E-CNY: Balancing Privacy and Security[1]

MU Changchun

CF40 Member;

Director, Digital Currency Research Institute, People's Bank of China

Abstract: *The e-CNY is characterized by controllable anonymity which, while manifesting its nature as an M0 and meeting demand for anonymous transaction and privacy protection, can help address money laundering, terrorist financing, tax evasion and other irregularities and protect financial stability. Going forward, China needs further efforts at two fronts to improve its digital legal tender: enhance lawmaking and improve the top-level design; and reinforce technology application while stepping up risk control.*

The e-CNY is issued by the People's Bank of China (PBC) and co-operated by designated institutions. It can be account-based, quasi account-based, or value-based. With an underlying broad account system, it supports bank account loose coupling and is convertible to physical Renminbi at 1:1. Also a measure of value like the material currency, it is part of the Renminbi legal tender system.

The e-CNY supports controllable anonymity. This important feature of the electronic currency manifests its nature as an M0 and helps meet reasonable public demand for anonymous transaction and privacy protection. At the same time, it can help prevent money laundering, terrorist financing, tax evasion and other irregularities and crimes while protecting financial stability.

[1] *This article was published on Modern Bankers, Vol. 9, 2022. It is translated by CF40 and has not been subject to the review of the author. The views expressed herewith are the author's own and do not represent those of CF40 or any other organizations.*

I. AS AN M0, THE E-CNY IS SUPPOSED TO MEET INDIVIDUAL DEMAND FOR PAYMENT ANONYMITY

First, the e-CNY is designed with privacy protection in mind.

Consumers in the big data era are attaching greater importance to privacy protection. Electronic payment represented by mobile payment provides greater convenience than traditional cash payment, but it has yet to fully take the place of cash for one important reason—cash is anonymous and by nature protects consumer privacy.

The e-CNY is poised as money in circulation, or M0. A retail central bank digital currency (CBDC), it is introduced against a rapidly modernizing payment system and the e-payment boom—especially mobile payment boom—in China to meet the increasing demand for more diversified means of payment.

Thus, the e-CNY should be designed with the anonymity of individual transactions in mind to protect consumer privacy: 1) it should cater to the demand for small daily payments while ensuring the confidentiality of such transactions; 2) it should protect consumer information from a clearly-defined list of subjects during e-CNY transactions including merchants and other unauthorized third parties; 3) it should promote proper use of personal information, and protect basic consumer information collected by operators and behavioral data generated during transaction and consumption from leakage.

In the future digital retail payment system, the e-CNY and the money in the e-accounts of designated operators can both serve as a cash-type means of payment. At the same time, physical yuan will still boast advantages that make it irreplaceable by any other payment tools. **The e-CNY and the physical yuan will run parallel over the long run.** As long as the demand for physical money persists, the PBC will never stop providing physical yuan or phase it out compulsorily.

Second, the two-tier operational system of the e-CNY can effectively prevent unauthorized access to personal information.

The e-CNY adopts a two-tier operation system where the PBC provides the digital currency to designated operators who then put it into circulation. Operators collect information necessary to their functioning, including personal information generated during the provision of e-wallet services. The PBC only handles cross-institutional transaction information transferred to it via interconnected platforms to perform its due roles in such transactions and for account reconciliation purposes.

Meanwhile, **all e-CNY wallets and related personal data are anonymized to transaction counterparties and other involving commercial institutions,** which have no access to any full information on consumers' daily transaction or spending to protect privacy. With normal transactions, no organization or individual shall be authorized with access to any related information. Only when certain legal conditions are met such as when susceptible transactions have taken place can competent authorities request operators to provide such information within legally allowed scope with security precautions in place.

The PBC acts in strict accordance with laws and regulations including the *Cybersecurity Law* and the *Personal Information Protection Law of the People's Republic of China*, and adopts advanced technologies and stringent management mechanisms to protect personal information:

On technology, it implements access control, multiple identity authentication and other advanced technologies to protect data security and prevent unauthorized access to or disclosure, use, tampering, damage and loss of personal information.

On management, it sets up an internal firewall, and puts in place a set of systems including special staffing, business isolation, hierarchical authorization, check and balance and internal auditing to protect information security and privacy. All e-CNY-related information will be encrypted and kept safely, and all customer data will be de-identified. No organization or individual, internal or external, shall have unauthorized access to these data, and any violator shall be held accountable.

It’s obvious that both operators and the PBC are acting strictly in accordance with applicable laws and regulations, with personal information protection systems, internal controls, and proper procedures for safeguarding customer information in place.

Third, the e-CNY wallet matrix is designed in the principle of “anonymity for small-amount transactions, and traceability for large-amount transactions”.

Traditional payment tools including electronic and bankcard payment are both linked to the bank account system which implements the real-name registration system, and thus cannot provide payment anonymity as required. **But the e-CNY wallet is loosely coupled with bank accounts and so less reliant on financial intermediaries, thus enabling anonymity of small-amount transactions from a technological point of view.**

Under the above-said principle, the e-CNY wallet features a multi-dimensional matrix where wallets are divided into different levels, soft and hard wallets, and main wallets and sub-wallets that enable omni-scenario application both online and offline, addressing the diversified demand of different users at various levels and in various forms.

First, the e-CNY wallets are divided into different levels based on the level of identity recognition, all with different single transaction, daily transaction and balance limits. Level-4 wallets can be activated just with a phone number. According to the *Cybersecurity Law* and the *Personal Information Protection Law of the People's Republic of China*, operators are not allowed to disclose the information of the phone number owner to any third party including the PBC, and so these wallets are as a matter of fact anonymous. Level-4 wallets are used for small-amount cash spending scenarios. The PBC disclosed in its report on the operation of the e-CNY payment system in Q2, 2021 that in non-cash payment scenarios, consumers spent an average of 603 yuan per bank card transaction. With every transaction capped at 2000 yuan, level-4 wallets can undoubtedly meet people’s demand for anonymous payment on a daily basis. The other three levels of the wallets are real-name based, and the

upper limit for single payments goes up as the level of identification increases. This could meet public demand for large-amount payment while providing traceability to prevent risks. Compared with electronic account opening, the e-CNY system collects less information from users.

Second, e-CNY wallets include soft wallets and hard wallets. The four types of soft wallets and the hard wallets to which they belong are all anonymous in order to meet public demand for anonymous transactions online and offline in small amounts. In addition, hard wallets adopt a quasi-account system and require no user identity, and so play a positive role in promoting anonymity with small-amount payment. During Beijing Winter Olympics, the hard wallets with a quasi-account system were rolled out to provide services.

Third, e-CNY wallets include main wallets and sub-wallets. Users can activate sub-wallets under a main wallet to pay on e-commerce platforms, a means to protect privacy. Previously, when people shopped on e-commerce platforms, they were required to provide relevant user payment information during the payment process, so that e-commerce platforms were able to obtain all personal information. However, in terms of e-CNY, as all user information has been de-identified, no information will be provided to e-commerce platforms such as bank account number and validity except for the phone number used to activate the sub-wallet, thus protecting privacy.

Fourth, the e-CNY system collects necessary information only based on client preference. Based on the two-tier system and the wallet matrix, the e-CNY follows the principles of independence, transparency and minimization, and only collects necessary information that is directly relevant.

For one thing, users have the right to disable the access at any time, upon which the e-CNY application will immediately stop processing personal information to ensure user autonomy. The app also strictly implements the decision of users should they refuse to grant access to their information.

For another, the e-CNY app does not ask users to grant access to all information at once. Instead, it only requests information that is necessary and reasonable on a

case-by-case basis. It would inform users of the intended use of the information, the access to which is then granted only if the users agree. It lists all detailed information it needs to provide services and the corresponding scenarios, so that users can understand what permissions are needed from them and why.

Last, the e-CNY system only acquires and processes personal information that is necessary and directly relevant. The e-CNY app only collects information so that it can enable user registration, login, password amendment and retrieval, and other basic account functions; operators of e-CNY wallets only collect information on user identity and transaction necessary for the digital currency to serve its roles in payment and other basic services.

In addition, to protect the security of users' assets, the e-CNY system only collects information necessary for risk control to enhance risk identification and prevent theft, malicious loss report and online frauds. In a word, the e-CNY provides the strongest level of user privacy protection among all existing digital payment tools.

II. E-CNY SHOULD COMPLY WITH GLOBAL STANDARDS AND DOMESTIC LAWS AND REGULATIONS ON ANTI-MONEY LAUNDRING AND ANTI-TERRORIST FINANCING

First, anonymity based on controlled risk is the consensus of international standard-setting organizations and central banks.

"True freedom is impossible without a mind made free by discipline." If we only focus on personal privacy protection and do not control the anonymity of e-CNY, and ignore the risks brought by the convenience, scale and cross-territory of financial products and services in the digital era, e-CNY will be used for crimes with serious consequences.

To protect financial security and stability, global central banks and international organizations have all attached great importance to risk prevention while exploring the anonymity of CBDCs, and those that fail to meet anti-money laundring, anti-terrorist financing and anti-tax evasion purposes will be vetoed.

E-CNY anonymity is a limited anonymity with controlled risk, as a fully anonymous e-CNY can never work. In his speech on digital currencies and the future of the monetary system, Agustín Carstens, General Manager of the Bank for International Settlements (BIS), pointed out that "a purely anonymous system will not work". He called the idea of complete anonymity a "chimera", arguing that since "the vast majority of users would accept for basic information to be kept with a trusted institution – be that their bank or public authorities", and "enabling identification to a certain degree is critical to the security of payment systems, anti-corruption, anti-money laundering, and anti-terrorist financing", it is therefore "a must to strike a balance between convenience and traceability". (Agustín Carstens, *Digital Currencies and the Future of the Monetary System*, 2021, P7-8)

Agustín Carstens's opinion is mirrored in a report jointly compiled by the Bank of Canada, European Central Bank (ECB), Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements. According to the report titled *Central Bank Digital Currencies: Foundational Principles and Core Features*, "Some have argued that the main benefit a CBDC could bring would be some level of anonymity for electronic payments. 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, ECB, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, Bank for International Settlements Central bank, *Digital Currencies: Foundational Principles and Core Features*, 2020, P6)

The ECB said in the report *Exploring Anonymity in Central Bank Digital Currencies* that "the ongoing digitalization 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". This echoes the idea of Fan Yifei, Deputy Governor of the PBC, about controllable anonymity for

balancing purposes which he first proposed in his article *Considerations on Central Bank Digital Currencies*.

Obviously, full anonymity has never been considered by central banks as an option in the design of CBDCs. **Limited anonymity in accordance with anti-money laundering and anti-terrorist financing requirements is the international consensus instead.**

Second, e-CNY needs to meet anti-money laundering and anti-terrorist financing requirements.

The Financial Action Task Force (FATF) stated in *FAFT Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, "Once a CBDC is established, financial institutions, designated non-financial businesses and professions and VASPs 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." (FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins*, 2020, P27)

In addition, the report also mentions regulation on stablecoins, "Jurisdictions which are now undergoing the mutual evaluation and follow-up processes are already being assessed on their implementation of the revised FATF Standards on virtual assets and VASPs. 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." (FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins*, 2020, P21)

To ensure information sharing between different institutions and fulfillment of anti-money laundering obligations, CBDCs should comply with data transfer rules.

The Bank for International Settlements agrees that "a general purpose CBDC might be an alternative to cash in some situations," but it also states that "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." (Bank for International Settlements, Central *B*ank *D*igital *C*urrencies, 2018, P1)

The Bank of England holds the same views. (Bank of England, Central *B*ank *D*igital *C*urrency: *O*pportunities, *C*hallenges and *D*esign, 2020, P22)

One big concern is that CBDCs, with their digital characteristics, would be extremely risky with the same level of anonymity as physical currency. The FATF report states, "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. A point of comparison might be highly liquid bearer bonds, as these would be potentially high-value bearer instruments. 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." (FATF: *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins*, 2020, P26）

This is because it's highly costly to use cash in illegal transactions. Its transportation, check and delivery are all expensive and susceptible to miscount, damage, loss or forgery. The cost rises nonlinearly as the amount of cash involved increases. But the cost of using digital currencies remains almost the same regardless of the volume of transactions. The fact that cash is not easy to carry in large quantities has made it harder for it to be used in money laundering and terrorist financing activities, and so its anonymity is more tolerable. **But as CBDCs are much more portable, they would be easily exploited for unlawful purposes if it's as anonymous as cash.** Therefore, CBDCs should not have the same level of anonymity as cash.

Third, the e-CNY system should prevent telecommunication fraud and other risks.

Internet and telecommunication frauds and irregularities are becoming increasingly rampant in recent years. Over a million criminals are involved in online frauds today across China, causing direct economic losses of over 100 billion yuan annually. The online space is also deluged with gambling activities. In 2019 alone, Chinese law enforcement agencies cracked over 7,200 online gambling crimes that involved a total of more than 18 billion yuan. The Chinese government has taken special actions to combat telecom fraud, online gambling, and other illegal activities. Most of the money involved was transferred through false bank accounts and payment accounts.

Under the traditional bank account system, account opening requires real-name authentication; customer due diligence measures are in place throughout the business relationship, such as ranking the risks according to user or account attributes and regularly reviewing basic user information. But these procedures are still not enough to prevent illegal online gambling and telecommunication frauds based on bank accounts.

It is thus evident that criminals are always looking at the loopholes of anti-money laundering rules and systems, and various illegal and criminal acts continue to flow into areas receiving policy supports. CBDCs collect less user information than bank accounts or e-payment tools, and they are more portable than cash. If they are made highly anonymous, they will be easily used by criminals as a hotbed for illegal transactions. They will become a tool of telecommunication fraud, online gambling, money laundering, drug trafficking, or even terrorist financing, and will not meet the standards set by international organizations such as the FATF.

Therefore, the regulatory rules for cash circulation do not fully apply to e-CNY, and the anti-money laundering regulations for e-CNY should be determined by the substance of its business, to assist the authorities in recovering losses, protecting people’s property and safeguarding social stability in the event of e-CNY-related telecom fraud.

Finally, anti-money laundering, anti-terrorist financing, and anti-tax evasion responsibilities should follow the “risk-based” principle and clearly defined for different entities.

The PBC attaches great importance to the anti-money laundering system for e-CNY by establishing a management and supervision system with a clear division of roles and responsibilities, realizing closed-loop management of "pre-assessment, mid-event monitoring, and post-event supervision".

The anti-money laundering and anti-terrorist financing functions of e-CNY business solutions need to be independently assessed to ensure compliance with international standards such as those of FATF, as well as domestic laws and regulations. Appropriate risk mitigation measures should be developed for any potential risks assessed.

As the main direct provider of e-CNY services to customers, operating institutions have anti-money laundering obligations and **are required to fully perform their core** anti-money laundering and anti-terrorist financing **obligations such as conducting customer due diligence and reporting large and suspicious transactions.**

According to the FATF and China's anti-money laundering requirements, operators and other commercial institutions may entrust other institutions to carry out due diligence on their customers by signing agreements with them. However, the ultimate sharing of responsibility for customer due diligence needs further theoretical studies. Suspicious transactions need to be monitored and identified regardless of the amount of funds or value of assets involved. To prevent criminals from evading regulation by opening anonymous accounts in bulk, splitting transactions, and making small, high-frequency transfers in and out, operators and other commercial institutions need to monitor small anonymous transactions in e-CNY and report suspicious transactions.

Currently, some CBDCs, including the e-CNY, are designed and used primarily to meet domestic retail payment needs. The cross-border and international use is more

complex and involves legal issues such as anti-money laundering and customer due diligence, which are being explored in depth internationally, and PBC is also involved in the related studies.

III. THE NEXT STEP FOR E-CNY

First, we should strengthen legislation and improve the top-level design. To put in place the requirement of "controllable anonymity" for e-CNY, we should make four institutional arrangements:

1. Establish an information isolation mechanism. The independence of operating institutions to carry out e-CNY business should be clarified and the use of e-CNY customer information should be regulated by establishing an e-CNY customer information isolation mechanism and usage restrictions. E-CNY operators need to set up a sound internal control system and a monitoring mechanism for customer information protection, so that they can only gain access to information solely for risk analysis and monitoring purposes when illegal transactions such as money laundering, terrorist financing and tax evasion may be involved, in order to fulfill anti-money laundering, anti-terrorist financing and anti-tax evasion obligations and ensure that customer information is used within a minimal scope.

2. Clearly define the legal conditions for e-CNY wallets to be inquired, frozen or deducted. Such moves can only be allowed at the request of competent authorities with proper legal authorization for statutory causes, otherwise operators have the right to decline.

3. **Set up a punishment mechanism.** Regulatory authorities could enforce penalties on operators who illegally handle information of e-CNY users and strengthen supervision according to their own duties.

4. **Improve laws and regulations on anti-money laundering and anti-terrorist financing with the e-CNY.** Based on FATF principles and the features of e-CNY, we should study and introduce regulations to address money laundering and terrorist financing via e-CNY in due course.

Second, we should enhance technological application in risk prevention and control.

The application of emerging technologies has provided new ways for financial risk management, and it has become a trend to improve risk management capacity through technological measures. In order to strengthen risk monitoring and control of e-CNY, especially in terms of anti-money laundering and anti-terrorist financing, more technologies need to be employed.

E-CNY regulation will step up the application of regulatory technologies such as big data, artificial intelligence, and cloud computing to enrich the means of financial regulation and enhance the ability to identify, prevent and resolve cross-sector and cross-market financial risks. These technologies will also be widely applied in key links such as customer due diligence, monitoring of suspicious and abnormal transactions, and regulatory reporting to enhance risk prevention and disposal related to the use of e-CNY.

IV. CONCLUSION

To sum up, as a legal tender issued by the PBC, e-CNY will fully respect user privacy, protect personal information, and prevent risks associated with the illegal use of customer information. Like other digital payment instruments, e-CNY provides features such as convenience and instant settlement. On top of that, it also offers a unique design—controllable anonymity—that other digital payment instruments do not have. On the one hand, controllable anonymity can meet the public demand for personal information protection; on the other hand, it can help prevent and reduce the risk of e-CNY being used for illegal and criminal activities, maintain financial security, and strike a balance between protecting personal privacy and combating crime, which is in line with the consensus of central banks and international organizations.

It should be noted that **on the premise that physical currency is still issued, the public will not lose access to physical cash with full anonymity due to the**

issuance of e-CNY. Meanwhile, controllability does not mean control and domination. Rather, it is meant to prevent and control risks and combat crimes, which is necessary for safeguarding public interests and financial security. In short, **the controllable anonymity arrangement of e-CNY will play a positive role in offering a better user experience and safer payment services.**