Balancing Privacy and Security: Theory and Practice of the E-CNY's Managed Anonymity

Author: Changchun Mu[1]

The e-CNY is the digital version of China's fiat currency and is similar to cash in circulation. To keep up with the digital economy's growing demand for privacy protection, the People's Bank of China (PBC) introduced "managed anonymity" as one of the design features of its central bank digital currency (CBDC), the e-CNY. This paper highlights the e-CNY's two-tier operating structure, wallet matrix design and user consent properties. It considers the anonymity feature of CBDCs, including international perspectives, financial integrity rules, risk prevention precautions and, in particular, the e-CNY's framework for Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) compliance. It summarises several design aspects of the e-CNY that are key to permitting "managed anonymity". Finally, the paper reflects on improving legal frameworks as well as enhancing AML/CFT capabilities. While privacy protection is considered imperative, preventing risks – including money laundering, the financing of terrorism and tax evasion – remains a priority. In all, the design of the e-CNY must reflect a delicate balance between privacy protection and risk prevention, one which will continue to be refined going forward.

Journal of Economic Literature (JEL) codes: E41, E42, E58, G21, O31
Keywords: CBDC, Central Bank Digital Currencies, e-CNY, digital currencies, anonymity, privacy, AML/CFT, Anti-Tax Evasion, digitalisation, digital economy, central banks, payments system, mobile payments, cross-border payments

1. Introduction

The e-CNY is issued by the PBC and managed by designated authorised operators. It is compatible with account-based, quasi-account and value-based methods. It is loosely coupled with bank accounts. It is equivalent to physical CNY in terms of value and legal status. The e-CNY supports managed anonymity. On the one hand, the e-CNY functions as M0 and ensures the public's legitimate anonymous transaction and personal information protection needs. On the other hand, it is designed to maintain financial security by preventing money laundering and terrorist financing, tax evasion and other criminal acts.

2. Design features of the e-CNY's "managed anonymity"

[1] Changchun Mu is the Director-General of the Digital Currency Institute at the People's Bank of China (PBCDCI). Contact PBCDCI via email: strapl@pbcdci.cn

2.1. Design principles of the e-CNY's privacy protection

In the era of big data, consumers pay increasing attention to personal privacy protection. Although electronic payments, in particular mobile payments, are more convenient than using cash, there are still consumers who choose cash for their transactions. An important reason is that cash transactions are anonymous, which naturally protects consumers' privacy. The e-CNY is a retail central bank digital currency issued to the public. It is designed to be like cash in circulation and offers the public more choice in its payment methods.

The e-CNY's design should meet the legitimate needs of individuals for anonymous transactions and strengthen the protection of consumer privacy. First, it should be compatible with the public's habit of making small-value, anonymous transactions. Second, it should ensure that consumers' personal information is not obtained by merchants and other unauthorised third parties. Third, it should protect basic consumer information collected by the authorised operators and ensure that it is not leaked. The e-CNY will coexist with physical CNY for a long time. No one will be forced to use it. In the future, the digital retail payment system, the e-CNY and the electronic account funds of designated operating institutions will operate seamlessly and constitute a cash-type payment instrument. Nevertheless, physical CNY has irreplaceable advantages compared to other payment methods. As long as there is demand for physical CNY, the PBC will not stop supplying it or mandate its disappearance.

2.2 The e-CNY's two-tier operating system

The e-CNY adopts a "two-tier" operating system. The PBC supplies e-CNY to the authorised operators, which provide exchange and circulation services to the public. The authorised operators collect the personal information necessary for the services and operations. The personal information generated by the wallet is collected and stored by the authorised operators. The PBC only processes inter-institutional transaction information and does not hold personal information. ID anonymisation technology is used between e-CNY wallets and the personal information exchanged between all wallets is anonymous to counterparties and other commercial institutions. For legitimate transactions, none of the above entities can obtain complete transaction and consumption behavior information to protect consumers' privacy. Under normal conditions, no other party has the right to obtain the transaction information.

Only when suspicious transactions arise can the authorised operators apply to obtain relevant data for further analysis to ensure the fulfillment of their legal obligations, such as with respect to AML/CFT. In addition, when relevant authorities obtain consumers' personal information with legal warrants, they will strictly confine the

scope of knowledge obtained and its use to the authorisation of laws and regulations. Moreover, they will take security protection measures.

The PBC strictly abides by the "Network Security Law", the "Personal Information Protection Law" and other laws and regulations. It ensures the security of personal information through advanced technical means and strict management mechanisms. The PBC adopts industry-leading technology, such as access control security and multi-factor authentication to protect data security and prevent data from unauthorised access, public disclosure, use, modification, damage or loss. The PBC has set up a "firewall" internally and strictly implements information security and privacy protection through institutional arrangements such as specially-assigned responsible persons for maintenance, business isolation, hierarchical authorisation, post checks and balances and internal audit. Information relating to the e-CNY will be sealed and stored and all customer information will be de-identified. Without legal authorisation, neither the PBC's internal personnel nor any external business unit or individual may inquire or use it at will. Unauthorised inquiry or use of personal information will be investigated according to law and those responsible would be held accountable.

Therefore, both the authorised operators and the PBC will establish personal information protection systems and internal control management mechanisms in strict accordance with the requirements of laws and regulations. They will protect customer information and ensure the security of personal information.

2.3 The e-CNY's wallet matrix design

Traditional payment instruments, via mobile or bank cards, are connected to the bank account system. Since opening a bank account requires real-name verification, these instruments cannot meet the public's demand for anonymous payments. The loose coupling between the e-CNY wallet and the bank account reduces the dependence on financial intermediaries in the transaction process and allows for anonymity for small-value payments. The e-CNY forms a wallet matrix through the design of different dimensions such as KYC-level classification, soft wallet and hard wallet, parent wallet and sub-wallet, and follows the principle of "anonymity for small amounts, traceability for large amounts in accordance with the law". Moreover, it enables online and offline applications in all use cases. Thus, the e-CNY is able to meet users' differentiated needs.

The e-CNY wallets are divided into different levels according to the KYC level. Different types of wallets are given different single transaction, single-day transaction and balance limits according to the strength of KYC. The e-CNY allows for the opening of anonymous wallets. Level-four wallets only require a phone number to be opened. According to the "Network Security Law", the "Personal Information Protection Law" and other relevant laws and regulations, telecom operators shall not arbitrarily disclose the identity information behind the mobile phone numbers to third

parties including the PBC. The level-four wallets are anonymous and are designed for small-value transactions. According to the statistics in the *The Payment System Report* (Q2 2021)released by the PBC, the average bank card payment was CNY 603 (USD 89.33), while the level-four wallet single transaction limit is CNY 2,000 (USD 296.29). This should be sufficient to meet the anonymous transaction needs of the public. The first-, second- and third-level e-CNY wallets are real-name wallets and the single transaction limit increases with the KYC level. Still, compared with the nine elements of information needed to open a bank account, the e-CNY's system collects less customer information than the traditional payment models.

The e-CNY wallets are divided into soft wallets and hard wallets according to the carrier. Under the wallet matrix, the level-four soft wallets and the hard wallets to which they belong are anonymous wallets, which can meet the needs of the public for online and offline small-value anonymous transactions. In addition, the quasi-account model hard wallet is not associated with the user's identity when issued, giving full play to the role of hard wallets in the field of small-amount anonymous payments. During the Winter Olympics in Beijing, e-CNY hard wallets were launched under a quasi-account model to provide services for foreigners who came to China for a short period of time.

The e-CNY wallet can be divided into a parent wallet and a sub-wallet according to the ownership of the authority. Users can open a sub-wallet under the e-CNY wallet and push it to an e-commerce platform to protect personal privacy. Previously, when the public was shopping on e-commerce platforms, they needed to provide relevant user payment information during the payment process. This would lead to the e-commerce platform obtaining the shopper's personal information. The e-CNY, on the contrary, de-identifies all user information. Except for the user's mobile phone number used to associate the account of the e-commerce platform when pushing the sub-wallet, it will not provide other user information to the e-commerce platform, such as bank card number or bank card validity period, effectively protecting the public's privacy.

2.4 The e-CNY's user consent policies

Based on the design of the two-tier operating system and wallet matrix, the e-CNY only obtains the personal information directly necessary for processing the transaction. The information is collected according to the user's consent and in accordance with the principles of autonomy, transparency and minimisation.

Users have the right to revoke relevant permissions at any time and the e-CNY app will immediately stop processing activities related to personal information, fully guaranteeing users' independent management. For users who choose not to provide permissions, the e-CNY app will strictly comply.

The e-CNY app does not use a package of authorisations to obtain relevant permissions from users. Instead, it applies to the user for the relevant permissions one-by-one according to specific business and use cases and after clearly informing the user of the purpose of their use. Only after the user agrees will the corresponding permissions be obtained. By specifying the permissions required to provide services and the corresponding use cases, users can fully understand the permissions they need to authorise.

Finally, the e-CNY only obtains the necessary personal information directly related to the purpose of processing. The e-CNY app only collects and processes necessary personal information to ensure the operation of basic functions such as registration, login, password modification and recovery. When authorised operators provide e-CNY wallet services to users, they also only collect necessary identity information and transaction information so as to ensure the operation of basic functions including payments. In addition, in order to ensure the safety of users' property, the e-CNY only collects the information required for risk control in the cases of theft, malicious loss reporting and tele-fraud. In short, the protection of user privacy by the e-CNY is the most advanced among the current electronic payment instruments.

3. Legal framework for the e-CNY's "managed anonymity"

3.1. International practices of "managed anonymity"

There is no true freedom without discipline. Without the necessary regulatory safeguards or risk control measures, fully anonymous CBDCs could be used for criminal activities. Ignoring risks associated with multisector and cross-border financial services may lead to disruptions in the financial system and affect the real economy. To fulfill their duty of maintaining financial security and stability, central banks and international organisations take risk prevention as a critical factor when exploring the anonymity of CBDCs. Any design that fails to satisfy AML/CFT and Anti-Tax Evasion requirements is unacceptable.

The ability of CBDCs to ensure anonymity will be limited by the need to implement risk controls. A completely anonymous CBDC is not feasible. As Agustín Carstens (2021, p. 7-8), General Manager of the Bank for International Settlements (BIS), pointed out in his *Digital Currencies and the Future of the Monetary System*: "a purely anonymous system will not work, and the vast majority of users would accept basic information being kept with a trusted institution – be that their bank or public authorities. Some form of identification is crucial for the safety of the payment system, preventing fraud, and supporting Anti-Money Laundering/Combating the Financing of Terrorism." This suggests that a balance needs to be struck between convenience and traceability.

Similarly, the BIS – together with seven central banks including the European Central Bank and the Board of Governors of the Federal Reserve System – jointly released the report *Central Bank Digital Currencies: Foundational Principles and Core Features*. They also rejected the possibility of fully anonymous CBDCs. The report points out that "full anonymity is not plausible. While anti-money laundering and combating the financing of terrorism (AML/CFT) requirements are not a core central bank objective and will not be the primary motivation to issue a CBDC, central banks are expected to design CBDCs that conform to these requirements (along with any other regulatory expectations or disclosure laws)." (Bank of Canada et al., 2020, p. 6).

In addition, the European Central Bank's report *Exploring the Anonymity of Central Bank Digital Currencies* delved into the balance between privacy protection and risk prevention (2019, p. 1), stating that "digitalisation of the economy represents a major challenge for the payments ecosystem, requiring that a balance be struck between allowing a certain degree of privacy in electronic payments and ensuring compliance with regulations aimed at tackling money laundering and the financing of terrorism (AML/CFT regulations)." The concept of a CBDC achieving a balance by managed anonymity was first proposed in the article *Some thoughts on CBDC operations in China* (Fan, 2018).

Central banks around the world have never considered that a CBDC would provide complete anonymity. The international consensus is for managed anonymity, so as to meet AML/CFT regulatory requirements.

3.2. Observing AML/CFT rules

A CBDC's ability to provide for anonymity cannot violate regulatory requirements such as AML/CFT and anti-tax evasion. In its *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins* (2020, p. 27), the Financial Action Task Force (FATF) clearly stated that "Once a CBDC is established, financial institutions, designated non-financial businesses and professions and VASPs [virtual asset providers] that deal in the CBDC will have the same AML/CFT obligations as they do with fiat currencies or cash. A customer transacting using a CBDC will have the same customer due diligence obligations as if it was an electronic transaction using fiat currency."

In this report, the FATF also mentioned that "The FATF will also continue to liaise with the private sector to monitor the sector's implementation of the new requirements, particularly the "travel rule" which enables the transfer of important identifying information between VASPs." (2020, p. 21). In order to ensure that relevant information is transmitted between different institutions and can fulfill the corresponding AML, the CBDC should also comply with the relevant requirements, such as the travel rule.

Although the BIS recognises the role of CBDCs as a substitute for cash, it also clearly requires compliance with the AML/CFT rules. Its *Central Bank Digital Currencies* report (BIS, 2018, p. 1) states " Although a general purpose CBDC might be an alternative to cash in some situations, a central bank introducing such a CBDC would have to ensure the fulfilment of anti-money laundering and counter terrorism financing (AML/CFT) requirements, as well as satisfy the public policy requirements of other supervisory and tax regimes." The Bank of England shared the same view in its report *Central Bank Digital Currency Opportunities, Challenges and Design* (2020, p. 22).

It is worth noting that since CBDCs are digitised, requiring the same level of anonymity as physical bank notes entails great risks. In its *Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins* (2020, p. 26), the FATF noted that "CBDCs could present greater ML/TF risks than cash. CBDCs could be made available to be used by the general public in retail payments or as accounts and, in theory, allow for anonymous peer-to-peer transactions. In this scenario, the CBDC would be acting as an instrument with the liquidity and anonymity of cash, but without the limitations on portability that come with physical cash. […] As they would be backed by the central bank of a jurisdiction, they potentially could be widely accepted and widely used. This combination of anonymity, portability and mass-adoption would be highly attractive to criminals and terrorists for ML/TF purposes."

As one of the focuses of international competition in the digital economy era, a CBDC will be scrutinised for its compliance with AML/CFT regulations. If the e-CNY only emphasises anonymity and relaxes requirements in CDD, it will not meet the requirements of the FATF and other international organisations. Indeed, it may be exploited and used by criminals, becoming a tool for money laundering, drug trafficking and terrorist activities.

3.3. Guarding against the risk of tele-fraud

In recent years, criminal use of the internet and telecommunications has intensified. The data from Liewang[2] shows that there are currently more than 1 million criminals engaged in tele-fraud activities nationwide, causing direct economic losses of more than CNY 100 billion (USD 14.82 billion) each year. There has been an endless stream of online gambling cases. In 2019, the public security agencies detected more than 7,200 criminal cases of online gambling. They seized and froze more than CNY 18 billion (USD 2.67 billion) of gambling-related funds. Most of the funds involved were transferred through falsely opened bank and payment accounts.

[2] https://110.360.cn/, an online platform operated by a public-private partnership between Beijing Municipal Public Security Bureau & Qihoo 360 Technology Co. Ltd.

In the traditional bank account system, KYC is required for users to open Types I, II, and III bank accounts. On the basis of the level of risk, the banks perform CDD checks and ongoing monitoring. However, even if strict CDD and continuous monitoring and cross-checking measures are taken, it is still unavoidable that criminals will use bank accounts to conduct online gambling, tele-fraud and other criminal acts.

First of all, the cost of illegal transactions using physical cash is very high. Large cash transactions require transportation, inventory, delivery and other logistics. At the same time, there are risks involved with inventory errors, damage, loss and counterfeit. As the physical cash transaction amount increases, its cost grows exponentially. For digital transactions, the cost is basically the same regardless of the amount. The inconvenience of carrying physical cash represents a friction for money laundering and terrorist financing. Therefore, the tolerance for the anonymity of cash is relatively high. The CBDC is more portable. If it were to provide the same anonymity as cash, it would greatly facilitate illegal transactions such as money laundering. Therefore, CBDCs should not have the same level of anonymity as physical cash.

Second, payment service providers have developed rapidly and online payments have become quite popular. Criminals have taken advantage of some PSPs' inadequate CDD. This has resulted in online payment accounts used for money laundering. Criminals are always on the lookout for weak links and loopholes, and criminal activities continue to flow to areas poorly covered by regulation. If the CBDC's anonymity is excessive, it will provide fertile grounds for criminals. A large number of illegal transactions will flow into the CBDC from electronic payments, making it a tool for tele-fraud and online gambling.

Therefore, the regulations for physical cash are not fully applicable to the e-CNY. The e-CNY's AML system should determine the regulatory measures to be taken according to the nature and follow the principle of "substance over form". In this way, it can assist the law enforcement agencies in recovering losses, protecting the public's property and maintaining financial stability.

3.4. Accountability and the principle of "substance over form"

AML/CFT considerations are at the core of the e-CNY design, and the PBC has established a management and supervision mechanism with a clear division of labour and responsibilities for the e-CNY to achieve closed-loop management of "pre-assessment, in-process monitoring, and ex-post supervision".

The e-CNY's business plan needs to undergo an independent assessment of AML/CFT functions to ensure compliance with international standards such as those set by the FATF, as well as the requirements of domestic laws and regulations. It also needs to formulate mitigating measures for the potential risks assessed.

Designated commercial banks serve as authorised operators of the e-CNY and provide e-CNY services directly to customers. They are the entities responsible for fulfilling the core AML/CFT obligations, including CDD, record-keeping and reporting large or suspicious transactions. According to the relevant FATF principles and Chinese domestic AML requirements, authorised operators and other commercial institutions may sign agreements and designate third parties to perform CDD checks on their behalf, but the ultimate responsibility should remain with the authorised operators. Specifically, suspicious transactions should be reported regardless of the amount of funds or asset value involved. In order to prevent criminals from opening anonymous wallets in bulk, structuring, or conducting small-value, high-frequency transfers using the e-CNY, authorised operators and other commercial institutions are required to monitor and report suspicious transactions even in the absence of real-name verification.

Currently, the e-CNY mainly serves domestic retail payment demands. Cross-border CBDC transactions are relatively complicated and can raise a number of legal challenges involving AML/CFT and KYC. In depth discussions regarding these issues are taking place internationally, and the PBC has actively participated in and contributed to related studies and working group discussions.

4. A way forward

4.1. Strengthen legislation and improve top-level system design

In order to ensure effective implementation of the e-CNY's managed anonymity, four corresponding arrangements need to be made in the top-level system design.

The first is to establish an information isolation mechanism. The independence of the authorised operators to carry out e-CNY operations should be clarified. The use of e-CNY customer information should be regulated by establishing a customer information isolation and protection mechanism. The authorised operators need to establish and improve their internal control systems and monitoring mechanism for customer information protection. Only when illegal and criminal transactions, such as money laundering, terrorist financing and tax evasion may be involved, can they apply for relevant customer information for risk analysis and monitoring, in order to fulfill AML/CFT obligations. Other participants, such as other commercial banks, PSPs, etc., have no right to obtain e-CNY customer transaction information. This ensures that customer information is used to a minimum.

Second is to clarify the legal conditions for digital wallet inquiry, freezing and withholding. Legally, only authorised authorities can inquire, freeze and withhold the user's e-CNY wallet.

Third is to establish an administrative punishment mechanism. Regulatory authorities may, according to their mandate, take punitive measures against authorised operators that handle e-CNY customer information illegally.

Fourth is to improve the e-CNY's laws and regulations with regard to AML/CFT. AML/CFT regulations, based on the relevant FATF principles, the characteristics of the e-CNY, should be released in a timely manner.

4.2. Improve risk control with new technology

Emerging technologies have revitalised the application of innovation to traditional financial risk management. In order to strengthen the risk monitoring of the e-CNY, especially in the areas of AML/CFT, it is necessary to leverage new technology to improve risk monitoring and prevention.

Risk management of e-CNY will motivate the application of regulatory technology. It will actively use big data, artificial intelligence, cloud computing and other technologies to enrich financial supervision and improve the ability to identify, prevent and resolve cross-industry and cross-market financial risks. The e-CNY's risk management and control will make full use of innovative technologies, in areas such as CDD, suspicious transaction monitoring and regulatory reporting, so as to improve risk prevention.

5. Conclusion

To sum up, as the digital fiat currency issued by the PBC, the e-CNY needs to do a good job of risk prevention on the basis of protecting privacy, so as to prevent it from becoming a tool used by criminals. The e-CNY provides the same portable, convenient features as electronic payment instruments, but also features a managed anonymous design that electronic payment instruments do not have. By mitigating the risk of criminals using e-CNY to conduct illicit transactions and maintaining financial security, it can achieve a balance between protecting personal privacy and combating crime, in line with the consensus of central banks and international organisations. The public can still obtain the complete anonymity provided by physical currency, which will not be affected by the issuance of e-CNY. At the same time, management does not mean control and domination. It is intended to prevent and control risks and fight crime, which are in line with the objective needs of safeguarding public interests and financial security. The e-CNY's managed anonymity will play a positive role in providing the public with better and more secure payment services.

References

Bank for International Settlements (2018). *Central bank digital currencies.* https://www.bis.org/cpmi/publ/d174.pdf Date of download: 2 Feb 2022

Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, and Bank for International Settlements (2020). *Central bank digital currencies: foundational principles and core features.* https://www.bis.org/publ/othp33.pdf Date of download:2 Feb 2022

Bank of England (2020). *Central bank digital currency: Opportunities, challenges and design*. https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593 Date of download: 2 Feb 2022

Carstens, A. (2021). *Digital currencies and the future of the monetary system*. [Speech transcript]. Bank for International Settlements. https://www.bis.org/speeches/sp210127.pdf Date of download: 2 Feb, 2022

European Central Bank (2019). *Exploring anonymity in central bank digital currencies*. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf Date of download: 2 Feb 2022

Fan, Y. (2018). Some thoughts on CBDC operations in China. *China Business News*, A05. https://www.centralbanking.com/fintech/cbdc/7511376/some-thoughts-on-cbdc-operations-in-china#:~:text=%20Some%20thoughts%20on%20CBDC%20operations%20in%20China,a%20surrogate%20mainly%20for%20M0%2C%20rather...%20More%20 Date of download: Feb 2 2022

Financial Action Task Force (2020). *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins.* https://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html Date of download: Feb 2 2022.

Standing Committee of the National People's Congress (2016). *Network Security Law of the People's Republic of China.* http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm Date of download: 2 Aug 2022

Standing Committee of the National People's Congress (2021). *Personal Information Protection Law of the People's Republic of China*. http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml Date of download: 30 July 2022

The People's Bank of China (2021). *The Payment System Report (Q2 2021)*. http://www.pbc.gov.cn/en/3688241/3688663/3688681/4263291/4337070/2021090917005234300.pdf Date of download: 21 Dec 2021