Challenges and Approaches to Anti-Money Laundering Assessment of Digital Renminbi from the Perspectives of Controlled Anonymity and Cross-Border Payments

Jialu Li *

School of Foreign Languages, Harbin University of Science and Technology, Harbin, 026000, China

* Corresponding Author Email: kzhsvkenwf@outlook.com

Abstract. The centralized digital currency that belongs to the People's Republic of China, which people call e-CNY, in its own nature brings up complicated thinking points for the obeying of laws that have the goal of stopping the unlawful moving of money. The present study inspects two main aspects: firstly, its structure of supervised transaction secrecy, and secondly, the influences of its application in international payments. When carry out the evaluation of whether the platform follows AML protocols, people must handle the two-side character of its designed privacy, which requires traceability for official organs while allowing users to keep pseudonym names, therefore it creates a new environment for regulation supervision that is different from traditional cash or completely anonymous digital property. At the same time, the function of cross-border payments brings extra levels of jurisdictional and monitoring complication, because transactions can go around current financial tracking systems, hence requiring the building of new international cooperation mechanisms and interoperable supervision technology. Therefore, hence a comprehensive strategy must be formulated, which integrates adaptive regulative technology, amended legal definitions for digital sovereign currency, and proactive participation in making global standards for the management of this kind of financial instruments.

Keywords: Digital yuan, anti-money laundering, customer due diligence, controlled anonymity, cross-border payments.

1. Introduction

As a sovereign digital currency that is positioned, China's e-CNY constitutes a strategic pillar of national financial infrastructure, and thus it acts as a useful mechanism for expanding the international application scope of its currency. Till the second half of 2022, the trading amount had gone beyond 360 million cases in over twenty test zones, with which were held experiment projects for cross-border payments concerning a number of cooperating countries. The innate construction of this digital money, which combines adjusted privacy protection measures with instant final settlement, reaches two goals: it allows individual privacy secrecy while allowing required supervision, at the same time it simplifies cross-border capital transfers and reduces connected costs. Notwithstanding, these exact attributes bring about notable compliance complications for current anti-money laundering (AML) protocols, which in the past are founded on confirmed identity accounts and monitoring of large physical cash movements. Already built supervisory models rely greatly on banking go-betweens and strict account recognition, therefore making them not suitable for new working parts such as peer-to-peer transfers and long-distance digital trades that go around traditional financial passages. The recorded events, which include the earliest legal accusations for illegal money circulation in provinces such as Henan and Zhejiang, show clear weak points. Malicious people have utilized wallets with few verification steps, the functions of them have no lasting network connection, and their separation from traditional bank accounts hence lets them get around organization monitoring systems. This kind of evasion makes core AML procedures become more complex, which includes confirming the identities of participants, verifying the legitimacy of financial activities, and guaranteeing the smooth carrying out of collaboration between different agencies. For example, certain wallet levels allow starting work only by a phone number, with no dependable personal identity proof. Adding to these

problems, the different international norms for user confirmation in cross-border transactions, together with the unclearness given by foreign-held accounts about beneficial ownership, create a situation that digital instrument holders stay hidden even though wallet tracing can be done. At the same time, the global supervision organizations, which contain the Financial Action Task Force (FATF), the International Monetary Fund (IMF), and the Bank for International Settlements (BIS), are strengthening their close inspection on central bank digital currencies (CBDCs), they have already issued special management guiding opinions that put transnational data exchange, interoperable identity frameworks, and adaptive oversight that matches risk level at the first place. According to these many-sided difficulties, this current analysis has the goal to describe the three-part compliance difficult problem that the e-CNY faces. This text puts forward a practical tactic that promotes current laws, strengthens technology monitoring abilities, improves management cooperation, and enhances international cooperation relationships; therefore, it does not seek a completely brand-new supervision framework. This kind of integrated path is designed to push forward a systematic, technology-supported, consistent carrying out of client checking responsibilities on the entire digital yuan network, hence finally giving a conceptual foundation for its legal development and wider global acceptance.

2. Challenges in Anti-Money Laundering Compliance for Digital Yuan

Although Digital Yuan brings an era of state-combined currency, the work that makes its mechanisms match already existing anti-money laundering rules gives the regulatory frameworks a multi-faced group of difficulties.

One main regulation barrier comes from the problematic verification of which people are actually utilizing the finance services. Multitudinous digital currency wallets, which only undergo the most meagre identity verification procedures, prevent traditional banks and payment processing institutions from carrying out standard background examinations of their users. This loophole is utilized by professional services which are constructed to conceal the origins and endpoints of funds. The being there of technical resolving methods, including personal blockchains and individual-centered digital identity systems which allow persons to hold control over their own certificates, does not fix this condition, because existing laws cannot make such new things and compulsory obedience obligations match each other, thus it keeps going a split between that which can be achieved on technical side and that which is acknowledged by law. The international enforcement work is furthermore obstructed by non-uniform national regulations concerning identity verification and personal data protection, which lets criminal persons hide themselves through overseas company frameworks or accounts that cannot be traced, hence this leads to the actual dilemma that data can be obtained in one jurisdiction but cannot be used legally in another jurisdiction. This difficulty is further increased by the basic structure of crypto-currencies, which has no central organization that can be compared with traditional finance to take and unify the duty for stopping illegal money activities, hence hence adding multiple levels of complication to government investigations.

One main difficult problem is the verification of the legitimacy of transaction behaviors. The immediate clearing which the Central Bank Digital Currency has inside itself allows assets that got obtained illegally to be quickly sent and broken apart through many layers [1]. A time interval in reporting, which is a feature of offline payment ways, provides a weak point where the real track of money can be hidden through broken transfers between wallets and countries. At the same time, the digital environment of cross-border business harms the traditional dependence on paper trade inspections, therefore making the lasting duty of checking opposite parties frequently not able to work effectively for finding false business reasons. Although the bottom distributed account book technology can guarantee a forever examination route, regulatory persons face mixed obstacles: on technology aspect and law aspect, in the legal and actual obtaining of this kind of information under the frameworks of data protection. Therefore, the current supervision has a division of two opposing parts [2]. Although the monetary organ can carry out macroeconomic surveillance through analysis

infrastructure, the fine-grained detection mainly relies on warning messages from reporting subjects, therefore leading to intelligence which is both late and incomplete [3].

The appearance of a central bank digital currency brings deep difficulties to legal systems and cross-area supervision coordination, a difficult problem most sharp inside anti-money laundering work. The problems which continue to exist can be seen in both the national and also the international scopes. In China, laws which are made for traditional bank business have a basic bad matching on the whole. They do not possess accurate guiding rules for wallet verification levels or for drawing lines allowable hidden identity in small business deals, thus making rule-making empty spaces that can be used for washing money through this new channel [4-6]. One crucial example is the laws that make currency forgery a crime, which these laws take tangible counterfeiting as their precondition. Through obvious comparison, the digital yuan is made up of coded data on a spread account book, hence illegal duplication needs advanced data processing, program duplication, or cheating address copying. These behaviorally different actions cannot be easily prosecuted through old accusation types, hence they cause large judicial uncertainty. On the global scope, the whole picture is broken into pieces by differing stances which every nation holds on the categorization of digital assets. The lack of unified global norms for the supervision of central bank digital currencies makes this disagreement even more serious [7,8]. Even already established rules such as the Financial Action Task Force's "Travel Rule" thus prove not enough to manage the detailed cross-border movements of the digital yuan, therefore damaging legal information sharing and thus blocking joint law execution. Furthermore, this currency's possibility to pass through national boundaries makes worries about capital flight become stronger, and pulls existing foreign exchange management measures apart, thus giving policy makers the difficult work of balancing transaction speed with strict supervision. In the final analysis, the solving of this many-sided deadlock requires a jointly worked strategy that combines legal changing, progressed technical means, and reinforced global collaboration.

3. Pathways for Improvement

For the difficulties that have been found before, this research puts forward four pieces of pointed changes which are fixed in the country's present law framework. These adjustments on the fundamental level are designed for facilitating the effective execution and continuous promotion of compulsory client identity verification procedures when they concern the digital currency which is issued by China's central bank.

For the purpose of solidifying the financial supervisory framework that belongs to a sovereign digital currency, the basic legal laws must need relatively big promotion. The first important thing must be done is that people amend the Anti-Money Laundering law to add clear working rules for the digital yuan. These rules would draw clear lines for expenditure upper limits and user identity verification requirements, which are divided into types based on how deep customer background checks go; One special mechanism can force stronger checks for assigned account grades when total payment amounts cross a set threshold. At the same time, the clear definition of this digital tool as legal money with complete settlement functions requires formal confirmation, which can be obtained through judicial explanation or amendments to the central bank's management statute and national currency rules, hence hence strengthening its legal position for strict supervision. Furthermore, in order to deal with enforcement work under the digitalized background, judicial precedents ought to guide the building of standards for proving guilty consciousness in money laundering crimes, together with a clear division of the compulsory compliance inspections that banking institutions must finish when they use advanced technologies. Alongside these inside-country measures, by adopting globally watched practices, a approved-channel framework for the cross-border transmission of important supervisory data ought to be established, allowing controlled information exchange which strictly maintains the protection of sensitive personal information and national data security benefits.

One more priority includes enhancing the technological and management system inside financial supervision, starting by incorporating data produced by the digital Renminbi into the existing

structures that are used to find illegal money flows. This lays the foundation for building complex analysis frameworks which are used for discovering particular abnormal modes, these include the fast building of many accounts and the often moving of small amounts of money across nation boundaries. Using the built-in verifiability and everlasting record that distributed ledger technology supplies permits the establishment of mechanisms that can link user identifying codes with encryption wallet information in a secret way, hence enabling the full rebuilding of capital flows without destroying personal privacy protection measures [2,9]. Moreover, the building of interoperable data roads which connect the central bank digital currency platform to organs which take charge of customs, tax management, and cross-border capital flows is a thing of necessity [10]. Via the utilization of self-executing contract agreements, continuous business dealings can be independently checked against formal business files, which thus greatly enhances both the time efficiency and accuracy of checking processes. Simultaneous projects should study calculation methods that keep data secrecy, allowing joint risk evaluation among many organizations without requiring the raw swapping of private information, hence breaking down information obstacles and thus getting a more complete and strict monitoring system.

The third strategy pillar includes re-making supervision systems to cultivate cooperative organization cooperation relationships. A basic step requires an explicit division of anti-money laundering responsibilities for the central currency organ, retail bank organizations, and net service suppliers inside the digital currency system, hence resulting in a combined assessment system established by common opinions. Methods of regulation must be adjusted on the basis of risk, hence transaction channels and wallet kinds which undergo different levels of identity checking therefore require different rule systems. Therefore, financial interactions which have low threat can get advantages from simplified flows that put convenience at the first place, while situations which show raised risks therefore require strict inspection steps. Special alertness must be carried out for those especially easy-to-attack regions, including laundering plans that use hand-held equipment, transnational digital asset dealing platforms, and pay activities that are completed without net connection; these make it necessary to have special following metrics and strengthened safety rules for hardware connection mouths such as automatic cash machines that are made for the digital yuan. For the systematic settlement of the problem of information fragmentation, the leading function of the central bank is of great importance when people arrange a scheme that uses distributed ledger technology to manage client identity data among those organizations that are under regulation. This system can help the safe, rule-following on privacy exchange and verification of user information, thus effectively breaking basic barriers to data flow.

One key urgent requirement for the whole world’s money system is that it needs to let regulation structures match in each area, a job that needs strong international communication to be done. Taking part in the formulation of general anti-money laundering rules for digital currencies issued by countries through platforms such as the Financial Action Task Force and the Bank for International Settlements is necessary, with related work also directed at guaranteeing that digital currency information exchanges include systems like China's digital yuan [3,8]. The cooperative modes shown by projects including Canada’s Project Jasper and Singapore’s Project Ubin, which have finished the integration of technical systems, the alignment of governance rules, and the connection of regulatory supervision, hence give a valuable blue print. This experience ought to give guidance to the making of a special coordination organ for anti-money laundering works, which will be jointly run together with main trade partners and countries that participate in the Belt and Road Initiative. The operational effect can be obtained through compiling a common storage bank of authenticated client identity examination data, establishing a rule for checking and reacting to warnings about suspicious trade activities within a two-day time period, and spreading advanced monitoring technologies, hence thus enhancing the combined influence of cross-border cooperation against financial criminal behaviors. At the same time, people must have active participation in making the international governance rules which supervise cross-border flow of digital currency. The goal of this is to build a fair global

regulation framework; this framework at the same time protects the monetary independence of sovereign nation-states.

4. Conclusion

The inside characteristics of China's central bank digital money bring big problems for the carrying out of rules that are made to stop money-related crimes, therefore making regulatory idea-building need to change greatly from existing rules. While traditional supervision depends on checked user personal identities connected to accounts, therefore the digital yuan's ability for trade actions with insufficient verification, instant clearing, and working ability without internet connection has destroyed the basic support of current watching systems. Therefore, the related organs have the problem that they cannot with reliability find out which person is carrying out a payment, confirm the lawful property of the payment event itself, and unify legal standards, above all between different law regions. This circumstance brings up spaces where electronic money holders can be identified while the people who use them stay hidden, plus there is no supervision for payment behaviors that take place outside internet. Moreover, the manifestation of this currency in the form of cryptographic data brings complications to legal classification, hence leaving behaviors such as altering its code or constructing unauthorized access passages in a vague zone that lies outside traditional financial fraud legal provisions. To solve these gaps, it is not so much a question of constructing a completely new supervision system as it is a matter of strategically updating the existing one through overall readjustment that concentrates on legal, technical, and procedure aspects. Essential for this modernization is the full embedding of customer check requirements into every phase of the currency's life cycle, moving the attention from tracking accounts to an overall model which tracks identity features, trade flows, and basic data rules. At the same time, the regulation boundary must therefore expand from a national direction to hold the international cooperation mechanisms. The future increase of digital yuan's application in cross-border trade requires that anti-money laundering systems must always keep being adjustable and accept unceasing improvement.

References

[1] Yue Ping, Yang Jingjing, et al. Risk and prevention: the construction and prospect of anti-money laundering function of digital RMB. Journal of Shanghai University of Political Science and Law, 2023, 38(4): 29-40.

[2] Liu Qianqian, Han Hongying, et al. Analysis on the application of cross-border payment of digital RMB and anti-money laundering. Northern Finance, 2024, (06): 101-104.

[3] Xing Aifen, Fu Shuju, et al. Criminal Law Challenges and Countermeasures of Digital RMB. Xuehai, 2022, (5): 120-130.

[4] Islam M. M., et al. A Low-Cost Cross-Border Payment System Based on Auditable Cryptocurrency With Consortium Blockchain: Joint Digital Currency. IEEE Transactions on Services Computing, 2023, 16(3): 1614-1628.

[5] Research on the Impact of Digital Currency on Anti-Money Laundering and Countermeasures. FE003552, 2024.

[6] Lin Muxi, Cai Lingnan, et al. Anti-money laundering mechanism and policy suggestions of digital RMB. Journal of Liaoning University (Philosophy and Social Sciences Edition), 2022, 50(6): 58-64.

[7] Zhang Kui. Thoughts on digital currency's development and risk control. Financial Economy, 2021, (1): 3-8.

[8] Sule A. K., et al. Implementing Blockchain for Secure and Efficient Cross-Border Payment Systems. International Journal of Research and Innovation in Applied Science, 2024, 9(12): 47-75.

[9] Liu J. The Roles of Technology in Anti-Money Laundering. Science Insights, 2025, 46(4): 1813-1819.

[10] AllahRakha N., et al. Privacy and Security Risks in Cross-Border Digital Payment Systems. Lex Journal of International Human Rights, 2025, 33(2): 553-584.