Proceedings of ICMRED 2025 Symposium: Effective Communication as a Powerful Management Tool
DOI: 10.54254/2754-1169/2025.BL24135

The Application of Blockchain and AI in Financial Security: Improving Market Assessment and Risk Management of CAPM

Ruini Weng

Wenzhou-Kean University, Wenzhou, China
2872482885@qq.com

Abstract: With the rapid development of blockchain and artificial intelligence (AI), their integration in financial security has gained increasing attention. This paper explores how these technologies can enhance the capital asset pricing model (CAPM) in market assessment and risk management. Blockchain ensures transparent and tamper-proof financial transactions, while AI leverages big data and machine learning to identify risks and uncover investment opportunities. Through vase studies, this paper explores the integration path of blockchain and AI within CAPM. The results show that this combination not only optimizes CAPM's risk assessment process but also improves its adaptability and predictive accuracy in complex markets. This integrated method helps financial institutions to assess risks more scientifically and make forward-looking decisions. Overall, the synergy between blockchain and AI provides a new path for financial security, enhancing system transparency, responsiveness, and institutional competitiveness. This fusion technology opens up a new situation for the innovative application of CAPM and provides theoretical support and practical reference for building a more intelligent, efficient and secure financial system.

Keywords: Blockchain, Artificial Intelligence, Financial Security, Capital Asset Pricing Model

1. Introduction

In the modern financial system, financial security is the cornerstone of global economic stability and growth. With the rapid development of information technology, financial market risks have become increasingly diverse and complex, putting pressure on traditional risk management methods. Therefore, developing forward-looking, systematic, and intelligent financial security strategies has become a key focus of current research and practice. In recent years, blockchain and AI have been widely applied across the financial industry. Blockchain, with its decentralized, transparent, and tamper-proof nature, offers a secure infrastructure for financial transactions. Simultaneously, AI enhances risk identification, market forecasting, and decision-making through big data analytics and machine learning [1, 2]. The integration of these technologies is reshaping financial security and driving innovation in risk management models. Particularly, when classic tools like the CAPM face challenges in data quality and forecasting, blockchain and AI offer new solutions. Blockchain helps to ensure data authenticity and transparency in CAPM parameter estimation, while AI can improve predictive accuracy and responsiveness to market changes [3, 4]. Thus, studying their synergy in

DOI: 10.54254/2754-1169/2025.BL24135

optimizing models and enhancing risk assessment has theoretical value and practical significance, offering financial institutions more efficient tools and contributing to the stability of evolving financial markets.

2. Key issues and challenges in financial security

In the digital financial era, data privacy and security have become prominent concerns. The widespread application of blockchain and AI enables more efficient decision-making and risk control through large-scale data collection and analysis. However, protecting sensitive customers and transaction data remains a major challenge. Particularly in identity authentication and access control, asymmetric encryption plays a key role [5]. Although blockchain enhances data transparency and security through decentralization, its public ledger mechanism can expose personal information. In addition, decentralized systems require robust access control mechanisms to prevent unauthorized data access and tampering—an area where financial institutions face ongoing difficulty.

Beyond data security, system scalability and operational efficiency present further challenges. As transaction volumes grow, traditional financial infrastructures struggle to process large datasets in real time. Although blockchain offers a secure and transparent recording method, it open falls short in high-frequency trading scenarios. To address this, the RBFT algorithm, an improved Raft consensus, has been proposed to enhance Byzantine fault tolerance [6]. And BLS aggregate signatures are used to increase consensus efficiency [7]. However, integrating these advanced technologies involves high costs, requiring institutions to balance performance improvements against resource investments, while ensuring agility in volatile market environments.

Legal and compliance risks also hinder technological adoption. The rapid development of blockchain and AI often outpaces regulatory systems, leading to uncertainty. For example, during the 2017 ICO boom, many cryptocurrency projects operated in legal grey zones, some eventually found to be fraudulent. In response, the U.S. Securities and Exchange Commission (SEC) investigated multiple cases involving illegal securities issuance [8]. The decentralized nature of blockchain complicates legal liability attribution, and dynamic consensus protocol present further challenges for oversight [9]. On a global level, differences in data protection, anti-money laundering, and anti-fraud increase compliance burdens and legal risks for cross-border operations.

Finally, user trust and acceptance are essential but often overlooked. Despite the potential of blockchain and AI, public understanding of these technologies remains limited. A lack of awareness can hinder adoption and reduce willingness to share data. To overcome this, financial institutions must invest in education, training, and transparent communication to build user confidence. Establishing rigorous security standards and demonstrating the reliability of new systems are also vital steps in gaining user trust and facilitating broader technology integration. To sum up, from data privacy to system performance, from legal compliance to user trust, the challenges facing financial security are multi-dimensionally complex.

3. Blockchain technology overview

3.1. Basic principles and characteristics of blockchain

Blockchain is a distributed ledger system that offers decentralized, tamper-proof, and highly transparent data management—key features that provide strong technical support for enhancing financial security [1, 6]. Its transparency allows all participants to verify transaction records in real time, enhancing fraud prevention and trust. The immutability feature ensures that once recorded, data cannot be easily modified or deleted, thus reducing risks of tampering or data loss. In addition, decentralization eliminates reliance on a single central institution, thereby reducing the risk of single-

DOI: 10.54254/2754-1169/2025.BL24135

point failure. Collectively, these characteristics highlight blockchain's potential to transform traditional financial systems into more intelligent and reliable infrastructures.

3.2. Application of blockchain in financial security

Blockchain has become an important tool in strengthening system stability and transactional transparency across financial security scenarios. Key applications include:

First, in the field of transaction audit and risk control, blockchain enables real-time monitoring and data tracking of the entire transaction process, significantly improving risk control efficiency and regulatory transparency. Second, the smart contract function supported by blockchain can automatically execute contract terms under preset rules, reducing human errors and moral risks. Third, in scenarios such as international payments, asset registration, and supply chain finance, blockchain technology provides a decentralized transaction environment, significantly reducing transaction costs, and improving efficiency and security. For example, consortium chains have been proven effective in trade finance, bills management, and letters of credit, improving cross-institutional data sharing while maintaining privacy protection [10].

3.3. Blockchain-enabled finance model: the rise of DeFi

Decentralized finance (DeFi), especially applications built on Ethereum, has fully demonstrated the huge potential of blockchain technology in improving financial security and efficiency. DeFi eliminates intermediaries and enables users to directly engage in a series of financial activities such as lending, asset trading, and derivative contracts, significantly reducing transaction costs and operating thresholds. With the help of smart contracts on the Ethereum platform, the DeFi system can automatically execute preset rules and avoid human intervention, thereby enhancing the transparency and credibility of financial transactions. For example, the Compound and Aave protocols on the Ethereum platform allow users to borrow and lend with crypto assets as collateral without credit review. This mechanism not only ensures the security of funds but also speeds up the circulation of funds [11].

The rapid expansion of DeFi has attracted a large amount of capital inflow from all over the world. Data shows that the total value locked in DeFi protocols in 2021 once exceeded the US$100 billion mark, fully demonstrating its important position in the current financial market [12]. This explosive growth not only promotes innovation in financial services, but also provides a new technical path for the financial system's risk resistance. DeFi's typical applications fully demonstrate the potential of blockchain technology in improving the transparency, execution efficiency and system security of financial transactions. This technical system not only promotes the innovation of financial service models, but also lays a solid foundation for building intelligent and decentralized financial infrastructure, and expands the development path of the future financial system.

4. Overview of AI technology

4.1. Basic concepts and technologies of AI

AI technology is booming and profoundly reshaping the operating paradigms of various industries. The core concept of AI is to simulate and enhance the computing efficiency of human intelligence, covering multiple levels such as learning, reasoning and self-correction. At present, the main branches of AI technology are machine learning and deep learning, and their core is to simulate human intelligence and achieve autonomous learning and analysis. Specifically, machine learning technology extracts massive amounts of data to enable computers to self-optimize and upgrade based on experience. Deep learning, as a cutting-edge method of machine learning, uses neural networks to

DOI: 10.54254/2754-1169/2025.BL24135

simulate the structure of the human brain and cope with complex data processing problems with higher accuracy and efficiency. Neural networks have shown broad application potential in areas such as image processing and natural language processing [2]. The deep integration of these technologies has effectively promoted the innovative application and extensive expansion of AI in many fields, becoming one of the core driving forces for the development of modern science and technology.

4.2. Application of AI in security monitoring and risk assessment

AI technology has shown great potential in the field of security monitoring and risk assessment, especially in machine learning and deep learning. AI can analyze large amounts of data in real time and quickly identify potential security threats and risks. Machine learning algorithms can train historical data to identify general patterns and abnormal activities, thereby improving the sensitivity of security monitoring systems.

Relatively speaking, deep learning has achieved remarkable results in the field of image and video analysis, and can automatically detect and identify targets such as faces and vehicles, greatly improving monitoring efficiency and accuracy. AI technology has achieved remarkable results in the field of image and video analysis. Emotion recognition and expression recognition technology have significantly improved the performance of monitoring systems through deep learning. Applying AI technology to the risk assessment system of financial institutions can significantly reduce the incidence of fraud incidents, thereby protecting the interests of customers and financial institutions.

4.3. The practice and results of AI in financial security from PayPal

In the field of financial security, AI application cases continue to emerge. Among them, "PayPal" introduced machine learning algorithms to improve risk assessment and fraud detection capabilities, which is a representative case of the successful application of AI technology in financial security [4].

PayPal uses AI to analyze large amounts of transaction data, monitor and evaluate the legitimacy of transactions in real time, and quickly identify abnormal behavior. The system automatically generates risk scores based on historical transaction patterns and user behavior, and takes corresponding security measures. This not only effectively reduces fraud losses, but also improves the user's transaction experience. In addition, PayPal's AI algorithm continues to learn and optimize over time to adapt to new fraud methods and trends. Through this innovative AI application, PayPal has achieved remarkable results in the field of financial security, demonstrating how technology can improve the security and operational efficiency of traditional industries.

5. Application of AI and blockchain in CAPM

CAPM is a financial model used to determine the expected rate of return of an asset. The model emphasizes the trade-off between risk and return and is widely used in portfolio management and capital cost calculation [13]. CAPM can provide an effective portfolio management tool by assessing systemic risk and has a wide impact in financial theory and practice [14]. However, with the increasing complexity of the financial market and the dynamic evolution of the data environment, the traditional CAPM has exposed certain limitations in high-frequency data processing, dynamic risk identification and information asymmetry. To meet this challenge, the development of financial technology in recent years has promoted the deep integration of AI and blockchain technology in the field of financial risk management, providing a new path for the upgrading of traditional financial models.

Under this integration framework, AI and blockchain technology each assume key functions: AI mainly conducts in-depth analysis of historical data, asset prices, macroeconomic indicators and corporate financial information through data mining and modeling, thereby identifying nonlinear risk

DOI: 10.54254/2754-1169/2025.BL24135

factors and potential market trends, and dynamically predicting β values and expected returns of investment portfolios; while blockchain relies on its decentralized ledger and hash encryption mechanism to ensure the integrity and immutability of data, especially in multi-institutional collaborative modeling and cross-platform data sharing scenarios, which can effectively prevent data forgery and abuse.

In actual applications, some financial institutions have introduced similar technology combination practices in their internal risk control systems. For example, IBM has explored the integration of AI and blockchain to enhance credit risk management processes. The company's approach involves using blockchain to create a secure and transparent financial transaction ledger, combined with AI algorithms to analyze and predict credit risk based on transaction data. This integrated solution aims to improve the accuracy of credit risk assessment and reduce operational inefficiencies, demonstrating the potential of combining these technologies to create a more powerful and reliable credit risk management system [15, 16]. This synergistic application of technologies not only provides more accurate and reliable input data for the CAPM, but also enhances its ability to perceive market risks and its robustness in a volatile environment, thereby promoting the pricing method of financial assets to be more intelligent and secure.

Despite the promising prospects, the integration of this technology still faces many challenges. First, financial data is highly sensitive, and AI model training relies on a large amount of personal and institutional data, which requires a balance between model performance and privacy protection. Second, the technical complexity and high operation and maintenance costs of blockchain also place high demands on the technical architecture of institutions. In addition, regulatory policies are still uncertain about cross-border data flows, algorithm transparency, and crypto asset processing, which further increases the difficulty of implementation.

In order to achieve the deep integration of AI and blockchain in financial modeling, financial institutions need to establish a sound data governance and compliance framework, strengthen cross-departmental technical collaboration, and increase employee training investment in the application of new technologies to achieve the simultaneous improvement of risk management capabilities and technological progress. Looking ahead, the synergy of AI and blockchain will play an important role in multiple financial scenarios such as smart contract execution, real-time risk warning, digital identity authentication, and supply chain finance. As these two technologies continue to mature, traditional models such as CAPM are expected to be endowed with higher data processing capabilities and stronger dynamic adaptability, thereby promoting the financial risk management system to a more intelligent, transparent and personalized development stage.

6. Conclusion

This study explores the application of blockchain and artificial intelligence in the field of financial security, and focuses on the potential advantages and practical cases of the combination of the two. Through the analysis of application cases of different financial institutions, it is found that the combination of blockchain-based data transparency and artificial intelligence's intelligent analysis capabilities can help improve market risk identification, credit approval efficiency and investment decision support. In addition, the results show that this combination can not only improve the efficiency and security of financial operations, but also promote the transformation of traditional financial services. Blockchain and artificial intelligence show great potential in improving financial security, but their limitations cannot be ignored. For example, data privacy and compliance issues still hinder the combination of the two, and the complexity and high cost of technical implementation also increase the difficulty of application. Therefore, while promoting the application of technology, financial institutions should carefully assess the possible risks and challenges to give full play to the advantages of both. In the future, the technological development of blockchain and artificial

DOI: 10.54254/2754-1169/2025.BL24135

intelligence will show a deeper integration trend, and the financial industry will benefit from the new application scenarios that will emerge in the future. In addition, the policy and regulatory system will continue to evolve to adapt to the rapidly developing technology. Industry integration will also bring new opportunities and challenges, and promote in-depth cooperation among all parties in interconnection, exchange and data sharing. Future areas of research may include exploring the use of more complex algorithms and smart contracts, as well as potential applications in new areas such as e-commerce, supply chain, and digital identity.

References

[1] *Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.*

[2] *Ishola, A. M., & Obansa, M. S. (2023). The impact of artificial intelligence on financial risk management. International Research Journal of Engineering and Technology, 10(1), 112–118.*

[3] *Fu, J., Qiao, S., Huang, Y., & others. (2020). A study on the optimization of blockchain hashing algorithm based on PRCA. Security & Communication Networks, 2020, Article 8876317.*

[4] *Ghosh, S., Das, N., Das, I., & Maulik, U. (2019). Understanding deep learning techniques for image segmentation. ACM Computing Surveys, 52(4), Article 73.*

[5] *IBM. (n.d.). What is asymmetric encryption? IBM. Retrieved April 29, 2025, from https://www.ibm.com/think/topics/asymmetric-encryption*

[6] *Bai, F., Li, F., Shen, T., et al. (2024). RaBFT: An improved Byzantine fault tolerance consensus algorithm based on Raft. The Journal of Supercomputing, 80, 21533–21560.*

[7] *Li, Z., Sonnino, A., & Jovanovic, P. (2023). Performance of EdDSA and BLS signatures in committee-based consensus. In Proceedings of the 5th Workshop on Advanced Tools, Programming Languages, and PLatforms for Implementing and Evaluating Algorithms for Distributed Systems (Article 13, 5 pages). Association for Computing Machinery.*

[8] *U.S. Securities and Exchange Commission. (2017, December 4). SEC emergency action halts ICO scam. https://www.sec.gov/newsroom/press-releases/2017-219*

[9] *Alzahrani, N., & Bulusu, N. (2019). A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol. Concurrency and Computation: Practice and Experience, 31(16), e5232.*

[10] *Beijing Fintech Industry Alliance Data Committee. (2022). Research report on privacy-preserving financial applications based on consortium blockchain technology. Beijing: Beijing Fintech Industry Alliance. Retrieved from https://www.hbbill.com/front/information/detail.do?id=402880847fb4e348017fcdbaedc10020*

[11] *Castro-Iragorri, C., Ramirez, J., & Velez, S. (2021). Financial intermediation and risk in decentralized lending protocols. arXiv.*

[12] *Dos Santos, S., Singh, J., Thulasiram, R. K., Kamali, S., Sirico, L., & Loud, L. (2022, June). A new era of blockchain-powered decentralized finance (DeFi)-a review. In 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1286-1292). IEEE.*

[13] *Elbannan, M. A. (2015). The capital asset pricing model: an overview of the theory. International Journal of Economics and Finance, 7(1), 216-228.*

[14] *Gao, X., Dai, L., Zhang, J., Han, S., & Chih-Lin, I. (2015, June). Capacity-approaching linear precoding with low-complexity for large-scale MIMO systems. In 2015 IEEE International Conference on Communications (ICC) (pp. 1577-1582). IEEE.*

[15] *Farazi, M. Z. R. (2025). Evaluating the impact of AI and blockchain on credit risk mitigation: A predictive analytic approach using machine learning. International Journal of Science and Research Archive, 13(1), 575–582.*

[16] *Eniola, J., & Amos, G. (2024). AI and Blockchain: A New Era for Credit Risk Mitigation in Financial Services. Retrieved from https://www.researchgate.net/publication/387107823_AI_and_Blockchain_A_New_Era_for_Credit_Risk_Mitigation_in_Financial_Services ResearchGate*