Dean&Francis

ISSN 2959-6130

A Review of Financial Information Security Technologies Based on Blockchain and Artificial Intelligence

Chuyang Jiang

College of Business, University College Dublin, Singapore, 328071, Singapore
jiangchuyang020507@163.com

Abstract:

As FinTech advances rapidly, information security plays a key role in maintaining the stability of the modern financial system. Yet, traditional centralized security systems are increasingly revealing their limitations when facing new attacks like Advanced Persistent Threats (APTs), data tampering, and identity theft. In response, blockchain and artificial intelligence (AI), as two disruptive technologies, provide new ways to ensure data integrity and boost intelligent defense, respectively. Blockchain achieves data tamper-proofing and transparent traceability via decentralized ledgers, encryption mechanisms, and consensus algorithms, while AI utilizes machine learning and deep learning to enable smart detection, real-time monitoring, and risk alerting. Through the literature review and case studies, this paper explores the core connotations and risk environment of financial information security, systematically elucidating the application mechanisms, synergistic effects, and integration paths of blockchain and AI in the financial field. The study finds that the combination of the two significantly improves the security and intelligence level of the system in areas such as fraud prevention, risk control, privacy protection, and compliance auditing, demonstrating scalable innovation potential. In light of persistent issues like privacy protection, algorithm credibility, and regulatory standardization, this paper outlines potential future enhancements, offering theoretical guidance and practical insights for developing an intelligent and reliable financial information security framework.

Keywords: Blockchain, Artificial Intelligence, Financial Information Security, Intelligent Risk Control, Collaborative Mechanisms

1. Introduction

In the context of the expanding digital economy and increasing financial globalization, financial information has emerged as a vital strategic asset for the country. The openness and complexity of the financial system have enhanced the efficiency of information flow, but at the same time, they have exposed it to a wider range of network threats [1]. Traditional security architecture mainly relies on firewalls, intrusion detection systems and centralized encryption algorithms. Its "boundary protection" model is inadequate in the face of new threats such as distributed attacks, supply chain vulnerabilities and data tampering. The technological landscape for securing financial information has been significantly expanded by recent advances in blockchain and artificial intelligence (AI). In particular, blockchain eliminates the reliance on centralized institutions through distributed ledger technology, ensuring the authenticity and integrity of data, while artificial intelligence uses machine learning algorithms to achieve real-time monitoring and prediction of risks, enhancing the dynamic defense capabilities of the financial system [2]. Through the integration of the two technologies, a "decentralized + intelligent" security framework can be established, offering financial institutions a more transparent, dependable, and traceable operational environment. By reviewing and analyzing existing literature and examining relevant case studies, this paper investigates the role of blockchain and artificial intelligence in financial information security from the aspects of technical principles, application mechanisms, synergistic advantages and development challenges, providing a reference for the design and innovation of financial technology security system.

2. Financial Information Security Risks and Protection Requirements

2.1 Data Security and Transaction Protection

Ensuring the confidentiality, integrity, availability, and non-repudiation of data and transactions is essential for financial information security, which must also contend with increasingly complex security challenges [3]. Among these, data security forms the foundation. Sensitive information can be effectively protected through encryption, access control, and permission management, thereby preventing leakage or tampering. For example, banks typically protect customer account data via hierarchical encryption and dynamic password verification to lower the risk of internal and external attacks. Transaction security is the core of the reliable operation of financial business. Transaction security prevents forgery and tampering via identity verification, transaction signature and anomaly monitoring, and mobile payment platforms boost transaction reliability by employing multi-factor authentication and real-time risk assessment. At the same time, system security provides support for transaction security, and high availability architecture, fault tolerance mechanism and multi-active data center can maintain the continuity and stability of transactions when attacks or failures occur. Besides, compliance and auditability are necessary conditions to ensure the legality and traceability of transactions. Financial institutions must adhere to regulatory requirements, maintain complete operation records, and enhance transaction security while also mitigating risks through effective log management and auditing.

2.2 External Threats and Internal Risks

Financial information systems face diverse and evolving security threats. External threats are the most common form, mainly including distributed denial-of-service (DDoS) attacks, APT attacks, and phishing attacks. These attacks usually directly influence the availability and continuity of the system, putting the operation of financial business at risk of interruption. Internal risks are also not to be ignored. And some employees may compromise data security and the institution's reputation by engaging in unauthorized access or misusing information. These risks are often difficult to fully eliminate with traditional protection methods and must be managed via a combination of access control, behavior monitoring, and auditing mechanisms [4]. In addition, third-party risks are also an important part of financial security. Security weaknesses in outsourced payment gateways, cloud service providers, or supply chain components can serve as entry points for external attacks. As AI technology becomes more widely employed, the prevalence of intelligent attacks is steadily rising. Attackers use machine learning algorithms, automated scripts or data poisoning methods to carry out precise penetration, which puts forward higher requirements for system defense capabilities [4]. These risks are intertwined, making the financial security environment increasingly complex. In this context, financial institutions must establish a comprehensive and multi-layered protection system to deal with various threats from the inside and outside.

2.3 Legal Regulations and Supervisory Requirements

Financial information security relies on both technical safeguards and a robust legal and regulatory framework [5]. For instance, the European Union's General Data Protection Regulation (GDPR) requires financial institutions to adhere to the principles of legality, transparency and minimization throughout the entire data processing process, protect the rights of data subjects, and establish a complete record and audit mechanism. Likewise, the United States (U.S.) Gramm-Leach-Bliley Act (GLBA) sets forth extensive information security requirements for financial institutions, including the protection of customer data, risk assessments, security management plans, and supervision of third-party service providers. It emphasizes the establishment of a cross-departmental information security governance system, mitigating operational risks and legal liabilities through a combination of institutional policies and technical measures. This framework addresses not only external threats but internal and supply chain risks, boosting the resilience of financial institutions against complex threat environments. Regulatory agencies typically mandate that financial institutions implement a security governance system spanning the entire data lifecycle, including risk assessment, incident response, data auditing and compliance reporting. And this institutional arrangement promotes the development of financial security technology, making security protection gradually shift from purely technology-driven to "institutional protection and technology integration."

3. The Role and Limitations of Blockchain Technology in Financial Security

3.1 Technical Principles and Security Mechanisms

Blockchain is a distributed ledger system whose security relies on the synergy of cryptographic algorithms, timestamp mechanisms, and consensus protocols. The hash chain structure ensures data immutability, while consensus mechanisms like Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) enable transaction validation and anti-counterfeiting in a decentralized system. The application of smart contracts expands the functionality of blockchain, enabling transactions to be executed automatically according to preset conditions, reducing human intervention and operational risks [6,7]. These mechanisms offer new technological solutions for financial information security.

Blockchain has shown broad potential in transaction anti-counterfeiting, identity verification, audit tracking, and anti-money laundering supervision. For instance, JPMorgan Chase's JPM Coin utilizes blockchain ledgers to enable real-time interbank clearing and fund transfers, hence reducing settlement risks [8]. In terms of identity management, decentralized identity (DID) systems enhance the autonomy and verifiability of user data, avoiding the risks of monopoly and leakage caused by centralized storage of identity information. In supply chain finance scenarios, platforms such as AntChain use on-chain records to track asset transfers, realize the authenticity verification of trade finance, and prevent double pledging of bills [9]. The traceability of blockchain is also leveraged for anti-money laundering (AML) oversight. And financial institutions utilize on-chain monitoring to detect suspicious transactions and enhance risk management [10].

3.2 Application Limitations and Development Pathways

Blockchain has outstanding advantages in security and transparency, but its application in the financial field is still subject to multiple restrictions. Performance bottleneck is the main obstacle. The transaction throughput of public chains is limited and it is difficult to support high-frequency business. While data transparency boosts traceability, it also introduces the risk of privacy breaches, particularly when handling personal financial information. Vulnerabilities and logical defects in smart contracts may also be exploited by attackers, leading to financial losses or system failures. Regulatory adaptation presents greater complexity. The decentralized nature of blockchain reduces the direct intervention capacity of regulatory bodies, complicating the allocation of responsibilities and risk management [11]. In response to these problems, academia and industry have proposed a variety of improvement directions. Hybrid chain architecture is used to boost system performance, layered design helps to optimize consensus efficiency, and privacy enhancement technologies like zero-knowledge proof attempt to achieve a balance between transparency and confidentiality. The effectiveness of blockchain as a core component in the financial security system ultimately hinges on achieving a dynamic balance between technological innovation and regulatory coordination.

4. The Application and Advantages of Artificial Intelligence in Financial Security

4.1 Intelligent Detection and Proactive Defense

Artificial intelligence is reshaping the financial risk prevention and control system. By leveraging deep learning and machine learning models, the system can extract critical features from complex transaction and behavioral data, establish a dynamic risk identification network, and shift from a "post-event response" approach to a "pre-event warning" system [12]. Models based on random forests or neural networks can identify defaults and suspicious transactions in advance in the credit approval and payment process, significantly improving the accuracy and timeliness of risk identification [13]. At the network defense level, AI has strengthened the ability to detect anomalies. Convolutional neural networks (CNNs) can analyze the structure of malicious code, and recurrent neural networks (RNNs) can capture the time series features of attack behavior and identify potential intrusion paths. Compared with traditional protection that relies on rules, AI can complete modeling and predictive response before the threat occurs, forming an active defense system with self-learning and adaptive capabilities. This mechanism enhances the resilience of the system and promotes the evolution of financial risk governance from static control to dynamic control.

4.2 Data Protection and Intelligent Governance

Artificial intelligence is shifting from an auxiliary tool to a core of governance in data protection. Its algorithmic system enables dynamic supervision of data access and operation behavior and promotes the refinement of data ownership and compliance management. Systems based on natural language processing (NLP) can identify risk information in text in real time. Federated learning and privacy-preserving computing allow data to remain "accessible but not visible" in a distributed environment, ensuring a balance between the efficiency of model training and the need for privacy protection [12,13]. At the same time, AI-driven compliance audit mechanisms are also reshaping the relationship between regulators and enterprises. Automated data classification, access control and anomaly tracking enable financial institutions to generate verifiable compliance reports in real time, reducing the uncertainty of manual audits. More importantly, artificial intelligence is guiding financial security to evolve from a "defense system" to a "governance system". Risk control is no longer limited to technical protection, but forms an organic linkage with business processes, legal norms and ethical constraints. This transformation has laid the foundation for the development of intelligent regulation and compliance technology [14].

5. Synergistic Mechanisms and Innovative Applications of Blockchain and Artificial Intelligence

Blockchain and AI complement each other across data, model, and governance layers. Blockchain creates a trustworthy data environment, ensuring the integrity and authenticity of information while reducing model biases. AI, on the other hand, optimizes blockchain operations through algorithmic predictions and resource scheduling, enhancing consensus efficiency and system stability. In the governance layer, AI's decision-making processes and outcomes are recorded on-chain, ensuring traceability and verifiability [15]. This collaborative mechanism strengthens system security and transparency, laying the foundation for the intelligent evolution of the financial security framework.

In the financial field, the combination of the two has shown application value. In the intelligent anti-fraud system, blockchain ensures the credibility of transaction data, and AI identifies abnormal behavior in real time, which significantly improves the accuracy of fraud detection. After a large commercial bank introduced this technology, the identification rate increased by about 30%. In compliance auditing, AI can automatically analyze smart contract execution logs, discover potential violations and generate reports, reduce labor costs and improve regulatory efficiency. In privacy computing and joint risk control, blockchain enables secure data sharing between institutions, while AI uses federated learning for cross-institutional risk modeling. The blockchain-based federated learning platform, jointly developed by ICBC and several other institutions, has enabled a data analysis model of "usable but invisible" for anti-money laundering monitoring. Nonetheless, its practical application is still limited by privacy protection, algorithm interpretability, and insufficient system standardization. AI models rely on large volumes of data, but data sharing is constrained by compliance regulations. Additionally, black-box algorithms complicate regulatory oversight, and limited blockchain interoperability restricts effective cross-institutional collaboration. Future efforts should concentrate on privacy-enhancing computing, AI-powered dynamic consensus mechanisms, and algorithm governance systems. And the integration of trusted computing and auditable AI will elevate financial information security to a new standard.

6. Conclusion

With the continuous evolution of blockchain and artificial intelligence technologies, the financial information security system is shifting from static defense to intelligent collaboration. The future security architecture will focus on privacy protection, cross-chain interconnection, and algorithmic transparency. First, the combination of privacy-preserving computation and trusted AI will become a mainstream trend. Through technologies such as multi-party secure computation, homomorphic encryption, and zero-knowledge proofs, financial institutions can conduct joint analysis without disclosing raw data, achieving collaborative security where "data is usable but not visible." Second, cross-chain interconnection and intelligent governance will break down barriers between different financial systems, enabling the trusted flow of data and assets. Third, on-chain auditing mechanisms for AI models will ensure the transparency and traceability of algorithmic decisions, thus enhancing regulatory agencies' trust in AI systems. Besides, standardization and ecosystem development are key to advancing technological integration. In addition, establishing unified data security standards and algorithmic governance frameworks will foster a sustainable and regulated fintech ecosystem. The deep integration of blockchain and artificial intelligence not only strengthens the protection capabilities of financial information security at the technological level but also reshapes the trust mechanism of the financial system at the institutional and governance levels. The new security system, which integrates the two, will be characterized by data credibility, algorithmic intelligence, and regulatory transparency, providing solid support for the sustainable and healthy development of digital finance.

References

[1] Yu, Y., & Qayyum, M. (2023). Impacts of financial openness on economic complexity: Cross-country evidence. International Journal of Finance & Economics, 28(2), 1514-1526.

[2] Kukman, T., & Gričar, S. (2025). Blockchain for quality: Advancing security, efficiency, and transparency in financial systems. FinTech, 4(1), 7.

[3] Lee, J. K., Choi, Y. R., Suh, B. K., Jung, S. W., & Kim, K. I. (2025). A Survey on Energy Drainage Attacks and Countermeasures in Wireless Sensor Networks. Applied Sciences, 15(4), 2213.

[4] Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2022). A Unified Framework for Risk-Based Access Control and Identity Management in Compliance-Critical Environments.

[5] Whitaker, J. A., Thornton, M. L., Collins, E. P., Hayes, R. M., & Yusuff, M. (2024). Legal and Regulatory Frameworks for Quantum-Resistant Financial Data Protection.

[6] Kadam, A. A., & Pitkar, H. (2025). Blockchain-Enabled Lean Automation and Risk Mitigation in Supply Chain 4.0 A Systematic Review and Future Directions. Journal of Economics, Finance and Accounting Studies, 7(3), 64-81.

[7] Boranbay, S., Ilyassova, G., Musin, K., Karibayeva, A., Tuleubekova, M., & Balobeyev, A. (2025). Legal Formalization of Smart Contracts: Returning the Term Contract within the Legal Framework. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 17(2), 04525006.

[8] Li, J., Chen, M., & Xu, Y. (2021). A review of the application of blockchain technology in the financial sector. Friends of Accounting, (22), 137-142.

[9] Zhao, X., Zou, Y., & Liu, M. (2022). A discussion on financial service innovation based on blockchain technology. China Certified Public Accountant, (09), 98-100.

[10] He, H., & Li, C. (2022). Analysis of network security based on blockchain technology. Network Security Technology and Application, (09), 23-25.

[11] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309.

[12] Bai, X., Xu, C., Liu, X., & Zhang, L. (2022). A review of blockchain Internet of Things (IoT) security technologies and

key technical analysis. Information Technology, (10), 24-30.

[13] Dong, L., & Li, Y. (2021). An analysis of blockchain technology and its applications in information security. Finance and Economics Review, (01), 48-49.

[14] El Khoury, R., Alshater, M. M., & Joshipura, M. (2025). RegTech advancements-a comprehensive review of its evolution, challenges, and implications for financial regulation and compliance. Journal of Financial Reporting and Accounting, 23(4), 1450-1485.

[15] Kshetri, N. (2025). Building Trust in AI: How Blockchain Enhances Data Integrity, Security, and Privacy. Computer, 58(2), 63-70.