Decoding the rise of Central Bank Digital Currency in China: designs, problems, and prospects

Pangyue Cheng¹

Accepted: 27 January 2022

© The Author(s), under exclusive licence to Springer Nature Limited 2022

Abstract

During the Covid-19 pandemic, there has been a rapid shift in global transaction patterns from offline to online digital payment models, along with a growing interest in the development of Central Bank Digital Currencies (CBDCs) in various countries. This article spotlights the unexamined issue of digital currency regulation by examining the practice and related regulatory rules of the pilot CBDC in China. Beginning with the global design choices of digital currencies, the article comparatively examines the technical design of China's CBDC, known as e-CNY. It further triggers a rethinking of conventional regulations for the protection of digital currency information by investigating the gap between the actual operation and design of e-CNY, as well as the gap between pilot policies and legal provisions such as the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. This article argues that, on the one hand, the legislative balance between the protection of personal information and the regulation of illicit financial activities involved in the “loosely coupled account link” system of e-CNY should be reconsidered. On the other hand, the delineation of rights and responsibilities between dissemination institutions, payment service providers, and end-users needs to be further redefined and clarified.

Keywords Central Bank Digital Currency (CBDC) · Design choices · e-CNY pilots · Personal information protection

Introduction

Over the past two decades, innovative technologies have reshaped the monetary and payment systems at an unprecedented pace. The emergence of multiple digital currencies, including but not limited to mobile money (like M-Pesa) and cryptocurrencies based on distributed ledger technology (DLT)¹ and blockchain (such as Bitcoin, Ethereum, and Diem), continue to challenge traditional regulations governing currency at the domestic and international levels.² In addition, unregulated, crypto-digital currencies have provoked an explosive growth of fraud, theft, and hacking problems, which pose a ubiquitous threat to traditional financial regulation and banking systems under the purview

and control of national regulatory authorities, such as central banks.³

Central banks in many countries, such as the Bank of Canada, the Bank of England, and the People's Bank of China (PBOC) are, therefore, exploring the possibility and feasibility of introducing a state-regulated, central bank-backed digital currency to address the aforementioned issues arising from the anonymity of traditional digital currencies,

✉ Pangyue Cheng
pangyue_cheng@u.nus.edu

¹ Faculty of Law, National University of Singapore, 469G Bukit Timah Road, Singapore

¹ According to the Bank for International Settlements (BIS) report, DLT refers to “the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate, and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes”. See BIS [11] Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework, Basel, Switzerland: Committee on Payments and Market Infrastructures. CPMI Paper no. 157.

² Didenko et al. [21] After Libra, Digital Yuan and COVID-19: Central Bank digital currencies and the new world of money and payment systems. Sydney, Australia: The European Corporate Governance Institute. ECGI Working Paper Series 65/2020.

³ Cunha et al. [17] From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution. Future Internet 13(7): 165.

of which China is at the forefront.⁴ In April 2020, the PBOC distributed 10 million e-CNY (or digital yuan) to Shenzhen residents, thus making China one of the first countries to experiment with Central Bank Digital Currency (CBDC) in reality.⁵ Although the research and use of CBDC are still in their initial stages, the enormous financial and market potential of state-backed digital currency would lead to the rapid spread of CBDC around the world.

Since CBDC is still in the process of research and development, there is no uniform and conclusive definition of this digital currency, but it generally has three unique characteristics that distinguish it from physical money, e-money, and conventional cryptocurrencies. Firstly, the CBDC is issued by a central bank, which represents a liability of the central bank rather than a private financial institution and is likely to have a similar value to the fiat currency issued by that central bank⁶; secondly, the CBDC is virtual money in digital form instead of physical form; and thirdly, while it may use blockchain or DLT to facilitate transactions and settlements, the CBDC is centrally controlled and supervised by the central bank.

Besides, the advantages and disadvantages of CBDC have been discussed in numerous banking analyst reports and academic studies around the world. In general, the advantages of CBDC include efficiency, convenience, safety, integrity, accessibility, settlement finality, and financial inclusion,⁷ while the disadvantages typically include misuse of financial data and user privacy.⁸ However, with the ongoing concerns about the protection of digital information associated with CBDC, there has little legal and policy analysis related to

the information protection regulation of CBDC,⁹ despite the emergence of financial and technological research on CBDC,¹⁰ and despite the fact that China has already launched experiments of e-CNY in pilot cities and plans for further experiments at the Beijing 2022 Winter Olympics.¹¹ Thus, it is significant to examine the new issues developed by the emergence of CBDC and to fill this literature gap in the context of increased cashless payment during the Covid-19 pandemic, particularly in China, where the CBDC was first put into use in reality. The analysis in this paper will have broader implications for state-backed digital currencies in other jurisdictions. Moreover, when the development of CBDC poses potential or substantial risks to the financial market and personal privacy, it is necessary to address the challenges from a legal perspective and to propose a viable set of solutions to the problems.

Before analyzing the practical and regulatory issues of CBDC, it is necessary to investigate the available design choices, which are inextricably linked to the further regulation of CBDC. In addition, this article spotlights the unexamined issue of digital currency regulation by empirically examining the practice and related regulatory rules of the pilot in China. It triggers a rethinking of conventional regulations for the protection of digital currency information by investigating the gap between the actual operation and design of CBDCs, as well as the gap between pilot policies and legal provisions such as the Cybersecurity Law, Data Security Law (DSL), and the Personal Information Protection Law (PIPL). This paper argues that on the one hand, the legislative balance between the protection of personal information and the regulation of illicit financial activities involved in the “loosely coupled account link” (*song ou he*) system of e-CNY should be reconsidered. On the other hand, the delineation of rights and responsibilities between dissemination institutions, payment service providers, as well as end-users needs to be further redefined and clarified.

The structure of the paper is as follows. Section “A review of CBDC design choices in various countries” examines the different models and the current development status of CBDCs in various countries, with an emphasis on reviewing CBDC design features and existing implementations. The purpose is to compare China’s CBDC design choices with those of other countries and provide the theoretical

⁴ In 2014, the PBOC established a research group on legal digital currency, which focused on the issuance of digital currency, related key technologies, and the context for currency issuance and circulation. Furthermore, the CBDC Research Institute was launched in 2016 to complete the construction of the initial prototype system of Chinese CBDC (e-CNY), followed by joint research trials with commercial institutions (such as Ant Group, China UnionPay, etc.) in 2017. See PBOC [32] Working Group on E-CNY Research and Development of the PBOC. Beijing, China: Progress of Research and Development of E-CNY in China, Bordo, M. D., and Levin, A. T. (2017) Central bank digital currency and the future of monetary policy. Massachusetts, US: National Bureau of Economic Research. NBER Working Paper 23,711.

⁵ Jiaying and Karman [24] Background and Implications of China’s E-CNY, 11 January, <https://ssrn.com/abstract=3774479>, accessed 29 August 2021.

⁶ Boar and Wehrli [15] Ready, Steady, Go?—Results of the Third BIS Survey on Central Bank Digital Currency. Basel, Switzerland: Bank for International Settlements. BIS Working Paper no. 1146.

⁷ See, e.g., BIS [14–14] CBDCs: an Opportunity for the Monetary System. Basel, Switzerland: Bank for International Settlements. Basel, Switzerland: Bank for International Settlements. BIS Annual Economic Report.

⁸ *Ibid.*, at 69, 72, and 75.

⁹ The exceptions are Jiang and Lucero, *supra* note 5; Didenko et al., *supra* note 2.

¹⁰ See, e.g., Morales-Resendiz et al. [29] Implementing a retail CBDC: Lessons learned and key insights. Latin American Journal of Central Banking 2(1): 2; Adrian and Mancini-Griffoli [1] The Rise of Digital Money. Annual Review of Financial Economics 13(1), Bech and Garratt [8] Central bank cryptocurrencies. BIS Quarterly Review, September.

¹¹ Jiang and Lucero, *supra* note 5, at 4.

background for further analysis. Section “[Practical and regulatory issues of E-CNY pilot in China](#)” investigates two main legal problems accompanied by the e-CNY in China. The first problem pertains to the gap between theoretical design and empirical practice. The second problem relates to the legal challenges associated with the broad range of financial services offered by the issuing bank (central bank) and other payment service providers (such as telecom operators and commercial banks) to CBDC users. Section “[Proposed regulatory framework for CBDC in China](#)” proposes four main solutions to the emerging problems accompanied by the rise of CBDCs: (a) proposing new classifications and related regulations for information processing with respect to digital currency user’s information; (b) enhancing the compliance of current digital currency service providers; (c) delineating the rights and obligations of different levels of regulators; and (d) specifying the know-your-customer authority and prerequisites to combat criminal activities. Section “[Conclusion](#)” concludes.

A review of CBDC design choices in various countries

Central bank interest in CBDCs has grown rapidly in the Covid-19 pandemic era.¹² According to a survey on CBDC conducted by the Bank for International Settlements (BIS) in 2021, there have been more than 60 central banks exploring the potential of CBDC since 2014, in which 86% are actively engaged in CBDC research, 60% are conducting technology experiments or proofs of concepts, and 14% are moving forward with CBDC pilot projects.¹³ During the experimental and pilot process, these central banks, however, faced several choices in designing the CBDC architecture.¹⁴ The Different options bring correspondingly far-reaching positive impacts and risks,¹⁵ leading authorities cautiously choosing

the future direction of CBDC development through numerous pilot testing.¹⁶ Before investigating issues specifically related to the e-CNY, it would be helpful to get a view of the entire structure of CBDCs. This chapter thus examines the fundamental design options for central banks—what types of users will CBDCs serve? What operational roles will central banks and financial intermediaries play? What range of transactions will be of concern? And what prototypes and access technologies will CBDCs be based on?—by reviewing the latest research and project experiments of CBDCs in various countries.

Target users, operator roles, and scope of use

One of the important design choices facing CBDC issuers is the customers that they are targeting. The rights and responsibilities of central banks and other financial service providers may vary depending on the users. Thus, before analyzing the role of financial institutions, it is necessary to clarify the types of CBDC that are currently being studied in various countries. At present, two forms of CBDCs are available in central banks, retail CBDCs and wholesale CBDCs. The former is used in a larger financial context where both individual and financial institutions can use CBDC to support their financial transactions, while the latter is only concerned with specific financial operations between financial institutions and entities.¹⁷

Based on observations, retail CBDC projects are favoured in emerging markets and developing economies, such as Bahamas, Cambodia, and Mainland China, where financial inclusion and enhanced payment abilities seem to be the key drivers.¹⁸ For instance, Sand Dollar (or called B\$) was introduced to enhance payment services within the Bahamas’

¹² Saka et al. [34] Epidemic Exposure, Fintech Adoption, and the Digital Divide. CEPR Discussion Paper no. 16326.

¹³ Boar and Wehrli *supra* note 6, at 6.

¹⁴ Auer et al. [6, 7] Taking Stock: Ongoing Retail CBDC Projects. BIS Quarterly Review, 1 March, https://www.bis.org/publ/qtrpdf/r_qt2003z.htm, accessed 31 December 2021.

¹⁵ See, for example, Bordo and Levin [16] Central Bank Digital Currency and the Future of Monetary Policy. Massachusetts, US: National Bureau of Economic Research. NBER Working Paper no. 237611, and Bindseil [9] Central Bank Digital Currency: Financial System Implications and Control. International Journal of Political Economy 48(4): 303–335 (analysis of CBDC improves the transaction efficiency); see Allen et al. [3] Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. Massachusetts, US: National Bureau of Economic Research. NBER Working Paper no. 27634, and Engwet and Fung [22] Central Bank Digital Currency: Motivations and Implications. Ottawa, Canada: Bank of Canada. Staff Discussion Paper No.2017–2016 (analysis of CBDC to promote financial inclusion); see Bech and Garratt, *supra* note 10

Footnote 15 (continued)

(analysis of CBDC to minimize criminal usage); also see BIS (2021a, b, c Central Bank Digital Currencies: Financial Stability Implication. Basel, Switzerland: Bank for International Settlements. BIS Report No. 4 (analysis of the additional financial stability risks posed by CBDC).

¹⁶ See, for example, Mancini-Griffoli et al. [28] Casting light on central bank digital currency. Washington DC, US: International Monetary Fund. IMF Staff Discussion Note 8, Auer et al. [6, 7] Rise of the central bank digital currencies: drivers, approaches and technologies. Munich, Germany: CESifo Working Paper no. 8655; Agur et al. [2] Designing central bank digital currencies. Journal of Monetary Economics, available online 8 May 2021, 10.1016/j.jmoneco.2021.05.002.

¹⁷ Boar and Wehrli, *supra* note 6, at 4.

¹⁸ Boar and Wehrli, *supra* note 6, at 7; BIS [14–14] Central bank digital currencies for cross-border payments: report to the G20, July, <https://www.bis.org/publ/othp38.pdf>, accessed 2 January 2022; Kiff et al. [27] A survey of research on retail central bank digital currency. Washington DC, US: International Monetary Fund. IMF Working Paper WP/20/104.

scattered archipelago.¹⁹ E-CNY was also explicitly identified by the PBOC as a retail CBDC to better meet domestic retail payment demands.²⁰ Further, there are two existing models for retail CBDCs architectures—direct and indirect—in which the central bank and financial intermediaries play different operational roles. The design of a direct retail CBDC may convert the traditional two-tier monetary system to one-tier in which the central bank keeps all records of CBDC transaction and directly handle payment services for the general public.²¹ Research on direct retail CBDC research such as the E-krona project in Denmark,²² Norway²³ and Sweden,²⁴ Sand Dollar pilot in the Bahamas,²⁵ and Rafkróna in the central bank of Iceland,²⁶ examines the potential for CBDCs to diminish credit risks and reduce reliance on the other commercial agents. Direct retail CBDC is simple as it eliminates reliance on financial intermediaries; but on the other hand, a direct infrastructure implies that the former responsibilities of intermediaries, such as customer due diligence, account management, and payment services, are transferred from the private sector to the central bank, which may detract from the stability and efficiency of the payment system.²⁷ Thus, the indirect retail CBDC model seems less disruptive to the current payment system, as it still has the two-tier financial system, with the central bank responsible only for the wholesale accounts of financial intermediaries, and the latter continuing to be accountable to the public. A typical example is China's Digital Currency/ Electronic Payments (DC/EP) program, which explores a two-tier operating system centered on the PBOC. The project requires authorized financial intermediaries to exchange and circulate

e-CNY to the public, while the central bank is responsible for the issue and centralized management.²⁸

In contrast, research and experiments on wholesale CBDCs or interbank CBDCs have mostly been conducted in developed economies with relatively well-established interbank systems and financial trading markets, such as Hong Kong SAR, Singapore, Canada, the United Kingdom, France, and Japan,²⁹ where payment-related motivations such as efficiency, safety, and robustness are of greater concern than financial inclusion.³⁰ In addition, most of the wholesale projects are conducted on a cross-border basis to test the interconnection potential between different CBDC projects, such as HKSAR-Thailand, Singapore-Canada, Europe-Japan, etc.³¹ The wholesale CBDC project is less likely to influence the operational role of central banks and financial institutions because banks already have direct access to the central banks' electronic money.³² But consider that the wholesale project aims to promote security and efficiency in the institutional trading process, it may also provide CBDC accounts and payment services to other institutions such as securities participants and nonfinancial companies. For example, according to the final phase report of the Ubin Project launched by the Monetary Authority of Singapore (MAS), the Ubin V project has collaborated with 16 selected firms in multiple scenarios, including capital markets, trade and supply chain finance, insurance, and other institutional payment services such as media and advertising transactions and salary payments.³³ These selected institutions include not only financial firms, such as IEX, iSTOX, and Digital Ventures; but also non-financial firms like Aqilliz, Octomate, and Adecco.³⁴

In addition, in order to simplify cross-border payments, reduce transaction risks and costs, and improve payment efficiency, the cross-border wholesale CBDC programs currently examine three models to facilitate transactions between central banks. The first model attempts to eliminate the conventional trusted third party in interbank settlements and conduct direct payment versus payment (PvP)

¹⁹ *Ibid.*

²⁰ PBOC Working Group, *supra* note 4, at 4.

²¹ Auer and Böhme [5] Central Bank Digital Currency: the Quest for Minimally Invasive Technology. Basel, Switzerland: Bank for International Settlements. BIS Working Paper no. 948.

²² Gürtler et al. [23] Central Bank Digital Currency in Denmark? Copenhagen, Denmark: Denmark's National bank. Analysis no. 28.

²³ Norges Bank Working Group [30] Central Bank Digital Currencies Second Report of Working Group. Oslo, Norway: Norges Bank. Norges Bank Memo no. 2.

²⁴ Julin [25] The Riksbank's E-krona Project. Stockholm, Sweden: Sveriges Riksbank. Report 1.

²⁵ Central Bank of the Bahamas (2019) Project Sand Dollar: A Bahamas Payments System Modernisation Initiative, 24 December, <https://cdn.centralbankbahamas.com/download/022598600.pdf>, accessed 9 September 2021.

²⁶ Central Bank of Iceland (2018) Rafkróna? Central Bank Digital Currency Interim Report, September, https://www.cb.is/library/Skraa-rsfafrn---EN/Reports/Special_Publication_12.pdf, accessed 9 September 2021.

²⁷ Auer and Böhme, *supra* note 21, 88–90.

²⁸ PBOC Working Group, *supra* note 4, at 4.

²⁹ BIS, *supra* note 18.

³⁰ Boar and Wehrli, *supra* note 6, at 8.

³¹ BIS, *supra* note 18.

³² Deloitte [20] Are Central Bank Digital Currencies (CBDCs) the money of tomorrow? <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-are-central-bank-digital-currencies.pdf>, accessed 9 September 2021.

³³ Temasek and Monetary Authority of Singapore (2020) Project Ubin Phase 5—Enabling Broad Ecosystem Opportunities, 13 July, <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-Phase-5-Enabling-Broad-Ecosystem-Opportunities.pdf>, accessed 9 September 2021.

³⁴ *Ibid.*

services for cross-border transactions. For instance, in the Jasper-Ubin project of the Bank of Canada and MAS, two DLT-based CBDCs use Hashed Time-Locked Contracts (HTLC) technology to connect their payment networks and explore the potential of DLT interconnectivity mechanisms for CBDCs.³⁵ The second model retains the third institution between two separate CBDCs systems, but it contemplates a joint institution managed by specific central banks to serve cross-border payments. One example is the Inthanon-LionRock project developed by the Bank of Thailand (BOT) and Hong Kong Monetary Authority (HKMA), which uses a BOT-HKMA managed “corridor network” to initiate and settle cross-border payments between two separate CBDCs.³⁶ The third model extends CBDC cross-border payments from two banks to multiple banks through a common network. The model is being explored by MAS and Banque de France, who is testing the possibility of a shared corridor network of multiple CBDCs (m-CBDCs).³⁷ Through setting up smart contracts to automatically manage exchange rates between different CBDCs in real-time market transactions, the experimental m-CBDCs network integrates “automated liquidity pool and market-making services” to explore the potential of the cross-border CBDC payments in multiple central banks.³⁸

Infrastructure and access technology design

There are two kinds of CBDC infrastructures developed in central banks, the first one is based on DLT, and the second one is based on central control. As mentioned above, the DLT-based CBDCs draw on the concept of decentralized cryptocurrencies but compensate for the illegitimacy issues associated with complete anonymity by allowing validation by authorized verifiers.³⁹ Most of the planned CBDC prototypes are closely tied to multiple technologies of DLT,

for example, central banks in jurisdictions such as Brazil, Cambodia, Ukraine, Eastern Caribbean, and China have adopted DLT models.⁴⁰ The DLT-related design currencies are completely different from electronic currencies based on a trusted central payment system.⁴¹ Compared with a centralized intermediary payment system, the DLT design of CBDCs may facilitate business transactions and financial services through its accessibility, resilience, and transparency.⁴² Nevertheless, CBDC with DLT design is not without risk. Evolving DLTs may pose operational and security risks as well as potential disruptions to current monetary regulation. For example, multiple nodes of a DLT may create additional entry points for malicious intruders, cryptographic tools could have security breaches, and the current regulations may not be well established to confirm the rights and obligations of related parties.⁴³ In addition, the relevant non-central bank parties in a DLT-based CBDC may be entitled to participate in various scenarios of CBDC transactions without having sufficient security capabilities as a country’s central bank, leading to additional financial risks.⁴⁴ In most instances, these risks and disruptions are resilient and could be addressed through continuous improvements in the design of DLT-based CBDC frameworks,⁴⁵ but legal uncertainty, or even the lack of regulations to control risks and protect users, may undermine public confidence in digital currencies and further hinder their development.⁴⁶ Thus, considering that the decentralized nature of the DLT-based CBDC may diminish the management of the central bank and challenge the existing monetary regulation framework, there are a lot of countries, especially the top economies, that attempt to regulate or consider regulating digital currencies in the context of the central banking system.

In addition to the DLT-based CBDCs, there also exist CBDC infrastructures that are based on conventional centrally controlled mechanisms. With the conventional centralized databases, each update would be recorded on multiple physical nodes that are uniformly controlled by a top-level

³⁵ MAS (2019) Central Banks of Canada and Singapore Conduct Successful Experiment for Cross-border Payments Using Distributed Ledger Technology, 2 May, <https://www.mas.gov.sg/news/media-releases/2019/central-banks-of-canada-and-singapore-conduct-successful-experiment-for-cross-border-payments>, accessed 10 September 2021.

³⁶ Bank of Thailand and Hong Kong Monetary Authority (2020) Inthanon-LionRock, Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, accessed 10 September 2021.

³⁷ MAS (2021) Monetary Authority of Singapore and Banque de France Break New Ground in CBDC Experimentation, 8 July, <https://www.mas.gov.sg/news/media-releases/2021/monetary-authority-of-singapore-and-banque-de-france-break-new-ground-in-cbdc-experimentation>, accessed 10 September 2021.

³⁸ *Ibid.*

³⁹ BIS, *supra* note 6, at 79.

⁴⁰ Auer and Böhme, *supra* note 21, at 98.

⁴¹ BIS [10] Digital Currencies, Basel, Switzerland: Committee on Payments and Market Infrastructures. BIS Working Paper no. 1146.

⁴² Kiff et al., *supra* note 18, at 29.

⁴³ BIS, *supra* note 41, at 16.

⁴⁴ World Economic Forum [36] CBDC Technology Considerations White Paper. Digital Currency Governance Consortium White Paper Series, 19 November, https://www3.weforum.org/docs/WEF_CBDC_Technology_Considerations_2021.pdf, accessed 2 January 2021.

⁴⁵ See, for example, selecting permissioned and trusted platforms to reduce security concerns. Kiff et al., *supra* note 18, at 29.

⁴⁶ See Kapsis [26] Should we trade market stability for more financial inclusion? The case of crypto-assets regulation in EU. In A. Lui and N. Ryder (eds.) *FinTech, Artificial Intelligence and the Law*. London: Routledge, pp. 85–104.

node.⁴⁷ Such a method of recording data is faster than the DLT mechanism, where updates to the ledger need to be broadcast and wait for replies before they can be finalized in the ledger.⁴⁸ For example, the central bank of Ecuador (Banco Central del Ecuador) developed the Dinero Electrónico project between 2014 and 2018, in which the designed mobile payment system was maintained by the central bank.⁴⁹

Another technology related to the design of CBDC is the user access method. So far, central banks have designed two different ways for accessing CBDC (either retail or wholesale): account-based and token-based.⁵⁰ The account-based CBDC is similar to a bank account where user transaction data are recorded in a database tied to their identity.⁵¹ Thus, customers are required to prove their identity before proceeding with a CBDC transaction. The account-based design can be found in the Bahamas' Sand Dollar pilot, where the Central Bank of Bahamas examines the potential of the account-based Sand Dollar to defend against money laundering and other illicit activities.⁵² Another design solution of CBDC is based on digital tokens. It makes the user anonymous through the cryptographic scheme without the requirement of identification.⁵³ The token-based design would ensure universal access as it has cash-like attributes, and anybody can get access under a pseudonym.⁵⁴ Although token-based CBDC protects user privacy by default, central banks and other authorized institutions still have the right to track or share transaction data with participants on a need-to-know basis. In terms of the degree of anonymity, different CBDC projects have different regulations. For example, in China's DC/EP project, the identity of e-CNY users is "controllable anonymity", as high-value transactions will be traced by the central bank. It is also noted that to safeguard the privacy of users, the PBOC will not provide information to third parties (including the government) unless required by law and regulation.⁵⁵

In a nutshell, central banks around the world are exploring at least four levels of CBDC design. Firstly, according to the targeted users, CBDCs can be divided into the retail model and the wholesale model. In the retail design

mechanism, financial transaction systems can be integrated into a one-tier system under the direct control of the central bank, while some central bank programs continue to use the two-tier system. Secondly, as for the scope of application, CBDC programs of central banks can be generally divided into the domestic type and cross-border type. Wholesale CBDCs are more focused on the latter, as institutions have a greater need to improve the quality of cross-border transactions. In terms of cross-border wholesale CBDC, there are three kinds of models to choose from: no third-party, jointly managed corridor network, and shared m-CBDCs network. Thirdly, given the infrastructure technology of CBDCs, most central banks attempt to unlock the potential of DLT in the design of CBDCs to improve accessibility and transparency, while a few projects use traditional centrally controlled infrastructure. Finally, regarding user access mechanisms, customers of CBDCs may have two ways to get access. The first is similar to current bank accounts, where CBDC access is tied to the users' identity; and the second is cash-like, which provides users with relative anonymity to protect their privacy. Notably, some of the options are not exclusive, and numerous central banks have attempted to explore hybrid models that combine the advantages of different options.

Practical and regulatory issues of E-CNY pilot in China

It appears that China is now at a crucial crossroads in CBDC design. The PBOC's latest working paper in July 2021 states that it is attempting to explore the potential of e-CNY in terms of (1) retail model with a two-tier system⁵⁶; (2) domestic and cross-border types⁵⁷; (3) a combination of DLT technology and centralized management⁵⁸; and (4) cash-like controllable anonymity.⁵⁹ For the development of retail CBDCs, the BIS summarized four characteristics necessary for the retail model to be trusted and widely used: stability, accessibility, convenience, and security.⁶⁰ Therefore, in addition to theoretically analyzing the different design models of CBDCs in various countries, it is necessary to further investigate the actual practices and related regulations of e-CNY experiments and to conduct an empirical study incorporating the four necessary features of CBDCs. This chapter interrogates the pilot experience of China's e-CNY, analyses the Cybersecurity Law, DSL, PIPL, as well as the

⁴⁷ Auer and Böhme, *supra* note 21, at 92.

⁴⁸ *Ibid.*

⁴⁹ Arauz and Garratt [4] Dinero Electrónico: The Rise and Fall of Ecuador's Central Bank Digital Currency. *Latin American Journal of Central Banking* 2(2), 100,030.

⁵⁰ Auer and Böhme, *supra* note 21, at 86.

⁵¹ *Ibid.*, at 93.

⁵² Central Bank of the Bahamas, *supra* note 25, at 4.

⁵³ Auer and Böhme, *supra* note 21, at 88.

⁵⁴ *Ibid.*

⁵⁵ PBOC Working Group, *supra* note 4, at 7.

⁵⁶ *Ibid.*, at 3–4.

⁵⁷ *Ibid.*, at 4–5.

⁵⁸ *Ibid.*, at 10–11.

⁵⁹ *Ibid.*, at 5, 7, 9.

⁶⁰ Auer, R. and Böhme, R. (2020) The Technology of Retail Central Bank Digital Currency. *BIS Quarterly Review*, March.

specific Personal Information Protection Policy in e-CNY practice. It identifies gaps between practice and design concepts and highlights current regulatory issues in China's DC/EP project.

E-CNY Pilot in China

In DC/EP program, e-CNY is a legal tender, a liability of the central bank to the public, and a mainly substitute for cash in circulation (M0).⁶¹ Therefore, the e-CNY is certainly secure as it is backed by the sovereign credit of China.

As for the convenience of e-CNY, the DC/EP program has established pilots in ten cities⁶² and scenarios in the 2022 Beijing Winter Olympics to promote the domestic use of digital currency in China.⁶³ As of June 2020, the Chinese digital currency experiment has covered more than 1.32 million scenarios where merchants accept payments from customers using e-CNY, as well as 20.87 million individual users and 3.51 million corporate users who can use e-CNY payment services in their daily transactions, such as utility bill payment, shopping and catering, and public services.⁶⁴ Thus, the convenience of using digital payment services was evident in the DC/EP pilot. It was also observed that customers could make payments in real-time via QR codes or Near-Field Communication (NFC).⁶⁵ The current experience of paying with e-CNY is similar to that of mobile payments, but users can make offline transactions with the NFC technology, thereby increasing the convenience and stability of transactions.⁶⁶

In terms of accessibility, it should be noted that since the digital currency is still in the process of experimentation, cash-like universal accessibility has not yet been achieved, and only invited corporates and residents in pilot cities can use e-CNY services. Individuals who would like to participate in the experiment will need to apply for eligibility by providing their name or pseudonym and phone number to

the PBOC Digital Currency Institute or an authorized commercial bank.

Of the four necessary features of retail CBDCs, the most significant issue that should be concerned is privacy safeguards. According to the latest survey conducted by the European Central Bank in 2021, people are most concerned about the digital Euro in terms of user privacy.⁶⁷ Thus, it is important for policymakers to technically balance the protection of individual privacy with the monitoring of illicit transactions. As mentioned above, customers who want to use the e-CNY payment service should apply with their phone number, which is managed by the telecom companies. Changchun Mu, director of the Digital Currency Institute, said that under current regulations, telecom operators cannot divulge subscriber information to third parties such as the PBOC, thus the phone number-based accounts are completely anonymous to the PBOC and other payment service providers.⁶⁸ In practice, according to the current rules regarding telephone subscriber information, telecom service operators are required to register the true identity of subscribers,⁶⁹ which is supervised by the Ministry of Industry and Information Technology and local communications administrations in accordance with the law.⁷⁰ In other words, under the existing law, subscriber information may not be disclosed by telecom operators to the PBOC, but operators may provide user information to central and local communications regulatory authorities. Besides, it is worth noting that telecom operators and regulators are not allowed to provide information to others after obtaining subscriber information; and when the information is obtained in the performance of functions to protect cybersecurity, the obtained information could only be used for the purpose of maintaining cybersecurity.⁷¹

⁶¹ PBOC Working Group, *supra* note 4, at 2–3.

⁶² Up to now, pilot cities for e-CNY include Shenzhen, Suzhou, Xiong'an, Chengdu, Shanghai, Hainan, Changsha, Xi'an, Qingdao, and Dalian. *See, ibid.*, at 13.

⁶³ *Ibid.*

⁶⁴ *Ibid.*

⁶⁵ The Paper (2020) Shuzi Renminbi Quanliucheng Tiyan, Yiwen Daini Kankan Meixiangdao De Xijie (数字人民币全流程体验, 一文带你看看没想到的细节) [Full Experience of E-CNY, an Article to Show the Unexpected Details], 15 October, https://www.thepaper.cn/newsDetail_forward_9571162, accessed 10 September 2021.

⁶⁶ Wu, Y. et al., Shuzi Renminbi Shidian “Kuorong”, “Hua” Yang Fanxin (数字人民币“扩容”, “花”样翻新) [E-CNY Pilot Expansion with Innovative Consuming Method], 21 April, http://www.xinhuanet.com/fortune/2021-04/21/c_1127358019.htm, accessed 10 September 2021.

⁶⁷ Ikeda (2021) European Central Bank CBDC Survey Finds Privacy Is the Number One Concern for Digital Euro, 5 May, <https://www.cpomagazine.com/data-privacy/european-central-bank-cbdc-survey-finds-privacy-is-the-number-one-concern-for-digital-euro/>, accessed 10 September 2021.

⁶⁸ Du (2021) Yanghang Hui Zhangwo Yonghu Xinx, Qinfan Yinsi Ma? Mu Changchun Xiangjie Shuzi Renminbi “Kekong Niming” (央行会掌握用户信息、侵犯隐私吗?穆长春详解数字人民币“可控匿名”) [Will Central Banks Have User Information and Violate Privacy? Changchun Mu Explains “Controllable Anonymity” of E-CNY], 20 March, <https://www.yicai.com/news/100993230.html>, accessed 10 September 2021.

⁶⁹ Provisions on the Registration of True Identity Information of Telephone Subscribers (promulgated by the Instrumentalities of the State Council, All Ministries, Ministry of Industry and Information Technology, 16 July 2013, effective 1 September 2013), CLI.4.207022(EN) (Lawinfochina), article 3.

⁷⁰ *Ibid.*, article 4.

⁷¹ Cybersecurity Law of the People's Republic of China (promulgated by the Standing Committee National People's Congress, 11 July 2016, effective 1 June 2017), CLI.1.283838(EN) (Lawinfochina) [18], article 30.

Furthermore, according to the Draft for Public Solicitation of Comments of PRC People's Bank of China Law (PBOCL) released in 2020, the central bank would be responsible for establishing a national financial database, collecting and managing national financial industry statistical data and relevant information, and it shall establish a supervisory and management information sharing mechanism with the Financial Stability Development Committee of the State Council.⁷² In other words, both the central bank and the Financial Stability Development Committee might have the ability to access digital currencies user information in the future. Thus, although there are no established specific regulations in China regarding the data processing of CBDC user information, potential conflicts between the design assumptions of the DC/PE project—cash-like controllable anonymity—and existing or planned regulations have gradually emerged.

It is understandable that the PBOC would need to process user's information in certain circumstances—after all, one of the significant functions of the CBDC is to suppress illegal financial activities, such as tele-fraud, online gambling, money laundering, tax evasion, and terrorism financing.⁷³ However, with the rise of CBDC in China, the boundaries of the protection and appropriate use of customer information for digital currencies need to be clarified. As mentioned above, China's DC/EP pilot adopts a controllable anonymity theory that classifies access to users' personal information into different levels based on the value of user transactions, i.e., the small value is anonymous, and the large value is traceable.⁷⁴ The PBOC describes this controllable anonymous connection between user's commercial bank accounts and their e-CNY wallets as a “loosely coupled account link”. In practice, it is observed that there are currently four types of digital currency wallets available to the general public (see the following Chart), but except for the money in “red packets” freely distributed by the PBOC, the vast majority of users need to first bind their bank account and top up money from the bank account to the digital wallet, i.e., upgrade the digital wallet to Level II, which requires not only registering an account with their phone number but also requires the user to authenticate with their real name and bind their bank account. In addition, in the current digital currency experimental system, e-CNY users cannot connect their bank accounts to their e-CNY accounts without identity

authentication. Therefore, in most cases, PBOC can obtain user information when the user starts using e-CNY.⁷⁵

Different Levels of e-CNY Wallet in the Pilot

Wallet Type	Requirements for users	Wallet balance cap (RMB)	Single transaction cap	Daily transaction cap	Annual transaction cap
Level IV	Register with phone number	10,000	2000	5000	50,000
Level III	Authentication with Chinese Resident Identity Card	20,000	5000	10,000	No limit
Level II	Debit card binding	500,000	50,000	100,000	No limit
Level I	Bank counter certification	No limit	No limit	No limit	No limit

In addition to the telecom service operators and the PBOC, other related payment service providers were found to have potential access to user personal information during the e-CNY pilot. As mentioned above, China adopts a two-tier operating system for payment services: the central bank allocates quotas to designated commercial banks, which provide digital currency exchange and circulation services.⁷⁶ There are no uniform criteria for selecting designated banks and no disclosure of the amount of digital currency that commercial banks can have. What is certain, however, is that these designated commercial banking industries have the opportunity to access users' e-CNY account information.

In the beta version of the e-CNY wallet mobile application, there are currently seven commercial banks authorized to provide digital currency services, including six state-owned commercial banks⁷⁷ and one private-owned commercial bank (Zhejiang E-Commerce Bank), the latter of which has an inextricable relationship with Alipay—one

⁷² Notice by the People's Bank of China of the Request for Public Comments on the Draft to Revise the Law of the People's Republic of China on the People's Bank of China (Revision Draft for Comments) (promulgated by the People's Bank of China, 23 October 2020, deadline for comments 23 November 2020), CLI.4.15106(EN) (Lawinfochina) [31], article 41, 51, 52.

⁷³ PBOC Working Group, *supra* note 4, at 7.

⁷⁴ *Ibid.*

⁷⁵ The data are based on China's central bank digital yuan wallet application ‘e-CNY’ developed by the digital currency research institute of the PBOC.

⁷⁶ PBOC Working Group, *supra* note 4, at 8.

⁷⁷ These six state-owned commercial banks are regarded as China's six largest banks, including China Construction Bank, Industrial and Commercial Bank of China, Agricultural Bank of China, Postal Savings Bank of China, Bank of Communication, and Bank of China.

of the most successful mobile payment platforms in China. Before customers accept the digital currency services of commercial banks, they need to read and agree to the e-CNY Wallet User Service Agreement and the commercial bank's E-CNY Personal Information Protection Policy, respectively. According to these two legal documents, the designated commercial bank can collect digital currency user's personal information⁷⁸ and account information.⁷⁹ If the customer refuses to provide it, the only mobile application available for e-CNY transactions in the pilot will not have access to the bank account.⁸⁰ Furthermore, the protection policy specifies that commercial banks may collect, use, share, transfer, or even publicly disclose user's personal information.⁸¹

In summary, although the director of the Digital Currency Institute in China said that e-CNY wallets opened with telephone numbers are "completely anonymous" to the PBOC and the other operators,⁸² the current experiences show that telecom operators, telecom supervisory authorities, the PBOC, and delegated commercial banks all have the opportunity to access user's personal information. Admittedly, as e-CNY is still in its trial stage, the PBOC has not yet disclosed the technology and methods for protecting users' privacy, and it is unknown how the relevant service providers will collect and store the data and how they will prevent misuse or abuse of digital information. Furthermore, only delineated corporates and selected individuals in pilots can download the e-CNY application for registration and transactions, and regulations regarding the personal information of digital currency users have not yet been established, further investigation and research will be required in the future.

Current regulatory issues in digital currency personal information

In addition to technical protection of privacy, legal regulation of the personal information related to digital currency is also needed. In fact, the absence of specific regulations for digital currency user information does not simply mean that there are no existing legal provisions to protect customer information. This part will then analyze the impact

of existing regulations, particularly the newly enacted DSL and PIPL in 2021, on the protection of personal information related to digital currencies.

(1) Definition and protection principles of personal information

Under the current law, personal information in China refers to all kinds of information that can be used to identify natural persons— except for the information that has been anonymized.⁸³ According to the DSL and PIPL, any operational activity related to information (also called "data") is referred to as "information processing"⁸⁴ or "data processing",⁸⁵ which generally includes, but is not limited to, the collection, storage, use, processing, transmission, provision, disclosure, and deletion.⁸⁶

As regulated in the PIPL, the processing of personal identifiable information needs to comply with the principles of lawfulness, legitimacy, necessity, good faith,⁸⁷ clear and reasonable purpose, minimum impact and scope,⁸⁸ openness and transparency, and disclosure its processing rules, purposes, methods, and scope.⁸⁹ However, there is a gap between the information processing principles and the policies implemented in the e-CNY pilots. For example, according to the current digital currency personal information protection policies of Postal Savings Bank, when using its digital currency services, the individual's mobile device model, operating system, unique device identifier, logged-in IP address are collected with the purpose of proper operation of the service and security of the user's account.⁹⁰ However, such purpose is not clear, as it fails to disclose the criteria for "proper" or enumerate certain scenarios that could be considered "proper operations" or "safeguarding accounts". It is also questionable whether the process of customer's device information (such as unique device identifier) is consistent

⁷⁸ Including but not limited to the user's name, gender, nationality, place of birth, date of birth, type of ID, ID number and expiration date, personal biometric information, communication and contact method, place of residence or workplace address, family information, occupation information, account information, and property information.

⁷⁹ See, e.g., Zhejiang E-Commerce Bank E-CNY Wallet Personal Information Protection Policy, article 2.1 and article 2.2.

⁸⁰ *Ibid*, article 2.2.

⁸¹ See *Ibid*, article 3.1 and article 5.3.1.

⁸² Du, *supra* note 68.

⁸³ Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, 20 August 2021, effective 1 November 2021) [33], CLI.1.5055321(EN) (Lawinfochina), article 2 and 73.

⁸⁴ *Ibid*, article 4.

⁸⁵ Data Security Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, 10 June 2021, effective 1 September 2021), CLI.1.5015167(EN) (Lawinfochina) [19], article 3.

⁸⁶ *Ibid*, the latest 2021 PIPL further adds that the deletion of personal information is also a form of information processing, see PIPL, *supra* note 83, article 4.

⁸⁷ *Ibid*, article 5.

⁸⁸ *Ibid*, article 6.

⁸⁹ *Ibid*, article 7.

⁹⁰ Postal Savings Bank E-CNY Wallet Personal Information Protection Policy, article 1.4, accessed from the terms of using e-CNY through Postal Savings Bank account in the 'e-CNY' application.

with the “minimum impact and scope” principle. Indeed, whether accurate unique device identifiers are necessary for commercial banks when customers make payments using e-CNY with M0 attributes is an issue that requires commercial banks to further consider and provide a compelling justification to public users.

(2) Processing of different personal information

According to the Cybersecurity Law and DSL, China implements a “categorized and hierarchical data protection system” which employs different levels of protection depending on the significance of the data.⁹¹ In this case, information related to digital currencies would be considered critical as it relates to the financial sector that concerns the national economy, and the state will take a high level of protection to secure it.⁹²

Unlike the former that classifies the importance of data based on the industries and fields, the PIPL classifies personal information into two categories: (1) general personal information and (2) sensitive personal information. According to the PIPL, sensitive information specifically refers to information that, if disclosed or used unlawfully, could easily lead to the violation of personal dignity or damage to the safety of persons or property.⁹³ As for the processing of sensitive information, the processor is expected to meet the following conditions: (1) has its specific purposes, sufficient necessity, as well as strict protection measures;⁹⁴ (2) the individual is notified of its necessity and its impacts;⁹⁵ and (3) the individuals’ separate consent is obtained.⁹⁶ Similarly, e-CNY related service providers classify customers’ information into general information and sensitive information,⁹⁷ however, most commercial banking policies do not further detail the conditions or obligations of service providers to process sensitive information of e-CNY users. While the PIPL applies by default to all sensitive information processing practices of digital currency service providers, the absence of specific commercial bank operational processes and related obligations in the pilot customer information protection policy may lead to regulatory gaps in the protection of sensitive information of e-CNY users.

(3) Deletion of personal information

The collected personal information is required to be returned or deleted by the processor when the commission contract is terminated.⁹⁸ However, some commercial banks’ personal information protection policies in the current digital currency pilots stipulate that if the service is terminated, the commercial bank will stop collecting, anonymize the previously collected information or continue to use the previous information when it related to archiving, auditing, anti-money laundering, co-supervising, etc.⁹⁹ Other commercial banks do not determine the process of personal information upon termination of an e-CNY account, stipulating only that personal information will be “deleted or anonymized”.¹⁰⁰ In this context, there are potential conflicts between the current process of digital currency user’s information in the pilot and the new PIPL: Firstly, anonymizing previous information is not the same as the “anonymization” stipulated in the PIPL. According to the PIPL, anonymized personal information is not identifiable and cannot be recovered after anonymous processing. However, this contradicts the exceptions provided by the e-CNY service provider, where anonymized information can still be processed in certain circumstances, such as for anti-money laundering or regulatory purposes.

Secondly, if the anonymized information is not fully anonymized as specified in the PIPL, i.e., if the anonymized information can be recovered and used to identify individuals under specific circumstances, then the so-called anonymized information of the e-CNY service providers will be managed by the PIPL as personal information. However, in the new PIPL, the only two exceptions to the deletion of the previous information are (1) the retention period of the information prescribed by laws and administrative regulations has not expired; and (2) deletion of the previous information is technically difficult to realize;¹⁰¹ and in both exceptions, the information processor could only have two ways of processing previous information—(1) storing and (2) taking the necessary security measures to protect the information.¹⁰² Therefore, unless there are other laws and administrative regulations, commercial banks are not required to use the previous information for archiving, auditing, anti-money laundering, or regulatory purposes, let alone provide and disclose it to others. Although considering the

⁹¹ Cybersecurity Law, *supra* note 71, article 31; *ibid*, article 21.

⁹² *Ibid*.

⁹³ PIPL, *supra* note 83, article 28.

⁹⁴ *Ibid*, article 28.

⁹⁵ *Ibid*, article 30.

⁹⁶ *Ibid*, article 29.

⁹⁷ Zhejiang E-Commerce Bank E-CNY Policy, *supra* note 79, article 2.1.2. According to the policy, sensitive personal information of e-CNY users mainly includes ID number, personal biometric information, bank account number, credit information, property information, transaction information, etc.

⁹⁸ PIPL, *supra* note 83, article 21.

⁹⁹ See, e.g., Zhejiang E-Commerce Bank E-CNY Policy, *supra* note 79, article 4.4; China Construction Bank E-CNY Wallet Personal Information Protection Policy, article 2.2.

¹⁰⁰ See, e.g., Agricultural Bank of China E-CNY Wallet Personal Information Protection Policy, article 4.1.2 and 5.4.

¹⁰¹ PIPL, *supra* note 83, article 47.

¹⁰² *Ibid*.

pilot policy of digital currency service providers in China, the provider would delete its collected information upon request by e-CNY customers,¹⁰³ the process and manner in which customers could make such deletion requests remains uncertain.

(4) Regulation of personal information processor

According to the existing law, personal information processors are responsible for their activities and have an obligation to protect the information they process.¹⁰⁴ There are currently at least five types of institutions responsible for supervising and managing the conduct of processors. To begin with, the national cyberspace authority is the body with overall responsibility for regulation, mainly engaged in the overall planning and coordination of the protection of personal information at the national level.¹⁰⁵ Second, different departments of the Chinese State Council undertake the responsibility of supervising personal information protection within their respective functions.¹⁰⁶ Third, different departments of the local government bear the responsibility of regulation within their respective functions in their administrative areas.¹⁰⁷ Fourth, public, and national security authorities have a responsibility to oversee personal information protection and data security within their respective mandates.¹⁰⁸ Last but not least, some responsible processors of personal information also need to be supervised by an independent institution composed of external persons.¹⁰⁹

As mentioned above, there are several potential processors of digital currency user information in China's e-CNY pilot, including telecom operators, telecom supervisory authorities, the PBOC, and delegated commercial banks. While there is no clearly identified regulator for the processing of personal information by all CBDC-related institutions in China, it is no doubt that for information processed by telecom operators, their activities are regulated by national and local telecom administrative organs—the Ministry of Industry and Information Technology and local communications administration.¹¹⁰ The relevant telecom supervisory authorities and the PBOC would conduct their activities under the

supervision of their higher administrative authorities, such as the State Council.

However, for commercial banks that provide retail CBDC daily business, the specific regulator remains unclear: on the one hand, the China Banking and Insurance Regulatory Commission (CBIRC) is currently the main responsible authority for supervising and regulating the conduct of commercial banks; on the other hand, according to the latest working paper on digital currencies released by the PBOC, the PBOC is responsible for regulating the whole circulation of e-CNY and exploring the development of management methods for e-CNY to enhance the protection of personal information.¹¹¹ Furthermore, since commercial banks generally have a huge number of users and provide important financial services to them, the monitoring and protection of e-CNY customers' information meet the prerequisites of Article 58 in PIPL.¹¹² Therefore, commercial banks need to establish an independent institution composed mainly of external members to monitor the protection of users' personal information, and regularly issue their social responsibility reports on personal information for public scrutiny. Theoretically, multiple regulators could provide more comprehensive supervision for commercial banks. However, in practice, multiple regulations seem more likely to lead to the unclear delineation of responsibilities among various regulators, resulting in coordination costs, regulatory gaps, or regulatory overlaps.¹¹³

In conclusion, there are gaps between the current pilot policies of e-CNY in China and the regulation of personal information protection of digital currency customers. Further, the existing regulatory provisions do not provide comprehensive legal protection for digital currency users. Thus, there is a need to reconsider the future development of the regulatory framework for digital currency service providers, as well as the forward-looking provisions regarding the CBDC in China.

Proposed regulatory framework for CBDC in China

The regulation of CBDC needs to strike a balance between information protection and supervisory compliance. On the one hand, protecting user's personal information is a primary regulatory consideration; on the other hand, financial service

¹⁰³ Zhejiang E-Commerce Bank E-CNY Policy, *supra* note 79, article 6.2.

¹⁰⁴ PIPL, *supra* note 83, article 9.

¹⁰⁵ DSL, *supra* note 85, article 6; PIPL, *supra* note 83, article 60.

¹⁰⁶ *Ibid.*

¹⁰⁷ PIPL, *supra* note 83, article 60.

¹⁰⁸ DSL, *supra* note 85, article 6.

¹⁰⁹ PIPL, *supra* note 83, article 58.

¹¹⁰ True Identity Information of Telephone Subscribers, *supra* note 69, article 4.

¹¹¹ PBOC Working Group, *supra* note 4, at 14–15.

¹¹² PIPL, *supra* note 83, article 58.

¹¹³ Bischof, J. et al. (2021) A Tale of Two Supervisors: Compliance with Risk Disclosure Regulation in the Banking Sector. *Contemporary Accounting Research*, advance online publication 8 July, 10.1111/1911–3846.12715.

providers need to comply with “know-your-customer” guidelines to prevent criminal activities. The protection of the personal information of CBDC users is closely related to the success of digital currency generalization, and information protection is particularly important when the PBOC attempts to collaborate with other central banks to find the potential of m-CBDCs. This chapter, therefore, proposes a regulatory framework for CBDC information protection in China, linking digital currency protection to existing regulations, and discussing the identity of regulators and their specific rights and obligations within the future CBDC regulatory framework in China.

Refine the classification of information processing

The current classification of personal information protection is broadly divided into two types: the first classification is based on industry, which classifies information into general industry information and important industry information; and the second is based on whether the information is sensitive, classifying personal information into general information and sensitive information. The obligations of information processors differ according to the significance of the information—important industry and sensitive information require more processing prerequisites and protection measures. However, current regulations do not classify the processing of information, and different categories of processing may have varying effects on users.

More specifically, based on the degree of the potential impact of information processing on individuals, the information processing may be classified into (1) general information processing (e.g., collection, storage, use, and delete); (2) information processing involving third parties (e.g., transmission, provision, etc.); and (3) disclosing information. As for the second and third types of information processing, additional obligations need to be imposed on information processors.

In terms of general information processing, as mentioned above, there is a potential conflict between the PIPL and commercial banks’ policies regarding the deletion of customers’ personal information. This article suggests that commercial banks’ policies need to clarify whether they would anonymize or delete users’ personal information when the service ends. On the one hand, the commercial bank policy, in the name of “anonymization”, does not remove the identifiability of personal information as it can still be processed in certain cases. The policy needs to be modified to comply with the PIPL. On the other hand, considering the secrecy of financial crimes or crimes related to digital currencies, the complete deletion or anonymization of personal information may not be conducive to the tracking and investigation of crimes committed before the service is terminated. Thus, it is recommended that (1) a well-protected, specialized system

could be established to store the personal information of deregistered users; (2) relevant authorities, such as public security and national security authorities, may determine a reasonable period for the continued storage of the personal information; and (3) the law should establish prerequisites for the processing of information and require strict approval and necessity review by an independent third party for processing other than storage and adoption of protective measures.

Secondly, according to Article 23 in PIPL, when transmitting and providing information to others, the information processor is expected to notify the individual of the recipient’s basic information, including but not limited to its purposes, name, and contact number. Further, the consent of the individual has required if the domestic recipient changes the original purposes or methods of the processing;¹¹⁴ while for recipients outside of China, in addition to notification, the processor transmission and provision requires the individual’s separate consent.¹¹⁵ Considering that the information transmission would increase the risks of information leakage and that the absence of a separate consent may undermine the individual’s privacy self-management rights.¹¹⁶ It is suggested that in the case of domestic information transmission, separate consent is required for any processing of information, i.e., not only for changes in the purpose and method of processing, but all processing requires the individual’s separate consent.

As for the disclosure of information, processors need to obtain the individual’s separate consent before disclosing personal information.¹¹⁷ Nonetheless, considering that the disclosure of personal information could easily lead to irreversible effects on individuals, processors are recommended further to inform individuals of the possible effects of disclosure and warn of the risk of disclosure.

In short, it is recommended to improve the regulation of different types of processing information to provide more comprehensive protection for digital currency customers.

Enhance the compliance of CBDC service providers

As analyzed in Sect. “[Practical and regulatory issues of E-CNY pilot in China](#)”, there are a number of information protection issues related to individual e-CNY service providers in the pilot. Especially after the establishment of the new DSL and PIPL, commercial banks’ information protection policies should be refined and revised to comply with

¹¹⁴ PIPL, *supra* note 83, article 23.

¹¹⁵ *Ibid*, article 39.

¹¹⁶ Solove [35] Introduction: Privacy self-management and the consent dilemma. Harvard Law Review 126: 1880–1883.

¹¹⁷ PIPL, *supra* note 83, article 25.

the current regulations. In addition, all the digital currency service providers are expected to establish their personal information protection compliance system for digital currency users and be subject to regular review and oversight by external independent institutions as well as regulators.

In such cases, the know-your-customer institutions need to reconsider the reasonableness and necessity of the purposes for which they process personal information, particularly for the processing of sensitive information. Further, service providers are required to clearly inform e-CNY users of the specific purpose of their information processing practices, and any further processing that is inconsistent with that purpose, with exception as provided by law and administrative regulations, may require separate notification and get consent from the user. Thus, for the aforementioned example of commercial banks processing information related to personal mobile devices, banks are expected to explain their reasons for doing so.

In spite of self-censorship, external regulation is necessary to monitor the compliance of digital currency information protection obligators, which brings this chapter to the next suggestion regarding regulatory authorities for CBDC information processors.

Reshape the regulatory authority framework for CBDC service providers

As mentioned above, the multiple regulatory authorities of the commercial bank would lead to coordination costs, regulatory gaps, or overlaps in practice, thus it is necessary to clarify the major regulator of the information processing of CBDC service providers. Generally, the regulator of commercial banks in China is the CBIRC, which mainly regulates and supervises the market conduct of banks. In terms of specific CBDC users' personal information protection, the CBIRC is responsible for regulation. According to the existing established PBOCL, the PBOC is responsible for macro-control and maintaining the stability of the banking industry, and there is no provision for the PBOC to regulate the CBDC information of commercial banks.

Nonetheless, according to the latest revised draft of PBOCL, the regulatory scope of PBOC includes but is not limited to banks, financial asset management companies, trust and investment companies, and finance companies. Further, the PBOCL 2020 draft attempts to stipulate that PBOC is responsible for developing the fundamental system for financial consumer protection and leading the establishment of a coordination mechanism for financial consumer protection. Thus, the overall regulator of CBDC personal information protection is likely to be the PBOC in the future. In this context, it is significant to delineate the future rights and obligations of the CBIRC and PBOC.

First of all, while the national cyberspace administration is responsible for the overall supervision of personal information protection, the general planning and management institution concerning the information protection of digital currency shall be the PBOC. It is because that the information protection of digital currency is related to the credibility and stability of the whole financial system. PBOC, as the authority responsible for the issuance and circulation of digital currency, is more appropriate as the macro regulator of CBDC information.

Secondly, specific supervision of the protection of digital currency user information in commercial banks shall be carried out by the CBIRC. In other words, the daily processing of user information by commercial banks is supervised by the CBIRC, and the PBOC is responsible for coordinating and centrally supervising the information processing of multiple e-CNY service providers.

As for the external independent institution established for oversight purposes, considering that the independent institution is not a government authority, it is recommended that the institution shall be required to conduct independent reviews and disclose audit reports on the information processing of commercial banks and other digital currency service providers. Further, the regulations on the independent institution should be more specific about its composition, obligations, and relationship with other supervisors.

Specify the authority and prerequisites to 'Know-your-customer'

One of the overarching concerns in the design of the CBDC regime is to combat illegal activities involving currency transactions, which requires a balance between information protection and regulatory compliance. The PBOC emphasizes that the CBDC system collects less information on transaction payments than traditional e-money transactions because of its controllable anonymity and that CBDC transaction authorities shall not provide user information to third parties, including unauthorized government agencies unless otherwise required by law and other regulations.¹¹⁸ In this case, the anonymity of the CBDC design is necessarily required to meet the prerequisite of suppressing illegal activities such as money laundering, terrorist financing, and tax evasion.

The PBOC currently employs the size of the transaction amount to classify the degree of user information anonymity. However, when criminals use multiple user accounts to bypass the traceability requirements for large transactions and satisfy their criminal purposes through multiple anonymous small transactions, relying solely on the transaction

¹¹⁸ PBOC, *supra* note 4, at 7.

amount as the criterion for anonymizing user information may not fully combat illegal activities involving the misuse of CBDC. The difficulty of identifying user identity in the case of the small volume of transactions may hinder the fight against crime, so how to transmit information legally to reduce illegal crime is an issue that requires checks and balances. It is proposed to link CBDC transaction information to big data analytics, where authorized CBDC trading institutions are entitled to monitor payment transactions as stewards and to de-anonymize suspicious transactions when needed to combat illegal activities. In other words, anonymization does not mean that CBDC transaction information cannot be recorded and tracked. Further regulations regarding access to CBDC user information to combat crime are proposed to grant the relevant CBDC transaction agencies the right to monitor payment transactions, to conduct real-time monitoring and big data analysis of the frequency of transactions and transaction amount, etc., and to determine the prerequisites for the agencies to know their customers. The latest research report released by the PBOC lists several criminal activities with e-CNY that may require to be guarded, including but not limited to telecom fraud, online gambling, money laundering, and tax evasion.¹¹⁹ Nevertheless, the PBOC does not specify how to prevent such illegal activities with e-CNY misuse. It is recommended that the de-anonymization of CBDC user information and its transmission to other government agencies be specified and regulated by law in order to combat these criminal activities.

Conclusion

China has recently announced the outline of its 14th Five-Year Plan for National Economic and Social Development, deciding to establish a sound modern financial system with a high degree of adaptability, competitiveness, and universality, of which the digital currency is expected to be a significant component.¹²⁰ In such context, it is significant to examine the design and regulation of CBDCs based in China and with a global perspective. This article provides a comprehensive review of the design of CBDCs in various countries and, on this basis, illustrates the current design choices in China. It is the first article to analyze current e-CNY practice

and regulatory issues in detail through empirical and doctrinal studies, concluding that there are gaps between e-CNY design and practice, between practice and regulation, and between regulation and the expected information protection mechanism.

E-CNY in China has tremendous potential in the financial services sector, but many challenges must first be overcome. Considering the large number of digital currency users involved in the retail CBDC, improving the protection of user's information is a necessity. This article identifies the main issues of e-CNY in pilots and attempts to provide several suggestions for improving the protection of digital currency information. Although this paper has not further examined the issue of cross-currency and cross-border payments of e-CNY, it is necessary to address the practical and regulatory issues revealed in the current DC/EP pilot before discussing the internationalization of e-CNY. In this regard, this paper provides a sound basis for future research on the cooperation and transactions of multiple CBDCs.

Declarations

Conflict of interest The author states that there is no conflict of interest.

References

1. Adrian, T. and Mancini-Griffoli, T. 2019. The Rise of Digital Money. *Annual Review of Financial Economics*, 13(1).
2. Agur, I., Ari, A. and Dell'Ariccia, G. 2021. Designing central bank digital currencies. *Journal of Monetary Economics*. Available online 8 May 2021, <https://doi.org/10.1016/j.jmoneco.2021.05.002>.
3. Allen, S. et al. 2020. Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. Massachusetts, US: National Bureau of Economic Research. NBER Working Paper no. 27634
4. Arauz, A. and Garratt, R. 2021. Dinero Electrónico: The Rise and Fall of Ecuador's Central Bank Digital Currency. *Latin American Journal of Central Banking* 2(2), 100030.
5. Auer, R. and Böhme R. 2021. Central Bank Digital Currency: the Quest for Minimally Invasive Technology. Basel, Switzerland: Bank for International Settlements. BIS Working Paper no. 948.
6. Auer, R., Cornelli, G., and Frost, J. 2020. Taking Stock: Ongoing Retail CBDC Projects. *BIS Quarterly Review*, 1 March, https://www.bis.org/publ/qtrpdf/r_qt2003z.htm, accessed 31 December 2021.
7. Auer, R., Cornelli, G., and Forest, J. 2020. Rise of the central bank digital currencies: drivers, approaches and technologies. Munich, Germany: CESifo Working Paper no. 8655
8. Bech, M. L. and Garratt, R. 2017. Central Bank Cryptocurrencies. *BIS Quarterly Review* September.
9. Bindseil, U. 2010. Central Bank Digital Currency: Financial System Implications and Control. *International Journal of Political Economy* 48 (4): 303–335.
10. BIS. 2015. Digital Currencies, Basel, Switzerland: Committee on Payments and Market Infrastructures. BIS Working Paper no. 1146.

¹¹⁹ *Ibid.*

¹²⁰ PRC Government (2021) Zhonghua Renmin Gongheguo Guomin Jingji He Shehui Fazhan Di Shisige Wunian Guihua He 2035 Nian Yuanjing Mubiao Gangyao (中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要) [Outline of the Fourteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China and the 2035 Visionary Goals], 12 March, http://www.gov.cn/xinwen/2021-03/13/content_5592681.html, accessed 12 September 2021.

11. BIS. 2017. Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework, Basel, Switzerland: Committee on Payments and Market Infrastructures. CPMI Paper no. 157.
12. BIS. 2021. CBDCs: an Opportunity for the Monetary System. Basel, Switzerland: Bank for International Settlements. Basel, Switzerland: Bank for International Settlements. BIS Annual Economic Report.
13. BIS. 2021. Central bank digital currencies for cross-border payments: report to the G20, July, <https://www.bis.org/publ/othp38.pdf>, accessed 2 January 2022
14. BIS. 2021. Central Bank Digital Currencies: Financial Stability Implication. Basel, Switzerland: Bank for International Settlements. BIS Report No. 4
15. Boar, C. and Wehrli, A. 2021. Ready, Steady, Go?—Results of the Third BIS Survey on Central Bank Digital Currency. Basel, Switzerland: Bank for International Settlements. BIS Working Paper no. 1146.
16. Bordo, M.D., and Levin, A.T. 2017. Central Bank Digital Currency and the Future of Monetary Policy. Massachusetts, US: National Bureau of Economic Research. NBER Working Paper no. 237611
17. Cunha, P. R. et al. 2021. From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution. *Future Internet* 13(7).
18. Cybersecurity Law of the People's Republic of China (promulgated by the Standing Committee National People's Congress, 11 July 2016, effective 1 June 2017), CLI.1.283838(EN) (Lawinfochina).
19. Data Security Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, 10 June 2021, effective 1 September 2021), CLI.1.5015167(EN) (Lawinfochina).
20. Deloitte. 2020. Are Central Bank Digital Currencies (CBDCs) the Money of Tomorrow?, <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-are-central-bank-digital-currencies.pdf>, accessed 9 September 2021
21. Didenko, A.N. et al. 2020. After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems. Sydney, Australia: The European Corporate Governance Institute. ECGI Working Paper Series 65/2020.
22. Engwet, W. and Fung, B.S.C. 2017. Central Bank Digital Currency: Motivations and Implications. Ottawa, Canada: Bank of Canada. Staff Discussion Paper No.2017–16
23. Gürtler K. E. et al. 2017. Central Bank Digital Currency in Denmark? Copenhagen, Denmark: Denmarks National Bank. Analysis no. 28.
24. Jiaying, J. and Karman, L. 2021. Background and Implications of China's E-CNY, 11 January, <https://ssrn.com/abstract=3774479>, accessed 29 August 2021
25. Julin E. 2017. The Riksbank's E-krona Project. Stockholm, Sweden: Sveriges Riksbank. Report 1.
26. Kapsis, I. 2021. Should we trade market stability for more financial inclusion? The case of crypto-assets regulation in EU. In *Fin-Tech, Artificial Intelligence and the Law*, ed. A. Lui and N. Ryder, 85–104. London: Routledge.
27. Kiff, M.J. et al. 2020. A survey of research on retail central bank digital currency. Washington DC, US: International Monetary Fund. IMF Working Paper WP/20/104.
28. Mancini-Griffoli, T. et al. 2018. Casting light on central bank digital currency. Washington DC, US: International Monetary Fund. IMF Staff Discussion Note 8
29. Morales-Resendiz, R. et al. 2021. Implementing a Retail CBDC: Lessons Learned and Key Insights. *Latin American Journal of Central Banking*, 2(1), 100022
30. Norges Bank Working Group. 2019. Central Bank Digital Currencies Second Report of Working Group. Oslo, Norway: Norges Bank. Norges Bank Memo no. 2.
31. Notice by the People's Bank of China of the Request for Public Comments on the Draft to Revise the Law of the People's Republic of China on the People's Bank of China (Revision Draft for Comments) (promulgated by the People's Bank of China, 23 October 2020, deadline for comments 23 November 2020), CLI.4.15106(EN) (Lawinfochina).
32. PBOC. 2021. Working Group on E-CNY Research and Development of the PBOC. Beijing, China: Progress of Research and Development of E-CNY in China.
33. Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, 20 August 2021, effective 1 November 2021), CLI.1.5055321(EN) (Lawinfochina).
34. Saka, O. et al. 2021. Epidemic Exposure, Fintech Adoption, and the Digital Divide. CEPR Discussion Paper no. 16326.
35. Solove, D. J. 2012. Introduction: Privacy Self-management and the Consent Dilemma. *Harvard Law Review* 126 (7): 1880–1883.
36. World Economic Forum. 2021. CBDC Technology Considerations White Paper. Digital Currency Governance Consortium White Paper Series, 19 November, https://www3.weforum.org/docs/WEF_CBDC_Technology_Considerations_2021.pdf, accessed 2 January 2021.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Pangyue Cheng is a Ph.D. candidate and research assistant in the Faculty of Law at the National University of Singapore.