Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR28084

Consumer Rights Protection under the Legal System Construction of China's Digital Currency: Current Status, Challenges, and Improvement

Yanxi Xiong

Department of Economics, Xiamen University, Xiamen, China
18279685069@163.com

Abstract. This paper focuses on consumer rights protection during the promotion of China's digital currency, systematically analyzing the logic of the current legal system construction, practical difficulties, and improvement pathways in China. The research finds that in terms of legal tender status, the technical dependency leads to the risk of the legal tender commitment in offline payment scenarios being hollowed out. The controversy over property attributes causes ambiguous judicial adjudication standards, weakening the protection of users' property rights. In the operational mechanism, the dual-layer structure of "central bank - commercial banks - consumers" improves market efficiency but has given rise to systemic risks between the central and local governments, and the absence of regulations on cross-border flows. Through empirical analysis of typical cases, the paper reveals that new types of crimes have shown characteristics of technological trust abuse and the industrial operation of money laundering. Although judicial authorities have strengthened punishment through the comprehensive inference rule of subjective knowledge, there are still governance weaknesses in smart contract crimes and cross-border coordination. From a comparative law perspective, drawing on the EU' s MICA unified legislative model, the US functional regulatory matrix, and Japan's three-dimensional governance structure, the paper proposes a Chinese characteristic "technology - system - rights" coordinated solution: to formulate a special Digital Currency Consumer Rights Protection Regulation to clarify a three-tier legal framework, establish a central bank-led full-cycle regulatory closed loop, and implement mandatory source code audit disclosure and statutory standards for algorithm explainability.

Keywords: Digital Currency of China, Consumer Rights Protection, Legal Tender Status Dual-layer Operation System

1. Introduction

In the context of the global digital wave, central bank digital currencies (CBDCS) have become a significant focus of competition in the financial sector of many countries. Numerous nations, such as the United Kingdom, Singapore, and Sweden, are actively engaged in the exploration and practice of legal digital currencies, attempting to secure a place in this emerging field. However, most countries

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.BR28084

remain cautious. For example, the central bank of Denmark has explicitly stated that it will not issue a CBDC, as it believes that, given the country's specific circumstances, the costs of issuing a central bank digital currency would outweigh the benefits [1].

In contrast, China has been at the forefront of the research and promotion of central bank digital currencies. The pilot scope of the digital yuan (e -CNY) is continuously expanding, and its application scenarios are becoming increasingly diverse, demonstrating a strong "first-mover advantage."

The large-scale pilot of the digital yuan has brought many conveniences to consumers, improving payment efficiency and reducing transaction costs. However, its high-frequency transaction characteristics have also triggered a series of new consumer rights risks. On the one hand, the extremely fast transaction speed of the digital yuan means that system failures or network delays could lead to the loss or error of consumers' transaction information, thereby affecting their financial security and transaction rights. On the other hand, the anonymity of the digital yuan, to a certain extent, provides opportunities for illegal activities such as money laundering and fraud. Consumers may suffer financial losses without even realizing it. In addition, the promotion of the digital yuan also involves issues of privacy protection and data security. Consumers' personal information may be leaked or misused during transactions. The existence of these new risks poses unprecedented challenges to consumer rights protection.

The "14th Five-Year Plan for Digital Economic Development" clearly states the need to "emphasizing both security and development," ensuring the secure operation of the digital economy while promoting its development. As an important part of the digital economy, the development of the digital yuan must follow this principle. By studying consumer rights protection under the legal system of the digital yuan, we can provide theoretical support and practical guidance for its safe development. This will ensure that the digital yuan can effectively protect consumers' legitimate rights and interests during its promotion and use, thereby achieving sustainable development of the digital yuan and promoting the healthy prosperity of China's digital economy.

Moreover, current research on the digital yuan mainly focuses on the technical and macro-policy levels. In comparison, there is relatively little research on consumer rights protection under the legal system of the digital yuan. Systematic research from the multi-dimensional perspective of "technology - system - rights" is particularly lacking. This study aims to fill this gap. Through an in-depth analysis of the technical characteristics of the digital yuan, its legal system, and consumer rights, we aim to construct a comprehensive framework for consumer rights protection in the digital yuan ecosystem. This not only helps to enrich the theoretical system of digital yuan research but also provides valuable references for the formulation and improvement of relevant laws and policies. This will further optimize the legal system of the digital yuan and better protect consumers' legitimate rights and interests.

2. Manuscript an overview of China's digital currency legal system

2.1. Legal status and issuance mechanism

The legal status of the digital yuan is the core issue in the construction of its legal system. Article 19 of the draft amendment to the People's Bank of China Law explicitly grants the digital yuan the status of legal tender, establishing its legal tender attribute and stipulating that no unit or individual may refuse to accept it when the conditions for acceptance are met. This provides the fundamental legal guarantee for the legal efficacy, circulation enforcement, and public acceptance of the digital yuan. However, the implementation of the legal tender principle still faces multiple challenges [2]:

DOI: 10.54254/2753-7048/2025.BR28084

its technical dependency requires that transaction scenarios must have infrastructure such as e-wallets and network connections. Network interruptions, terminal failures, or device incompatibilities may effectively nullify the legal tender commitment. Although offline payment functions are a solution, their scope of application and rules for liability determination urgently need to be clarified by regulations. At the same time, the boundary between the legal tender requirement and the reality of coexisting diverse payment tools needs to be clarified—the tension between merchants' right to choose payment channels and the determination of "refusal to accept" (such as whether providing only a single non-digital yuan payment channel constitutes a violation) needs to be addressed, and the exchange and coordination mechanism between the digital yuan and traditional payment tools also needs to be standardized. In cross-border scenarios, the territorial limitations of legal tender sovereignty and the absence of international rules have become key obstacles, and it is urgent to build a cross-border clearing and regulatory coordination framework through bilateral or multilateral agreements.

Regarding the property attributes of the digital yuan, there is a tripartite controversy in academia: the property rights theory, the creditor's rights theory, and the data asset theory. The property rights theory argues that it meets the definition of "property" in the Property Law section of the Civil Code, with users having direct control and exclusive rights through digital wallets. The creditor's rights theory emphasizes its credit nature, arguing that holding it is essentially a creditor's claim for value redemption from the central bank. The data asset theory focuses on its encrypted data carrier characteristics, advocating for its regulation within the framework of data property rights. The theoretical divergence on property attributes has led to difficulties in judicial practice: courts, lacking unified adjudication standards, tend to avoid characterization in cases of ownership confirmation, execution objections (such as fund freezing), or data security claims, only acknowledging its economic value as legal tender. This uncertainty directly weakens the protection of users' property rights, especially in scenarios such as the division of joint property and inheritance, which may lead to conflicts in the application of law and urgently need to be clarified through legislation or judicial interpretation.

2.2. Operational mechanism and regulatory framework

The digital yuan adopts a "dual-layer operation system" led by the central bank, forming a triangular structure of "central bank - operating institutions - consumers." In this mechanism, the People's Bank of China, as the issuing body, has exclusive rights to issue the digital yuan, manage the basic system, and formulate core policies. It ensures the stability and security of the currency system through technical standards and compliance requirements. Legally authorized commercial banks and other operating institutions undertake the functions of distributing, exchanging, and providing circulation services to the public. This includes market-oriented operations such as wallet opening, payment clearing, and merchant access, forming the key link between the central bank and consumers. End consumers exercise monetary rights such as payment and storage through digital wallets, subject to identity verification and compliance requirements. This structure combines institutional advantages with market efficiency: the central bank maintains currency sovereignty and financial stability through top-level design, operating institutions accelerate scene penetration based on existing infrastructure, and consumers gain inclusive services of legal digital currency.

However, this operational mechanism has given rise to multiple regulatory dilemmas: when commercial banks expand their market share, they may transmit risks to the consumer end due to technical vulnerabilities (such as wallet security flaws), improper operations (such as non-compliant marketing), or system compatibility issues. The current regulatory rules lack detailed liability

DOI: 10.54254/2753-7048/2025.BR28084

provisions for operating institutions' technical safety standards, user data protection obligations, and service interruption responsibilities, leaving consumers facing dual risks of fund security and privacy leakage. There is tension between the central bank's supervisory power over operating institutions and the latter's independent management rights. For example, in anti-money laundering monitoring, the central bank needs to obtain transaction data in real-time, while operating institutions may restrict data sharing based on trade secrets or user agreements. When a large-scale system failure occurs, there is a lack of legal basis for distinguishing between the central bank's systemic risk management responsibilities and the operating institutions' daily maintenance responsibilities. The emergence of new application scenarios such as smart contracts and cross-border payments has exposed the inadequacy of regulatory rules' adaptability. The automatic execution of smart contracts may trigger payment behaviors that users are not fully aware of (such as conditional payment traps), and judicial jurisdiction conflicts, data localization requirements, and exchange rate risk management in cross-border flows all go beyond the regulatory scope of the current Cross-Border Payment Management Measures.

3. Current status and challenges of consumer rights protection in digital currency

Digital currency, as an emerging legal digital currency, has made certain progress in the protection of consumer rights, but it is still in the process of continuous improvement.

3.1. Account security and technical safeguards

Digital currency relies on block chain and distributed ledger technology to build a secure architecture at the base level. In theory, it has the characteristics of non-tamperable and traceable transaction data, which provides technical endorsement for the authenticity and integrity of transactions. Its security protection system adopts the mechanism of minimum privilege access control and dynamic multi-factor authentication, significantly reducing the risks of unauthorized data access, tampering, and leakage. Under the "dual-layer operation"framework, operating institutions implement full-cycle account monitoring through technologies such as biometric recognition, transaction behavior modeling, and real-time risk probes, and establish an intelligent risk control threshold system covering scenarios such as large-sum transfers, high-frequency transactions, and abnormal location logins [3]. Although this mechanism can effectively intercept overt theft behaviors, it still faces challenges from new types of attack methods: the potential threat of quantum computing to encryption algorithms, the double-spending risk in offline transaction scenarios, and the problem of asset loss caused by the physical damage of hardware wallets. It is necessary to enhance security depth through the iteration of national cryptographic algorithms and the mandatory specification of disaster backup.

3.2. Consumer data privacy protection mechanism

Digital currency achieves privacy protection through a controllable anonymity design of "front-end anonymity and back-end traceability" [4]: the information of both parties in a transaction is completely isolated from commercial institutions, and daily consumption tracks are not obtained by commercial entities. Operating institutions must follow the Personal Information Protection Law to establish a customer information firewall system, strictly limiting the scope of data collection (adhering to the principle of minimality), storage period (setting automatic destruction thresholds), and usage scenarios (limited to statutory reasons such as anti-money laundering). At the regulatory

DOI: 10.54254/2753-7048/2025.BR28084

level, a tiered authorization query mechanism is established only when a statutory suspicious transaction model (such as terrorist financing monitoring) is triggered, can authorized agencies obtain users' full-chain transaction data with a judicial warrant, and data desensitization and audit trails must be executed. The current weaknesses are: the dynamic balance between anonymity and anti-money laundering requirements has not been quantified (such as the threshold setting for large-sum anonymous transfers), the secondary leakage risk in cross-institutional data sharing, and the compliance conflict between decentralized identity (DID) technology and the current real-name regulation.

3.3. Transaction dispute resolution and compensation system

The current dispute resolution mainly relies on the internal appeal channels of operating institutions and regulations such as the Non-bank Payment Institutions Regulations. Consumers can initiate rights protection through mechanisms such as freezing disputed transactions and error reporting platforms, and operating institutions are required to complete evidence collection and verification within the statutory response time limit (it is recommended to refer to the payment institutions' requirement of an initial response within 5 working days). For fund losses caused by system vulnerabilities or maintenance negligence, the operating institutions are fully liable for compensation under the principle of presumed fault; however, for losses caused by consumers' own negligence (such as leaking dynamic verification codes, mistakenly confirming smart contract terms) or third-party crimes, there are problems of ambiguous liability determination and lack of compensation standards: the technical liability attribution of password devices being brute-force cracked, the judicial discretion scale of users' negligence in phishing scams, and the judicial jurisdiction conflict in cross-border transaction disputes. It is urgent to introduce the Digital Currency Business Error Handling Measures, clarify the rules of burden of proof reversal (operating institutions prove their own faultlessness), establish tiered compensation ratios (according to the degree of negligence), and establish a central bank-led arbitration backup mechanism.

3.4. Consumer education and risk prevention

With the continuous expansion of the pilot scope of digital currency, operating institutions and relevant departments have carried out publicity and promotion of digital currency through various channels, including online and offline publicity activities, media publicity, and community promotion, to popularize basic concepts, usage methods, and advantages of digital currency among consumers, and to improve consumers' awareness and acceptance of digital currency [5]. During the promotion process, relevant departments also focus on risk warnings to consumers, reminding them to be vigilant against digital currency scams and account theft, and guiding them to establish correct risk awareness and usage habits. However, the current consumer education content is not comprehensive and in-depth enough. The education on the complex technical principles of digital currency, potential risks, and specific measures for consumer rights protection is still relatively weak. Some consumers still have certain limitations in understanding and using digital currency. It is suggested to build a full-life-cycle education system: in the entry stage, strengthen the teaching of wallet grading security settings, in the application stage, embed risk simulation testing tools, and in the post-event stage, publicize typical dispute adjudication rules. At the same time, it is necessary to establish education effectiveness evaluation indicators (such as user security operation compliance rate) to promote the transformation of publicity from "knowledge coverage" to "capacity building".

DOI: 10.54254/2753-7048/2025.BR28084

3.5. Case analysis

The rise of digital currency in China has led to new types of crimes, shaping judicial adjudication through notable cases. In 2023, a fraud case in Shandong's Cao County saw criminals forge People's Bank of China documents, deceiving middle-aged and elderly victims into paying a 280-yuan fee to "activate" a 2.8-million-yuan digital currency credit, affecting over 10,000 victims and involving 70 million yuan. In Shanghai, a 2023 money laundering case exploited non-real-name digital wallets, with criminals withdrawing 123,000 yuan in cash via ATMs within two hours and laundering over 10 million yuan using 900+ wallets. These cases highlight technical trust abuse, where fraudsters mimic official interfaces, use urgent rhetoric to lower vigilance, and leverage instant digital currency transactions for rapid fund transfers.Money laundering has become industrialized. A Shanghai case revealed a three-tier system: upstream fraudsters funneled illicit funds into non-real-name wallets, mid-level "drivers" withdrew cash via ATMs, and downstream merchants converted funds into USDT for cross-border transfers. Anti-investigation tactics, like separating operators from phone numbers and cross-provincial operations, were used. In 2024, a Zhejiang case involved merchants laundering 500,000 yuan by disguising fraud funds as consumer transactions, exploiting loose account oversight. These cases expose the dual nature of digital currency's anonymity: it protects user privacy but enables regulatory arbitrage for illicit activities.Judicial responses have established key rules. Shanghai's Yangpu Court, referencing Supreme Court guidelines, inferred criminal intent from high-frequency wallet operations, abnormal commissions, and evasive tactics. Money laundering exceeding 100,000 yuan is deemed "serious," as seen in a Shanghai case with a 10-million-yuan flow, resulting in a 4.5-year sentence. Another case factored in untraceable upstream crimes as an aggravating circumstance. To counter risks, banks now monitor behavior, devices, and locations, freezing suspicious multi-wallet activities. Beijing prosecutors disabled ATM withdrawals for certain wallets and added facial recognition. The Supreme People's Court plans to criminalize wallet renting/lending, while Zhejiang's Shaoxing case imposed a merchant obligation to report abnormal profits. Smart contracts, like the "Yuanjiakuan" system, have protected prepayments, enabling automatic refunds for 1,300+ merchants in sectors like fitness and education since July 2024.Cross-border crimes remain challenging [6]. A Cambodian fraud group's use of anonymous wallets and virtual currencies highlights regulatory gaps. While a robust prevention framework exists, amendments to the Anti-Money Laundering Law and enhanced Interpol cooperation are needed to address smart contract fraud and cross-border fund flows.

3.6. Challenges faced

Despite progress in consumer rights protection, China's digital currency faces systemic challenges. Technically, advanced encryption and distributed ledgers are vulnerable to quantum computing, offline double-spending, and hardware damage. Hackers could steal wallet assets or alter records, while transaction traceability risks privacy leaks, exposing user identities and spending patterns. Data loss in offline payments and irreversible errors due to user mistakes further undermine security.Legally, the lack of specific legislation on digital currency's legal tender status, operator liabilities, and consumer rights creates uncertainty in dispute resolution. The fragmented regulatory framework, involving the People's Bank of China and other commissions, leads to overlapping compliance reviews and gaps in cross-border monitoring. Without multi-agency coordination, balancing innovation and risk control is challenging.Consumer trust is hindered by low awareness—only 17% of people over 60 understand wallet limit rules, and fewer than 5% recognize smart contract risks. Misconceptions about biometric data and institutional governance fuel skepticism.

DOI: 10.54254/2753-7048/2025.BR28084

Payment inertia favors third-party platforms, which dominate retail with mature systems and high penetration.

Cross-border use faces three contradictions: First, the tension between payment convenience and compliance costs. Current cross-border settlements need to coordinate domestic operating institutions, foreign correspondent banks, and multiple national clearing systems, and the complexity of the process increases the costs for merchants. Second, regulatory standard fragmentation. Major economies have conflicting requirements for digital currency account access, data localization, and anti-money laundering (AML). China's Cross-Border Payment Management Measures have not yet fully aligned with the FATF recommendations. Third, the inherent conflict of risk prevention and control targets. It is necessary to meet the transaction transparency requirements under the "travel rule" while maintaining the original intention of the controllable anonymity design [7]. There are technical bottlenecks in monitoring cross-border large-sum transactions.

The competitive market pattern increases the difficulty of promotion. The payment market shows a "duopoly + multipolar" characteristic. Third-party institutions weaken the penetration efficiency of digital currency with their scene monopoly of QR code payment (covering 98% of physical merchants) and the first-mover advantage in cross-border payment networks. In terms of cooperation mechanisms, the interest game between commercial banks and technology companies in terms of profit distribution and data ownership has delayed the construction of the ecosystem. Some financial institutions are negative towards wallet promotion due to the decline in clearing profits. Scene expansion is also restricted by the terminal coverage rate in rural areas (less than 40%) and the cost pressure of system transformation for small and medium-sized merchants, which restricts the realization of the inclusive finance goal.

These intertwined challenges—technical vulnerabilities, regulatory gaps, low consumer trust, cross-border complexities, and market barriers—undermine system credibility, market acceptance, and international expansion. A comprehensive solution requires integrated legislation, advanced regulatory technology, and global cooperation to strengthen consumer protections.

4. Pathways to improve consumer rights protection in China's digital currency: international experience from comparative law perspective

4.1. Legislative level

The European Union's Markets in Crypto-assets Regulation (MiCA) has constructed a systematic regulatory framework through a unified legislative model. It requires stablecoin issuers to maintain adequate reserves and undergo quarterly independent audits while mandating the disclosure of algorithmic risks and contingency plans. This type of (piercing-the-veil regulation) significantly enhances market transparency and consumer confidence. In contrast, in China's digital currency field, consumer rights protection regulations are currently scattered across multiple laws and regulations such as the Personal Information Protection Law and the Non-bank Payment Institutions Regulations [8].There are issues such as the legal tender effect not being legalized, unclear responsibility boundaries of operating institutions, and the lack of regulation on new risks (such as smart contract disputes), which lead to the fragmentation of consumer rights protection basis.

To bridge the institutional gap, it is urgent to formulate a special Digital Currency Consumer Rights Protection Regulation (it is suggested to set 30 core articles), focusing on clarifying a three-tier legal structure: First, to establish the legal tender status of digital currency and the legal nature of the dual-layer operation system, and to clarify the responsibility distribution between the central bank and operating institutions; second, to stipulate new rights such as consumers' fund security

DOI: 10.54254/2753-7048/2025.BR28084

guarantee right, contract clause objection right, and data portability right, and to accompany the obligations of operating institutions for system resilience testing and privacy design embedding; third, to build a dispute resolution special channel and error handling time-effect mechanism. This regulation needs to achieve two-way connection with the "Legal Digital Currency" special chapter in the Digital Economy Promotion Law (Draft) to clarify the digital currency's digital economy infrastructure attribute in the basic law, and at the same time, to detail the consumer protection operation rules in the special regulation, forming a three-dimensional protection system of "basic law positioning + special regulation implementation", and ultimately realizing the institutional transformation of consumer rights protection from fragmented relief to systematic protection.

4.2. Regulatory level

The United States has constructed a cross-departmental functional supervision matrix through the SEC, CFTC, and FinCEN, dynamically dividing jurisdiction based on the substantial risks of financial products: security tokens are subject to the SEC's information disclosure rules, derivatives belong to the CFTC's market manipulation prohibition category, and payment stablecoins are included in FinCEN's anti-money laundering framework. This regulatory model, oriented by the nature of behavior and supplemented by joint law enforcement actions (such as the 2023 "Crypto Sweep" that froze $4 billion in illegal assets), forms a powerful compliance deterrent. In contrast, in China's digital currency regulatory practice, the People's Bank of China is responsible for basic issuance management, the China Banking and Insurance Regulatory Commission focuses on the behavior supervision of financial institutions, and the State Administration for Market Regulation controls the payment compliance of merchants. The parallel operation of multiple tracks leads to the coexistence of functional overlap and vacuum - for example, the compliance review of smart contracts is suspended due to unclear subjects, and cross-border flow monitoring has collaborative blind spots due to data sharing barriers.

Therefore, it is urgent to establish a permanent regulatory coordination committee led by the central bank to reconstruct regulatory efficiency through a three-tier mechanism: First, to formulate the Digital Currency Joint Supervision Memorandum of Understanding, clarifying the responsibility boundaries of the central bank in coordinating systemically important risks, the China Banking and Insurance Regulatory Commission in auditing the compliance of operating institutions, and the State Administration for Market Regulation in investigating and dealing with merchant violations; second, to build a regulatory information sharing platform, forcing operating institutions to upload suspicious transaction chain diagrams (including cross-institutional fund flows) to achieve millisecond-level anti-money laundering risk warnings; third, to set up a joint evaluation group for innovative businesses, implementing a "joint access system in regulatory sandbox" for new forms of business such as smart contracts to avoid repeated or omitted approval access [9]. This mechanism can rely on the State Council's Financial Stability and Development Commission to achieve cross-ministerial decision-making integration, ultimately forming a full-cycle regulatory closed loop from risk monitoring to law enforcement punishment, providing collaborative institutional protection for consumer rights protection.

4.3. Platform governance

The Japanese Financial Services Agency (FSA) has constructed a systematic risk prevention and control mechanism in the field of crypto- assets through a three-dimensional governance structure of trading platform licensing access, mandatory isolation of cold wallet assets, and collaborative

DOI: 10.54254/2753-7048/2025.BR28084

supervision by the industry self-regulatory organization (JVCEA). This model, which deeply integrates technical standards (cold storage), market access (licensing management), and industry self-governance (self-regulatory codes), significantly enhances the level of consumer asset security. In contrast, in China's digital currency operation platform governance, although commercial banks and payment institutions undertake wallet service functions, there are dual shortcomings of insufficient technical transparency and lagging security defense - the lack of a key source code audit mechanism makes it difficult to find system vulnerabilities in time, the black-box characteristics of smart contract decision logic weaken consumers' right to know, and there is a lack of institutionalized vulnerability response channels.

Therefore, it is urgent to build a Chinese version of the platform governance paradigm: First, to establish a mandatory disclosure system for third-party source code audits, requiring operating institutions to regularly publish audit reports authenticated by national-level laboratories, focusing on verifying the reliability of the offline payment recovery module and the key management system; second, to implement a regulatory-driven white-hat bounty program, with the central bank setting up a special fund to reward vulnerability submissions and forcing operating institutions to fix high-risk vulnerabilities within 72 hours; finally, to introduce statutory standards for algorithmic explainability, stipulating that smart contracts must provide users with a visual path of decision logic (such as a tree diagram of the triggering conditions for fund freezing) and verify its understandability through regulatory sandbox testing. These three measures together form a chain governance closed loop of "technical transparency - security co-governance - decision knowability", ultimately strengthening consumers' trust in digital currency by reducing the uncertainty of technical black boxes.

4.4. Summary

From a comparative law perspective, enhancing consumer rights protection in China's digital currency system requires systematic integration of advanced international experience, tailored to the specific context of China's financial regulatory framework and digital currency development. The EU's Markets in Crypto-assets Regulation (MiCA) offers a unified legislative model that strengthens consumer safeguards through clear issuer disclosure obligations and stablecoin reserve requirements [10]. The US adopts a functional supervision approach, with the SEC, CFTC, and FinCEN performing distinct yet collaborative roles—a structure that could inform China's efforts to build a coordinated enforcement mechanism led by the People's Bank of China with support from the CBIRC and SAMR. Japan's Financial Services Agency provides further insights with its strict trading platform licensing, cold wallet mandates, and industry self-regulation (JVCEA), offering valuable lessons for technical governance in areas such as smart contract audits and algorithmic transparency.

Nevertheless, China faces several unique challenges in advancing digital currency consumer protection. At the legislative level, existing laws such as the People's Bank of China Law and the E-Commerce Law contain fragmented and inconsistent provisions regarding digital currency consumer rights, failing to keep pace with rapid fintech developments. Regulatory coordination between central and local authorities remains inefficient, with ambiguities in responsibility and barriers to interdepartmental collaboration impairing oversight. Technically, the "controllable anonymity" feature of digital currency introduces tensions between user privacy and transaction transparency. Additional concerns include smart contract security, system stability, and capacity to address emerging cybercrimes.

DOI: 10.54254/2753-7048/2025.BR28084

To tackle these challenges, the following pathways are proposed: First, enact specialized Digital Currency Consumer Rights Protection Regulations to systematically define the rights and obligations of all parties and establish efficient dispute resolution mechanisms. Second, optimize the regulatory structure by clarifying departmental responsibilities and enhancing coordination under the central bank's leadership, facilitating information sharing and joint enforcement. Third, strengthen technical governance through mandatory third-party security audits, algorithmic transparency standards, and improved system contingency plans. Finally, promote consumer education to raise public awareness of digital currency risks and self-protection.

From a broader perspective, the sound development of digital currency is not only vital for domestic financial stability but also essential to China's role in global digital currency competition. By constructing a consumer protection system that incorporates international best practices while aligning with national conditions, China can foster a trustworthy environment for widespread digital currency adoption and contribute its insights to global digital currency governance. As application scenarios expand and international cooperation deepens, this protective regime must continue to evolve in response to new challenges and opportunities.

5. Conclusion and outlook

As a key driver in the digital transformation of China's financial sector, the healthy development of digital currency relies on a robust consumer protection framework. Through comparative analysis of international models, this study identifies both references and unique challenges facing China, including fragmented regulations, insufficient supervisory coordination, technical risks, and cross-border usage issues. It is recommended that China enhance consumer protection through specialized legislation, coordinated oversight, technological governance, and public education to balance security and innovation.

Looking ahead, the global adoption of digital currency will present new opportunities and challenges. Expanded pilot programs and international cooperation may position it as a key tool for cross-border payments, though issues like regulatory alignment and anti-money laundering compliance remain. Technological advances will reshape security paradigms, calling for preemptive standards and regulatory sandboxes. Moreover, consumer protection should evolve from passive remediation to active prevention, leveraging smart contracts for auto-compensation and blockchain for efficient dispute resolution.

China's engagement in digital currency not only relates to national financial security but also represents a significant contribution to global digital currency governance. Moving forward, continued innovation integrating technology, regulation, and user rights will help establish an inclusive, secure, and forward-looking consumer protection model—showcasing China's approach as a reference for central bank digital currencies worldwide.

References

[1] Zhou, T. Y. (2025). Digital Currency System: System Anchoring, Gap Analysis, and Path Exploration. Hebei Enterprise, (08), 27-30. DOI: 10.19885/j.cnki.hbqy.2025.08.014.

[2] Xu, C. (2025). Personal Information Protection Dilemma and Countermeasures in Digital Currency. Northern Finance , (05), 73-81. DOI: 10.16459/j.cnki.15-1370/f.2025.05.018.

[3] Zhao, L. (2022). Legal Protection of Consumers' Personal Financial Information Rights - From the Perspective of Digital Currency. Finance Forum , 27(12), 38-47. DOI: 10.16529/j.cnki.11-4613/f.2022.12.008.

[4] Feng, S. X., & Yang, J. (2021). The Role of Digital Currency in Preventing Data Monopoly Risks of Internet Platforms. Reform , (12), 69-80.

DOI: 10.54254/2753-7048/2025.BR28084

[5] Wang, H. Y. (2025). On the Safety and Risk Prevention of Digital Currency Development. Financial Guest , (01), 54-56.
[6] Li, Y. (2024). “Yuanjiakuan” Solves Prepaid Consumption Protection Problems. China Quality March , (08), 36-38.
[7] Li, Z., & Huang, L. F. (2022). Legal Issues of Cross-border Circulation of Legal Digital Currency. Wuhan International Law Review , 6(02), 59-78. DOI: 10.13871/j.cnki.whuilr.2022.02.004.
[8] Guo, Y. (2024). Personal Information Protection in the Circulation of Digital Currency. Harbin University of Science and Technology . DOI: 10.27063/d.cnki.ghlgu.2024.001487.
[9] Zhang, L. L. (2022). Financial Risks and Prevention of Legal Digital Currency Applications - From the Perspective of Financial Consumer Rights Protection. Guangxi Social Sciences, (05), 19-24. DOI: 10.3969/j.issn.1004-6917.2022.05.003
[10] Zhang, Y. F. (2025). Consumer Rights Protection under the Legal Framework of Digital Currency. China Market Supervision Research , (05), 62-67.