Research on the Application of Blockchain Technology in Ensuring Network Security

Qingwang Jie[1], Xueyong Zhou[2]

Hebei Fangwei Network Technology Co., Ltd. Shijiazhuang, Hebei 050000

Abstract: ***With the rapid development of information technology, network security issues are becoming increasingly prominent, and traditional network security technologies are facing new challenges. The article aims to discuss the role of blockchain technology in ensuring network security, and analyze the advantages, challenges, and future trends faced by blockchain technology. This article first summarizes the definition, principles, and core characteristics of blockchain technology, and compares it with traditional network security technologies. Then, the article delves into the current applications and potential advantages of blockchain technology in network security from multiple perspectives, including data security sharing, authentication and access control, network attack protection, and smart contract security. At the same time, it points out the technical challenges, legal and ethical issues, and regulatory and policy deficiencies faced by the application of blockchain technology in network security, and finally provides relevant countermeasures and suggestions. Finally, a brief summary of the entire paper is made, highlighting the prospects and significance of blockchain applications in the field of network security, and pointing out future research directions and potential challenges, demonstrating the forward-looking and exploratory spirit of academic papers.***

Keywords: Blockchain technology; Network security; Data security sharing; Identity authentication; Smart Contract Security.

1. INTRODUCTION

The rapid development of information technology has made network security issues increasingly prominent, while traditional network security technologies are inadequate in the face of new challenges. Blockchain technology, with its unique distributed ledger, encryption algorithm, and consensus mechanism, has brought new solutions to network security. The article will conduct an in-depth exploration of the application of blockchain technology in ensuring network security, and analyze its advantages, challenges, and future development trends, with the aim of providing a new research perspective and solution ideas for the field of network security. Recent studies have advanced the modeling of robot-environment interactions [1] and intelligent monitoring systems leveraging multimodal data [2]. Concurrently, research focuses on reliability optimization in cloud environments [3] and trustworthy autonomous driving frameworks enhanced by blockchain technology [4]. In 3D generation, methods optimizing viewpoint consistency through diffusion models have been developed [5], while explainable AI frameworks are proposed for risk mitigation [6]. Robust 3D vision is addressed via cross-modal fusion networks for point cloud completion [7]. In data-driven applications, innovative cross-attention multi-task learning approaches improve digital advertising recall [8], and PID-based systems are designed for autonomous vehicle speed control [9]. Privacy preservation in distributed learning is a key concern, with studies proposing multi-layer defense strategies against attacks in federated learning [10] and robust frameworks for secure collaborative AI [11]. Furthermore, the integration of IoT with spatiotemporal graph networks enhances motion analysis [12]. Earlier work also established graph convolutional networks based on matrix factorization for recommendation systems [13].

2. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

2.1 Definition and Principles of Blockchain Technology

As one of the distributed ledger technologies, blockchain technology can be defined as a data storage structure jointly maintained by several nodes and cannot be tampered with. The core principle of this technology is to establish a decentralized network system, in which each node stores a copy of the entire network data. Blockchain uses encryption algorithms to ensure data security, and utilizes consensus mechanisms to verify and record transaction behavior, making data consistent and tamper proof.

The foundation of blockchain technology is blocks, each of which contains a set of transaction records and is linked to the previous block through cryptographic methods such as hash functions to form a chained data structure. This structure not only ensures data integrity, but also ensures that transaction records in the network are validated and consensus is reached through Proof of Work (PoW) or other consensus mechanisms [1]. The decentralization and consensus driven characteristics of blockchain technology give it unique advantages in the field of network security.

2.2 Core Characteristics of Blockchain Technology

The core features of blockchain technology are mainly manifested in its distributed ledger, encryption algorithm, consensus mechanism, and immutability.

One is that distributed ledger technology enables every node on the blockchain network to store a complete ledger data, and this decentralized data storage method enhances data security and reliability. Secondly, blockchain technology utilizes complex encryption algorithms such as hash functions and public-private key encryption to ensure data confidentiality and integrity. In addition, in blockchain networks, the process of reaching consensus between nodes is called consensus mechanism, among which common mechanisms include proof of work (PoW) and proof of stake (PoS). In order to ensure the smooth operation of the network, they adopt incentive and penalty strategies. Thirdly, blockchain has immutability, which means that once data is written into the blockchain, it cannot be easily modified or deleted, providing a strong guarantee for the security of data in the blockchain.

2.3 Comparison between blockchain technology and traditional network security technology

Compared to traditional network security technologies, blockchain technology has unique advantages in ensuring network security.

Firstly, blockchain distributed ledger technology can effectively prevent single point of failure and enhance system stability and reliability. Moreover, traditional network security technologies often rely on centralized servers, and when attacked, the overall system will be impacted to a certain extent.

The second is that blockchain encryption algorithms and consensus mechanisms provide multiple protections for data security, and traditional network security technologies may have vulnerabilities in data encryption and authentication. In addition, blockchain has immutability, and once the data is uploaded, it will be immutable, which has a strong support for the authenticity and integrity of the data. Traditional network security technologies may have insufficient protection for data integrity. However, in practice, blockchain technology also faces challenges such as slow processing speed and high resource consumption, which to some extent constrain its development in the field of network security. So in terms of network security, blockchain technology and traditional network security technology should complement each other's strengths and weaknesses, and work together to build a more secure and reliable network environment.

3. THE APPLICATION OF BLOCKCHAIN TECHNOLOGY IN NETWORK SECURITY

3.1 Application of blockchain technology in data security sharing

In the field of data security sharing, blockchain technology provides new ideas for solving this problem. The traditional data sharing model usually relies on centralized data sharing

Sharing databases not only increases the risk of data leakage, but also restricts the efficiency and scope of data sharing. Blockchain technology achieves data immutability and transparency by establishing a decentralized distributed ledger, laying a solid foundation for secure data sharing. One is that blockchain has immutability, ensuring that once data is recorded on the chain, it cannot be modified or deleted. This feature is crucial for protecting data integrity and authenticity. The second is that blockchain has transparency, which allows all participants to see and verify data in real time, which is conducive to building trust and reducing fraudulent behavior. In addition, blockchain has a distributed nature, where data is no longer focused on a single server, greatly reducing its likelihood of being attacked.

Blockchain technology has been applied in various data security sharing scenarios in practice. Taking the medical field as an example, the use of blockchain can achieve secure sharing of patient health records while protecting patient privacy. In terms of supply chain management, blockchain can be used to track product sources and circulation processes to ensure transparency and security in the supply chain. The use of blockchain in the financial sector can achieve transaction record sharing, increase transaction transparency and efficiency.

3.2 Application of blockchain technology in identity authentication and access control

Identity authentication and access control are at the core of network security. Traditional authentication systems generally rely on centralized databases to store user identity information and access permissions, which are not only vulnerable to attacks but also difficult to adapt to distributed and cross platform application scenarios. Blockchain technology provides decentralized solutions for identity authentication, access control, and other aspects.

The application of blockchain technology to identity authentication and access control has the following characteristics: firstly, it can be used to establish a decentralized identity authentication system. The system stores user identity information and access permissions in the blockchain, independent of centralized servers. This not only increases system security, but also enables users to authenticate themselves across platforms and applications without the need for repeated registration and login; The second is that blockchain can achieve fine-grained access control. Blockchain implements access control for users through smart contracts, ensuring that only users who meet the conditions can access specific resources. This mechanism can be used in various scenarios such as file sharing and cloud service access control within enterprises; The third is to use blockchain to improve the efficiency and convenience of identity authentication. For example, blockchain can be combined with biometric technology to achieve password free identity authentication. Users can use biometric features such as fingerprints and facial recognition to verify their identity without the need to memorize complex passwords; Fourthly, the use of blockchain can protect users' privacy. The blockchain system can encrypt and store user identity information and access records to protect their privacy. At the same time, blockchain has immutability and can ensure that user identity information is not tampered with by third parties without authorization.

3.3 Application of blockchain technology in preventing network attacks

In the field of network security, network attacks are considered one of the main threats, including but not limited to distributed denial of service attacks (DDoS), Malicious software and phishing attacks, etc. Blockchain technology provides a new defense mechanism for preventing network attacks due to its characteristics of immutability and decentralization [3]. Firstly, the distributed ledger structure of blockchain enables data to be stored on multiple nodes in the network, making it more difficult for attackers to tamper with the data. Secondly, the blockchain consensus mechanism requires the majority of nodes in the network to form consensus, which can effectively resist DDoS attacks. Attackers need to control a large number of nodes simultaneously to affect the normal operation of the network. In addition, the use of blockchain technology can track and determine the source of network attacks, and automatically implement security policies through smart contracts, thereby improving response speed and efficiency. However, blockchain technology also faces challenges in preventing network attacks, including node security and network scalability. Therefore, it is necessary to conduct in-depth research and optimization on blockchain technology in order to enhance its application effectiveness in network security.

3.4 Application of blockchain technology in smart contract security

Smart contracts, as an important part of blockchain technology, can implement contract terms without the need for intermediaries. The security of smart contracts is of great significance in ensuring smooth transactions. Blockchain technology provides security for smart contracts with features such as transparency and immutability. Firstly, smart contracts are open and transparent in terms of encoding and execution results, which is conducive to timely detection and correction of potential security issues. Secondly, blockchain has immutability, ensuring that smart contracts cannot be modified or deleted after deployment in the blockchain to protect contract integrity. In addition, blockchain technology can be combined with formal verification and other technologies to more rigorously verify whether smart contracts are secure. However, smart contracts also face challenges in terms of security, such as complex contract design and potential vulnerabilities. Therefore, it is necessary to strengthen the research on the security of smart contracts to improve their security and reliability.

3.5 Application of blockchain technology in network security regulation and policy recommendations

In today's rapidly developing blockchain technology, the application of blockchain in the field of network security has also received high attention from regulatory agencies and policy makers. Applying blockchain technology to network security regulation and policy recommendations can provide new ideas and methods for network security governance [4]. One is to use blockchain technology to record and track network security events, enhancing regulatory transparency and efficiency. Secondly, blockchain technology can provide data support and decision-making basis for policy formulation in conjunction with current network security regulations and policies. In addition, the use of blockchain technology can automate the supervision of network security, implement security policies through smart contracts, and conduct compliance checks. However, the application of blockchain technology in network security regulation and policy recommendations also faces challenges such as the lack of technical standards and inadequate regulatory frameworks. Therefore, it is necessary to strengthen the research on blockchain in network security supervision, continuously improve relevant technical standards and regulatory frameworks, and promote the healthy development of blockchain in network security.

4. CHALLENGES AND COUNTERMEASURES FACED BY BLOCKCHAIN TECHNOLOGY IN NETWORK SECURITY

4.1 Technical Challenges of Blockchain Technology in Network Security Applications

The first challenge that blockchain technology needs to face when applied to the field of network security is the technical level. The distributed ledger structure of blockchain not only enhances system security, but also brings about issues with data storage and processing efficiency. With the increasing amount of network data, ensuring the scalability of blockchain systems has become an urgent technical challenge that needs to be addressed. In addition, the consensus mechanism of blockchain systems has problems such as high energy consumption and low efficiency while ensuring data consistency. How to improve the operational efficiency of blockchain systems while ensuring security is also a technical challenge that needs further research [5]. When applying blockchain technology to network security, it is also necessary to address the security issues of smart contracts. Smart contracts are a very important part of blockchain technology, and the security of their encoding directly affects the overall security of the system. However, the writing and deployment of smart contracts involve certain complexities, and once there are vulnerabilities in the contract code, it may be maliciously exploited, leading to security risks. So how to enhance the security of smart contracts and prevent contract vulnerabilities is a technical challenge that blockchain technology needs to address when applied to network security.

4.2 Legal and Ethical Issues of Blockchain Technology in Network Security Applications

The application of blockchain technology in the field of network security not only faces technical challenges, but also involves legal and ethical issues. The anonymity and decentralization of blockchain technology not only enhance system security, but also provide opportunities for cybercrime. How to avoid the application of blockchain technology in illegal activities while protecting user privacy is a legal and ethical issue that needs to be considered. In addition, the application of blockchain technology in data sharing and identity authentication also involves data ownership and usage rights. How to reasonably determine the ownership and purpose of data, while ensuring data security and avoiding behaviors such as data abuse and privacy leakage, is also an urgent legal and ethical issue that needs to be addressed when applying blockchain technology to network security.

4.3 Regulatory and policy recommendations for blockchain technology in network security applications

In the face of the challenges faced by the application of blockchain technology in network security, in addition to improving the technical level and resolving legal and ethical issues, it is necessary to strengthen supervision and introduce relevant policies. Firstly, the government and relevant departments should increase the supervision of blockchain technology, introduce clear regulatory policies and standards to regulate the use of blockchain in the field of network security, and avoid technological abuse and risk diffusion. The second is to establish and improve the security assessment and risk prevention mechanism of blockchain technology. Timely discover and resolve security risks in the blockchain system through regular security assessments, enhancing system security and stability; The third is to strengthen the training of blockchain technology network security talents and technological innovation. Encourage universities and research institutions to conduct research and education on blockchain technology in order to cultivate more professional talents.

5. CONCLUSION

The article conducts an in-depth exploration of the application of blockchain technology in the field of network security, and comprehensively analyzes its technical principles, practical applications, challenges, and countermeasures. Domestic and foreign scholars widely believe that blockchain technology, due to its core features of distributed ledger, encryption algorithms, and consensus mechanisms, has brought new solutions to network security and can effectively address various challenges brought by traditional network security technologies.

The research conclusion shows that blockchain technology has significant advantages in data security sharing, identity authentication and access control, prevention of network attacks, and smart contract security. However, the application of blockchain technology in network security also faces technical challenges such as high resource consumption and slow transaction speeds. At the same time, there are also legal and ethical issues, as well as regulatory and policy deficiencies.

In short, the application of blockchain technology in the field of network security has broad prospects, but there are also many challenges. Only through multiple measures such as technological innovation, legal norms, and policy guidance can the potential of blockchain technology in the field of network security be fully realized, providing strong support for building a secure, reliable, and efficient network environment.

REFERENCES

[1] Guo, Y., & Tao, D. (2025). Modeling and Simulation Analysis of Robot Environmental Interaction. Artificial Intelligence Technology Research, 2(8).
[2] We, X., Lin, S., Pruś, K., Zhu, X., Jia, X., & Du, R. (2025). Towards Intelligent Monitoring of Anesthesia Depth by Leveraging Multimodal Physiological Data. International Journal of Advance in Clinical Science Research, 4, 26–37. Retrieved from https://www.h-tsp.com/index.php/ijacsr/article/view/158
[3] Yang, Y. (2025). Research on Site Reliability Optimization Technology Based on Synthetic Monitoring in Cloud Environments.
[4] Tang, Z., Feng, Y., Zhang, J., & Wang, Z. (2026). SVD-BDRL: A trustworthy autonomous driving decision framework based on sparse voxels and blockchain enhancement. Alexandria Engineering Journal, 134, 433-446.
[5] Lu, K., Sui, Q., Chen, X., & Wang, Z. (2025). NeuroDiff3D: a 3D generation method optimizing viewpoint consistency through diffusion modeling. Scientific Reports, 15(1), 41084.
[6] Zhang, T. (2025). From Black Box to Actionable Insights: An Adaptive Explainable AI Framework for Proactive Tax Risk Mitigation in Small and Medium Enterprises.
[7] Xie, J., Zhang, L., Cheng, L., Yao, J., Qian, P., Zhu, B., & Liu, G. (2025). MARNet: Multi-scale adaptive relational network for robust point cloud completion via cross-modal fusion. Information Fusion, 103505.
[8] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.
[9] Y. Zhang, Z. Tian and H. Hua, "Design of an Autonomous Vehicle Speed Control System Based on a PID Controller," 2025 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2025, pp. 491-495, doi: 10.1109/AEECA65693.2025.00092.
[10] Deng, X., & Yang, J. (2025, August). Multi-Layer Defense Strategies and Privacy Preserving Enhancements for Membership Reasoning Attacks in a Federated Learning Framework. In 2025 5th International Conference on Computer Science and Blockchain (CCSB) (pp. 278-282). IEEE.
[11] Sultan, N., Patwar, N., Wei, X., Chew, J., Liu, J., & Du, R. (2026). FedGuard: A Robust Federated AI Framework for Privacy-Conscious Collaborative AML, Inspired by DARPA GARD Principles. International Academic Journal of Social Science, 2, 1–16. https://doi.org/10.5281/zenodo.18253151
[12] Zhu, Y., Yu, W., & Li, R. (2025). SAGCN: A spatiotemporal attention-weighted graph convolutional network with IoT integration for adolescent tennis motion analysis. Alexandria Engineering Journal, 128, 652-662.

[13] Yang, J., Wang, Z., & Chen, C. (2024). GCN-MF: A graph convolutional network based on matrix factorization for recommendation. Innovation & Technology Advances, 2(1), 14–26. https://doi.org/10.61187/ita.v2i1.30