Scholar Publishing Group
International Journal of Business Management and Economics and Trade
https://doi.org/10.38007/IJBMET.2025.060122
ISSN 2790-0959 Vol. 6, Issue 1:213-220

Application and Development of Blockchain Technology in Financial Infraustructure Innovation

Yuxin Liu

Corporate Treasury-Chief Investment Office, JPMorgan Chase, Newark, 19107, Delaware, USA

Keywords: Blockchain technology; Financial infrastructure; Data security; Smart contract

Abstract: With the promotion and improvement of blockchain technology, blockchain technology has gradually penetrated into various fields within financial institutions and played a significant subversive role. Because of its decentralized, tamper proof and traceable characteristics, it can bring subversive solutions to the fields of payment settlement, identity authentication, data storage and so on. The distributed accounting method improves the speed of synchronous processing of information, the smart contract realizes the automation of business process processing, and the encryption measures improve the ability of data security protection. Technical performance bottlenecks, lack of privacy protection and lack of legal norms still restrict its wide application. This paper mainly studies the specific application of blockchain technology in financial infrastructure, systematically summarizes the problems encountered, and puts forward practical and effective improvement schemes.

Introduction

Financial market infrastructure (FMIS) is the support point for the normal operation of the modern financial system, covering the payment system and settlement system. Enterprise registration and related credit management constitute the key support links of financial market infrastructure. Traditional financial market infrastructure still lags behind in achieving real-time settlement, improving information transparency and enhancing mutual trust in the market. As an emerging technology, blockchain, based on distributed structure design and cryptography technology, has brought a revolution to the financial market infrastructure. At present, there are many innovative ways to put forward a variety of implementation schemes. From the dual perspective of technological innovation and policy adaptation, this paper discusses the application prospect and sustainable development strategy of blockchain in financial market infrastructure.

1. Overview of blockchain technology theory

Blockchain is a new type of information processing technology based on distributed database. It achieves reliable transmission and automatic execution of information through hash functions, consensus protocols, smart contracts and other means. Its structure is composed of blocks connected in chronological order. Each block stores some transaction information and is connected by hash function to prevent information from being tampered with. Consensus protocols are used in blockchain networks to establish trust relationships between nodes, such as workload proof protocol (POW) and equity proof protocol (POS), which help maintain the stable operation of decentralization; Smart contract is an electronic contract with built-in logic, which defines the behavior procedure that can be automatically executed after an event, greatly simplifying the transparency and convenience of business behavior. At present, blockchain technology has developed from cryptocurrency in the initial stage to smart contracts and assets in the medium term, and then to cross industry comprehensive application in the later stage, showing the innovation potential of transforming industries such as finance, logistics and government. Blockchain technology is becoming an important force to promote the innovation of basic system and the reconstruction of trust mechanism.

2. Application of blockchain technology in financial infrastructure innovation

2.1 Application framework of distributed ledger system

The construction of decentralized data structure and node consistency protocol supported by distributed ledger technology constitutes a solid, efficient and reliable digital information storage network foundation. The general basic framework consists of a node layer, a data dissemination layer, a consensus execution layer and a smart contract layer. Each part cooperates with each other to support basic tasks such as capital registration, transaction confirmation, payment and clearing. The multi node operation mechanism can effectively resist errors and avoid the global risk caused by a single fault. The core mechanism of the ledger is that the data cannot be tampered with and the correlation between blocks. Its block generation logic can be formally expressed as:

$$C_i = H(C_{i-1} \parallel TX_i \parallel T_i) \tag{1}$$

Of which,$\mathrm{C_i}$Is the hash value of the current block,$\mathrm{C_{i-1}}$Is the hash of the previous block,$\mathrm{TX_i}$为 It is a collection of transactions in this block,$\mathrm{T_i}$Generate a timestamp for the block,H Is a hash function.This structure ensures that any transaction change will affect the integrity of hash chain, so as to improve data security and verifiability.

2.2 Operation mode of smart contract chain

Smart contracts are a key part of the blockchain system. The core of smart contracts is to automatically execute tasks or rules. In the blockchain, smart contracts are executed according to a fixed logic. If a condition is met, they are automatically executed. For example, it can be applied to online transactions, online financial product clearing, online financial asset management, online credit evaluation, etc. It realizes the program response of frequent work mainly by embedding business rules in the process of program execution. Its main stages include: trigger input, condition confirmation, logic operator, state adjustment, result publication, etc., becoming an independent, traceable and public transaction processing framework. The behavior of smart contracts can be formalized into a state machine, in which the state transition is driven by input events, which can be expressed as:

$$S_{t+1} = \delta(S_{t,}\ I_t) \tag{2}$$

Of which,$\mathrm{S_t}$Is timetContract status of,$\mathrm{I_t}$Input information for the corresponding time point，δIs a state transition function,The behavior change path of the contract under different input conditions is defined. The formula reveals the chain evolution logic of the smart contract, that is, each state change originates from the combined reaction of the previous state and the new input. Through the state driven model, the contract can realize automatic response, condition execution and irreversible recording on the chain, significantly improving transaction efficiency and process transparency. Multiple smart contracts can be called and inherited through interface functions to build a multi-layer nested and interconnected financial service contract network, providing modular and automated system support for complex businesses.

2.3 Encryption certificate storage mechanism integration scheme

By encrypting and hashing the original data and writing it into the blockchain, the encrypted depository mechanism achieves the purpose of property right confirmation, tamper proof and traceability. This technology is widely used in financial bill confirmation, contract transaction review, judicial evidence collection and other scenarios. This combination method includes four main technical processes: data generation, hash extraction summary, encrypted storage, and on chain labeling, forming a trusted data closed loop of on chain and off chain collaboration. In the process of storing certificates on the chain, the hash value and time stamp together form an irreversible proof structure, which is often in the following form:

$$H_i = Hash(\mathrm{D}_i \parallel \mathrm{T}_i \parallel H_{i-1}) \tag{3}$$

Of which,$\mathrm{D_i}$Is clauseiRaw data,$\mathrm{T_i}$Is its timestamp,$\mathrm{H_{i-1}}$Is the hash value of the previous data,$\mathrm{H_i}$Is the chained hash result of the current certificate. The formula constructs a time-dependent hash chain structure to ensure that the data can not be tampered with or forged once the right is confirmed. By combining the encryption algorithm with hash chain mechanism, the system not only realizes the protection of data confidentiality and integrity, but also forms a collaborative trust foundation in the multi-party financial ecosystem. In the future, the mechanism can also be integrated with technologies such as zero knowledge proof and multi-party secure computing to further improve the data privacy protection ability and cross platform verification efficiency.

3. Application of blockchain technology in financial infrastructure innovation

3.1 Network performance bottlenecks limit transaction efficiency

Because blockchain is widely used in the financial system, it has higher requirements for the transmission speed and response timeliness of the blockchain system. At present, the mainstream public chain and alliance chain are generally faced with performance bottlenecks, and there are problems of transaction confirmation delay and network congestion under a large number of transaction requests. Traditional blockchain systems, such as bitcoin, adopt a single chain architecture and distributed transmission, resulting in slow transaction speed of the chain, and the number of transactions that can be completed per unit time is far lower than that of traditional payment networks. With the increasing number of nodes in the chain, the calculation of information synchronization and consistency becomes complex, which greatly affects the timely confirmation of transactions. Large scale contract calls will also lead to block capacity saturation in a short time, seriously affecting the system operation efficiency. For the financial infrastructure that needs second level response and large-scale clearing processing, such performance bottlenecks become the key obstacles to the actual deployment and business carrying capacity of the blockchain system.

3.2 Technical weakness of privacy protection mechanism

In the financial transaction system, customers' personal identity information, account balance and transaction information have high confidentiality requirements for privacy and personal information disclosure. However, the blockchain system has the characteristics of public transparency, which is difficult to meet the demand of high confidentiality. Even if conventional technical means such as address anonymity and mixer are adopted, the associativity between the behavior on the chain and the real identity cannot be completely shielded. At the same time, although zero knowledge proof, multi-party secure computing and other technologies have good privacy protection effect in theory, they are faced with problems such as huge computing cost, low data throughput efficiency and high implementation difficulty in practice, which can not meet the complex situation of frequent financial rules in financial transactions. At present, the trade-off between privacy and verifiability is still an unresolved problem. In the case of cross organizational scenarios and data sharing by regulators, it is easy to lead to the risk of data abuse or disclosure, which is the most important technical bottleneck for the deployment of blockchain financial services.

3.3 Lagging legal system affects business expansion

The development speed of blockchain technology has exceeded the upgrading speed of the current law, and there is a lack of unified and clear institutional support in the actual financial application process. There is no consensus on blockchain property rights, the legal status of smart contracts, the division of node responsibilities, cross-border information processing and other aspects around the world, which has led to legal instability in cross-border trading activities. Sub jurisdictions have not yet defined the evidentiary effect of records on the chain in judicial proceedings, blocking the practical application of blockchain technology in contract certification, transaction certification and other aspects. The lack of compliance protection hinders the financial industry's caution and hesitation in using blockchain technology, which in turn hinders the allocation of innovative products and resources. The channels of communication between regulators and technology are not smooth, resulting in the structural conflict between emerging technologies and the current regulatory mode, which hinders the in-depth integration and cross domain expansion of blockchain technology and financial infrastructure.

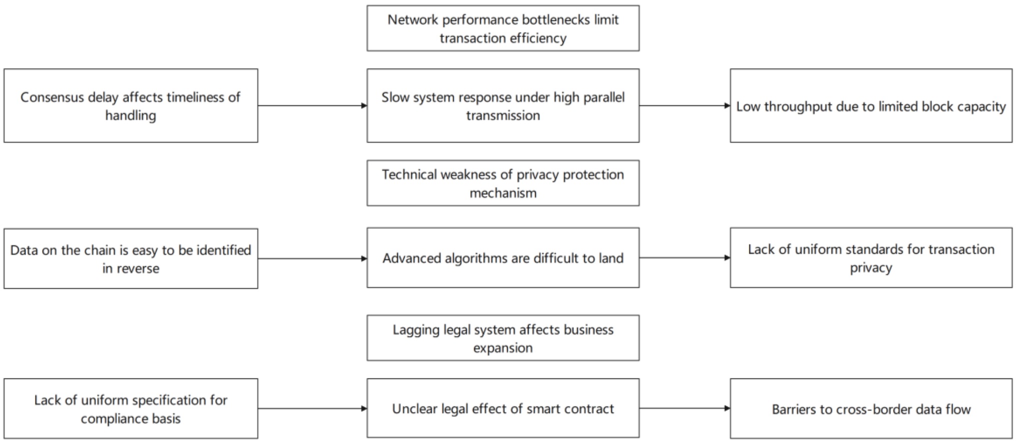
Network performance bottlenecks limit transaction efficiency
Consensus delay affects timeliness of handling
Slow system response under high parallel transmission
Low throughput due to limited block capacity
Technical weakness of privacy protection mechanism
Data on the chain is easy to be identified in reverse
Advanced algorithms are difficult to land
Lack of uniform standards for transaction privacy
Lagging legal system affects business expansion
Lack of uniform specification for compliance basis
Unclear legal effect of smart contract
Barriers to cross-border data flow

Figure 1 problems of blockchain technology in financial infrastructure innovation

4. Development strategy of blockchain technology in financial infrastructure innovation

4.1 Improve network architecture and processing capacity

To meet the high frequency and high reliability requirements of financial institutions' block trading, optimizing the structure has become an important way to improve the overall efficiency of the system. Through the modular design architecture, multi link concurrency and asynchronous technology, the throughput capacity and response speed of the system are increased. For example, hyperledgerfabric operates separately from the consensus phase and the execution phase, and can execute 3500+transactions in one second, an increase of 20582% over the traditional POW system, and the confirmation time is reduced by 96.15%. Nearprotocol uses a segmented chain design, which can execute 2200+transactions in one second, improving the throughput by 12841%, and reducing the confirmation time by 90.77%. China's Financial Alliance beta is designed in an asynchronous parallel architecture. It can trade 3100+transactions in one second, an increase of 18123%, and the confirmation time is less than one second.Details are as follows:

Table 1 performance comparison of different blockchain and financial system architectures

System architecture type	TPS (pen/second)	Confirm latency (s)	TPS improvement rate (compared to Ethereum)	Delay reduction rate (compared to Ethereum)
Ethereum（PoW）	17	13	—	—
Visa payment system	2400	2	↑14082%	↓84.6%
Hyperledger Fabric	3500	0.5	↑20582%	↓96.15%
Near protocol (fragment chain)	2200	1.2	↑12841%	↓90.77%
Financial Alliance chain beta	3100	1.0	↑18123%	↓92.3%

By using state channels, asynchronous BFT consensus algorithms, multi-layer design, and other methods, the efficiency of information exchange between nodes in blockchain systems can be improved, and consistency and task partitioning can be quickly achieved to solve the processing power and response delay problems of traditional architectures. In addition, the improvement of node layout, load balancing and the addition of edge computing devices can improve the scalability and fault tolerance of the system and ensure the security of financial transactions.

4.2 Building an encryption system to enhance data protection

To ensure the security of financial grade blockchain platforms, we need to continuously develop and improve their encryption algorithms. For example, in the traditional hash algorithm SHA-256, its latency is 120ms. Although this can effectively reduce latency, for users, this algorithm cannot achieve maximum complexity and privacy protection. The encryption algorithm can complete calculations during the encryption process, and its security is also extremely high. However, the delay time is relatively high at 2600ms, so compared to hash algorithms, it only has a processing efficiency of 2067%. In addition, zero knowledge proof (ZKP) can ensure anonymous authentication, but its average delay time is 950ms, which is 691.7% compared to hash algorithms, and it has been successfully applied in various privacy transaction systems. Finally, the MPC delay time is 1450ms, which is 1108.3% higher than the hash algorithm. Therefore, this approach is more suitable for data sharing between institutions. Therefore, it can be seen that if a multi style encryption architecture is established, performance and privacy protection must be balanced.

Table 2 illustrates the performance and fitness differences of various encryption methods. Hierarchical applications can enhance overall security capabilities while avoiding load issues caused by individual encryption mechanisms. By integrating various mechanisms in a mixed and applicable form, blockchain systems can balance security performance and efficiency in financial transactions, privacy identities, and model data to support the stability of high-speed, privacy, and advanced financial systems.

Table 2 Performance Comparison and Change Ratio of Blockchain Encryption Technology

Encryption technology type	Average delay（ms）	Delay growth rate (compared to hash)	Application scenarios
Hash function (SHA-256)	120	—	Data authentication and ledger verification
Zero Knowledge Proof (ZKP)	950	↑ 691.7%	Privacy transactions, authorization verification
Multi party secure computation (MPC)	1450	↑ 1108.3%	Cross institutional risk control and joint computing
Homomorphic Encryption (HE)	2600	↑ 2067%	Cryptography analysis, modeling of highly confidential data

4.3 Promote institutional integration and strengthen policy guidance

Promoting institutional integration is an important guarantee for the effective operation of blockchain financial infrastructure. National parliaments are actively promoting the introduction and improvement of laws and regulations related to the legality of legal digital currencies, smart contracts, and regulatory sandbox systems. Currently, Europe has implemented MiCA rules to provide equal protection for all types of cryptocurrencies, with smart contract rules accounting for 80%. On the basis of a legally stable currency, Japan has recognized over 90% of contracts and utilized regulatory sandboxes for 80% of cases. Domestically, it vigorously promotes financial technology innovation regulatory tools and has established sandbox pilot zones covering more than half of the country. Research on smart contract rules is still ongoing, accounting for 50%. Due to the division of labor in law enforcement, only 35% of states in the United States have implemented legislation on different assets. To accelerate the integration of technology and relevant policy adjustments, it is necessary to improve classification governance, judicial adaptation mechanisms, and compliance mechanisms. Comparison Table of Coverage of Blockchain Regulatory System Construction:

Table 3 Comparison of Coverage of Blockchain Regulatory System Construction

Country/Region	Coverage rate of cryptocurrency legislation	Confirmation level of smart contracts	Regulatory sandbox coverage	Estimation of institutional completeness
European Union	100%	80%	70%	83%
Japan	95%	90%	80%	88%
China	80%	50%	60%	63%
America	35%	30%	28%	31%

The estimation of institutional completeness can be concluded from the data analysis in the table that the development of the European Union and Japan is more prominent, and a three-dimensional support system consisting of technology, regulations, and supervision has been formed. China is working hard to build a complete cycle of systems, using experimental projects to clarify legislative paths. Future development may promote greater coordination among various departments, develop unified contract usage standards, and improve cross-border monitoring and coordination structures to meet the needs of blockchain financial services, and practice under policy guidance.

5. Conclusion

As an important technological force driving the transformation of financial infrastructure, blockchain is particularly evident in distributed accounting, smart contracts, and encrypted storage. However, it also faces challenges in practical applications such as network efficiency, personal privacy, and regulations. In order to fully unleash the value of technology, it is necessary to coordinate and promote from three aspects: network architecture optimization, encryption system construction, and policy system connection, and establish an efficient, secure, and compliant blockchain financial environment. In the future, we should continue to promote the standardization of technology, improve the legal system, and innovate regulatory mechanisms to provide solid guarantees for the large-scale implementation and sustainable development of blockchain in the financial field.

References

[1] Ballaji N. Smart Contracts: Legal Implications in the Age of Automation. Beijing Law Review, 2024, 15(03):1015-1032.

[2] Kuznetsov O, Frontoni E, Kuznetsova K, et al. NFT Technology for Enhanced Global Digital Registers: A Novel Approach to Tokenization. Future Internet, 2024, 16(7):252-252.

[3] Yu G, Tianyu Z, Peiwu D, et al. Innovation adoption of blockchain technology in supply chain finance. Production Planning & Control, 2024, 35(9):992-1008.

[4] Yi H, Lidong C, Qingyun X. Optimal pricing decisions for a global fresh product supply chain in the blockchain technology era. International Journal of Logistics Research and Applications, 2024, 27(5):649-666.

[5] R. S, B. P, S. V, et al. Evolutionary gravitational neocognitron neural network based block chain technology for a secured dynamic optimal routing in wireless sensor networks. Journal of Experimental & Theoretical Artificial Intelligence, 2024, 36(3):435-451.

[6] Su H, Luo W, Mehdad Y, et al. Llm-friendly knowledge representation for customer support[C]//Proceedings of the 31st International Conference on Computational Linguistics: Industry Track. 2025: 496-504.

[7] Wu Y. Software Engineering Practice of Microservice Architecture in Full Stack Development: From Architecture Design to Performance Optimization. 2025.

[8] Jiang, Y. (2025). Application and Practice of Machine Learning Infrastructure Optimization in Advertising Systems. Journal of Computer, Signal, and System Research, 2(6), 74-81.

[9] Zou, Y. (2025). Automated Reasoning and Technological Innovation in Cloud Computing Security. Economics and Management Innovation, 2(6), 25-32.

[10] An, C. (2025). Study on Efficiency Improvement of Data Analysis in Customer Asset Allocatior. Journal of Computer, Signal, and System Research, 2(6), 57-65.

[11] Huang, J. (2025). Optimization and Innovation of AI-Based E-Commerce Platform Recommendation System. Journal of Computer, Signal, and System Research, 2(6), 66-73.

[12] Qi, Y. (2025). Data Consistency and Performance Scalability Design in High-Concurrency Payment Systems. European Journal of AI, Computing & Informatics, 1(3), 39-46.

[13] Yuan S. Application of Network Security Vulnerability Detection and Repair Process Optimization in Software Development. European Journal of AI, Computing & Informatics, 2025, 1(3): 93-101.

[14] Lai L. Risk Control and Financial Analysis in Energy Industry Project Investment. International Journal of Engineering Advances, 2025, 2(3): 21-28.

[15] Zhu, Z. (2025). Cutting-Edge Challenges and Solutions for the Integration of Vector Database and AI Technology. European Journal of AI, Computing & Informatics, 1(2), 51-57.

[16] Chen M. Research on Automated Risk Detection Methods in Machine Learning Integrating Privacy Computing. 2025.

[17] Ding, J. (2025). Intelligent Sensor and System Integration Optimization of Auto Drive System. International Journal of Engineering Advances, 2(3), 124-130.

[18] Mingjie Chen. (2025). Exploration of the Application of the LINDDUN Model in Privacy Protection for Electric Vehicle Users. Engineering Advances, 5(4), 160-165.

[19] Liu, X. (2025). Research on Real-Time User Feedback Acceleration Mechanism Based on Genai Chatbot. International Journal of Engineering Advances, 2(3), 109-116.

[20] Zhang, M. (2025). Research on Collaborative Development Mode of C# and Python in Medical Device Software Development. Journal of Computer, Signal, and System Research, 2(7), 25-32.