intermediaries significantly affect the privacy landscape and create various privacy issues. 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 abuse—because the central bank by default collects, stores, processes, and potentially uses of 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, to some extent, provides better privacy protection, but it also compromises data integrity. In summary, the involvement of central banks and intermediaries in the CBDC system has a direct influence on the types of information these entities receive as well as further effects on 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 preventative measure. For instance, Section III concludes that a one-tier operational design could result in mass surveillance and data abuse. 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. In 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. I do not intend to define which roles central banks or entities should play, and I argue this is a decision CBDC designers should make in the first place to avoid privacy disruptions.

235 Id.
236 Id.
237 Id.
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 European Union’s General Data Protection Regulation, provide various levels of privacy protection. In the United States, some states have enacted privacy laws to provide certain degrees of privacy protection (e.g., California’s Consumer Privacy Act and Virginia’s Consumer Data Protection Act), as well as sectoral laws such as the Gramm-Leach-Bliley Act in the financial sector and the Health Insurance Portability and Accountability Act 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 primary protection or 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.

I am not arguing that ex post mechanisms such as punitive damages or injunctions are ineffective; they are certainly helpful, because punishment and deterrence can reduce future privacy violations. Instead, I argue 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.\(^\text{238}\) 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.\(^\text{239}\) He used blind signatures to


\(^{239}\) Id.
unlink the spending and receiving of a specific banknote.\textsuperscript{240} 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 is particularly helpful in delivering privacy protection in the CBDC system is zero knowledge proof (ZKP). The ZKP approach enables one party (the prover) to prove to another party (the verifier) that a given statement is true without revealing any additional information apart from the fact that the statement is indeed true.\textsuperscript{241} 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.\textsuperscript{242}

Bontekoe et al. proposed the use of ZKP to allow fully private transactions with the possibility of person-related monthly turnover or transaction limits.\textsuperscript{243} However, this approach contradicts anti-money laundering (AML) regulations and those combating the financing of terrorism (CFT).\textsuperscript{244} 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.\textsuperscript{245}

To that end, Jonas et al. presented a holistic approach for a privacy/compliance-by-design CBDC with ZKP.\textsuperscript{246} Simply put, they use commitments and nullifiers to obfuscate transfers so transfers are not linkable.\textsuperscript{247} All end users can privately register and maintain their private CBDC accounts.\textsuperscript{248} End users only send cryptographic proof of correct local accounting and compliance with the imposed limits of the ledger that the central bank maintains.\textsuperscript{249} The central bank only accepts a transfer proposal if ZKP rightfully proves it complies with the imposed limits.\textsuperscript{250}

Similarly, Wust et al. also designed a CBDC system, called Platypus, to provide strong privacy protection using Zerocash, a novel form of ZKP.\textsuperscript{251} The system assumes an authority is trusted
for the integrity of the currency (e.g., double-spending protection) but is not trusted for privacy. Platypus uses Zerocash to provide anonymity for the sender and recipient as well as secrecy of the transaction amounts.

However, not all privacy-enhancing or privacy-preserving technologies are mature, and ZKP has its drawbacks. The purpose of this paper is not to propose the perfect technological design offering flawless privacy protection in the context of CBDCs. Instead, my goal is to argue 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 is an iterative design process in which designers focus on the users and their needs in each phase of the design process. 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. Generally, user-centered design involves four distinct phases:

First, as designers working in teams, we try to understand the context in which users may use a system. Then we 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, you assess the outcomes of the evaluation against the users’ context and requirements, to check how well a design is performing…. From here, your team makes further iterations of these four phases, and you continue until the evaluation results are satisfactory.

FIGURE 7

---

252 Id.
253 Id.
254 What is User Centered Design?, THE INTERACTION DESIGN FOUNDATION, https://wwwinteraction-design.org/literature/topics/user-centered-design (last visited: Jul. 22, 2022). The term was coined in the 1970s and later Don 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. And 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).
255 Id.
256 Id.
257 Id.
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. If users require that their data not be shared with other entities except for entities directly 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, then 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 has adopted a user-centered approach and is currently finalizing its first iteration of evaluation.\textsuperscript{258}

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 further leads to 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. Users’ participation also guarantees that informed privacy decisions may be reliably exercised. In addition, putting 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.\textsuperscript{259}

**CONCLUSION**

\textsuperscript{258} See Exec. Order No. 14067, 87 FR 14143 (Mar. 9, 2022); see generally OFF. OF SCI. AND TECH. POL’Y, supra note 18.

\textsuperscript{259} \textit{What is User Centered Design?}, supra note 254.
In this paper, I demystify CBDCs by comparing CBDCs with other digital currencies and explain what motivates central banks to issue a CBDC. I also adopt a pragmatic approach to understanding privacy contextually and investigate privacy problems that could occur in four structural CBDC designs. Finally, I propose three legal and technical principles that central banks can follow if they decide to design a privacy-preserving CBDC.

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