A Preliminary Exploration of the Application of Edge Intelligence in Blockchain Security Defense

Nan Jiang
Changjun High School International Department, Changsha, 410002, China
vinson1087@outlook.com

Abstract

This article aims to explore the application of edge intelligence in blockchain security defense. Firstly, it introduces blockchain technology and the security challenges it faces, including the security of consensus mechanisms, vulnerabilities in smart contracts, and cyber attacks, etc. Then, the concept, characteristics and key technologies of edge intelligence were expounded, such as edge computing and artificial intelligence algorithms. Then, a detailed analysis was conducted on the specific application scenarios of edge intelligence in blockchain security defense, such as real-time security monitoring, abnormal behavior detection, and enhanced privacy protection. Finally, the development trend, challenges and value brought by the integration of edge intelligence in blockchain security defense were prospected.

Key words: Edge intelligence; Blockchain; Security defense; Real-time monitoring; Privacy protection.

1. Introduction

Since Satoshi Nakamoto proposed the concept of Bitcoin and expounded on its underlying technology in 2008, blockchain technology has triggered a transformative application wave in numerous fields such as finance, supply chain, healthcare, and government affairs, thanks to its decentralized, immutable, and traceable features [1]. In the financial sector, blockchain has enabled rapid settlement of cross-border payments, reduced transaction costs and enhanced transaction transparency. In supply chain management, blockchain can be used to track the real-time flow information of goods, ensuring the authenticity and quality traceability of products [2].

However, with the wide application and continuous development of blockchain technology, the security threats it faces are becoming increasingly complex and diverse. From early simple cyber attacks to today's advanced vulnerability exploits targeting consensus mechanisms and smart contracts, security issues have become a key factor restricting the further large-scale application of blockchain technology [3]. Traditional blockchain security defense methods, such as monitoring based on centralized security servers and rule-based intrusion detection systems, often have problems like response delays, inability to adapt to distributed environments, and difficulty in handling massive amounts of data, making it hard to meet the increasingly complex security requirements [4].

Edge intelligence, as an emerging technology that combines edge computing with artificial intelligence, has advantages such as low latency, high efficiency, and distributed intelligence [5]. Edge computing migrates computing tasks from the cloud to the network edge, enabling data to be processed closer to the data source and reducing the time and bandwidth consumption for data transmission to the cloud. Artificial intelligence algorithms endow edge devices with the ability to intelligently analyze and make decisions, enabling real-time processing and analysis of collected data and timely detection of potential security threats [6]. Therefore, edge intelligence offers new ideas and methods for blockchain security defense, which is expected to address the limitations of traditional security defense methods and enhance the security and reliability of blockchain networks.

2. Blockchain Technology and Its Security Challenges

2.1 Overview of Blockchain Technology

Essentially, blockchain is a distributed ledger technology, which consists of a sequence of data blocks arranged according to chronological order. Each of these data blocks encompasses transaction information from a specific time frame, along with the hash value of the preceding data block and a timestamp, among other elements [7] .In a blockchain

network, the nodes uphold the uniformity of the ledger by employing a consensus mechanism. This mechanism guarantees that the ledger data stored on every node is identical. Frequently used consensus mechanisms encompass Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and so on [8].

Smart contracts are automatically executed contracts on the blockchain. They exist in the form of code on the blockchain. When specific conditions are met, smart contracts will automatically perform corresponding operations without the intervention of a third party [9]. The emergence of smart contracts has enabled the application of blockchain technology to no longer be confined to simple value transfer, but can be extended to various complex business scenarios, such as decentralized finance (DeFi) and non-fungible tokens (NFTS).

2.2 Security Challenges Faced by Blockchain

Different consensus mechanisms have different security risks. Take the PoW mechanism as an example. It competes for the right to record transactions by requiring miners to solve complex mathematical problems. Although it ensures the security of the blockchain to a certain extent, it also has some security risks. Among them, the 51% attack is one of the most serious threats. That is, when an attacker controls more than 51% of the computing power, they can tamper with the transaction records on the blockchain and carry out malicious behaviors such as double-spending attacks [10].

Although the PoS mechanism has solved the problem of excessive energy consumption of the PoW mechanism, it also faces other security challenges, such as "unprofitable" attacks and "long-range attacks". In "unprofitable" attacks, attackers can influence the consensus process by temporarily holding a large number of rights and interests to obtain improper benefits. "Long-range attack" refers to an attacker using the rights information of historical blocks to tamper with the historical records of the blockchain [11].

The code of smart contracts may have vulnerabilities, which could be exploited by attackers, leading to attacks on the contracts and causing asset losses. Common vulnerabilities in smart contracts include reentrant attacks, integer overflows, improper permission control, etc [12]. A reentrant attack refers to an attacker who, during the contract invocation process, recursively calls the contract again before the contract state is updated, thereby repeatedly obtaining the assets within the contract.

Blockchain networks may be subject to various cyber attacks, such as distributed denial-of-Service DDoS and Sybil attacks. DDoS attacks affect the operation of the entire blockchain network by sending a large number of requests to nodes in the blockchain network, occupying the computing resources and network bandwidth of the nodes, causing them to be unable to work normally [13].

3. The Concept, Characteristics and Key Technologies of Edge Intelligence

3.1 The Concept of Edge Intelligence

Edge intelligence involves deploying artificial intelligence algorithms on edge devices, enabling them to have the capabilities of data processing and analysis, and achieving local data processing and real-time decision-making. Edge intelligence combines the low latency and high bandwidth of edge computing with the intelligent analysis capabilities of artificial intelligence, enabling rapid data processing and decision-making close to the data source, and reducing the time and bandwidth consumption for data transmission to the cloud.

3.2 Characteristics of Edge Intelligence

Low latency: Edge devices are located near the data source and can process and respond to data in a short time, meeting application scenarios with high real-time requirements.

High efficiency: Edge intelligence can reduce the amount of data transmitted to the cloud, lower the occupation of network bandwidth, and enhance data processing efficiency.

Distributed intelligence: Edge devices can independently process data and make decisions, and multiple edge devices can work collaboratively to achieve distributed intelligence.

Privacy protection: Data is processed locally, reducing the risk of data transmission over the network and helping to protect users' privacy.

3.3 Key Technologies of Edge Intelligence

Edge computing represents a technology that shifts computing tasks away from the cloud and towards the network edge, and by placing computing resources on edge devices, it enables the local processing of data. Algorithms of artificial intelligence, which encompass machine learning, deep learning, and various other types, are employed to analyze and construct models based on the data gathered by edge devices, ultimately facilitating intelligent decision - making. Moreover, the data collected by edge devices might originate from diverse sensors and devices, so data fusion and processing are necessary to enhance the quality and usability of the data.

4. Application Scenarios of Edge Intelligence in Blockchain Security Defense

4.1 Real-time Security Monitoring

In a blockchain network, edge devices can be deployed on each node to collect real-time data such as the operational status and transaction information of the nodes. Through edge intelligence technology, real-time analysis and processing of these data can promptly detect abnormal behaviors in the network, such as abnormal connections of nodes and abnormal transactions. For instance, when an edge device detects a sudden and significant increase in the transaction frequency of a certain node, it can immediately issue an alert to remind the network administrator to conduct further investigation and handling, thereby effectively preventing the occurrence of attack behaviors.

4.2 Abnormal Behavior Detection

Edge intelligence can use machine learning algorithms to model normal behavioral patterns in blockchain networks, and then detect abnormal behaviors by comparing real-time collected data with normal behavioral patterns. For instance, for the execution of smart contracts, a normal execution pattern model can be established by analyzing historical contract execution data. When there is a significant deviation between the new contract execution data and the model, it can be determined as abnormal behavior, which may be a sign of vulnerability or an attack. Edge devices can promptly upload abnormal behavior information to the blockchain network, triggering the corresponding security defense mechanism.

4.3 Enhanced Privacy Protection

Although transaction information on the blockchain is protected to a certain extent through encryption technology, there is still a risk of privacy leakage in some cases. Edge intelligence can preprocess transaction data on edge devices, such as data desensitization and encryption enhancement operations, to reduce the leakage of sensitive information. For instance, on edge devices, transaction amounts are blurred, retaining only the approximate range without transmitting the specific amount values, thereby protecting users' privacy. Meanwhile, edge intelligence can also utilize cryptographic techniques such as zero-knowledge proofs to verify the validity of transactions without disclosing transaction details.

4.4 Optimization of Consensus Mechanism

Edge intelligence can dynamically adjust the parameters of the consensus mechanism based on the real-time status of the blockchain network, thereby enhancing the security and efficiency of the consensus mechanism. For instance, in the PoW mechanism, edge devices can monitor the distribution of network computing power in real time. When they find that the computing power proportion of a certain mining pool is too high, they can automatically adjust the difficulty target to increase the difficulty for attackers to tamper with the ledger. In addition, edge intelligence can also combine the advantages of other consensus mechanisms to propose new hybrid consensus mechanisms and enhance the overall security of the blockchain network.

4.5 Smart Contract Security Audit

During the development stage of smart contracts, edge intelligence can play an important role in pre-emptive defense. By leveraging static analysis technology, intelligent auditing tools on edge devices can conduct in-depth analysis of contract code. By constructing code structure models such as syntax trees and control flow diagrams, common security risks that may exist in the code, such as reentry vulnerabilities and integer overflow vulnerabilities, can be precisely located. For instance, in the case of reentry vulnerabilities, static analysis tools can detect whether there is a situation in the contract where a function that can be called externally calls the external contract again before the state update.

Dynamic analysis involves running smart contracts in a simulated blockchain environment. Edge intelligence monitors the execution process of the contracts and collects runtime data, such as changes in variable values and function call stacks. By combining machine learning algorithms to model the runtime characteristics of normally running contracts, when a new contract exhibits behavior that deviates significantly from the normal model during dynamic analysis, it can

be determined that the contract may have potential risks. Edge devices conduct a comprehensive assessment of static and dynamic analysis results, providing developers with detailed vulnerability reports and repair suggestions, thereby reducing the chance of smart contract vulnerabilities entering the blockchain network from the source.

5. The Value Brought by the Integration of Edge Intelligence and Blockchain Security Defense

5.1 Enhance the Speed of Security Response

The traditional blockchain security defense system often relies on centralized security servers or cloud analysis platforms. Data needs to be transmitted from blockchain nodes to the cloud for processing and analysis, which will cause significant delays. Edge intelligence brings data processing and analysis capabilities down to edge devices, enabling security monitoring and decision-making to be completed quickly near the data source. For instance, in real-time security monitoring scenarios, edge devices can immediately respond to detected abnormal behaviors without waiting for data to be transmitted to the cloud, significantly reducing the security response time. This can promptly prevent the further spread of attack behaviors and effectively minimize the losses caused by security incidents to the blockchain network.

5.2 Enhance the Comprehensiveness of Security Defense

Blockchain networks have the characteristics of distribution and heterogeneity, and different nodes may face different security threats. Edge intelligence can deploy personalized security defense strategies on each edge node, conducting targeted security monitoring and protection based on the specific environment and business requirements of the node. Meanwhile, multiple edge devices can work collaboratively, share security information and threat intelligence, and form a distributed security defense network. This comprehensive security defense system can cover all aspects of the blockchain network, from the security of individual nodes to the collaborative defense of the entire network, effectively addressing various complex security challenges.

5.3 Reduce Security Costs

Traditional blockchain security defense methods usually require a large amount of computing and storage resources to support security analysis and processing in the cloud. As the scale of the blockchain network continues to expand, the security cost will also increase accordingly. Edge intelligence reduces the amount of data transmitted to the cloud by processing and analyzing data on edge devices, thereby lowering the demand for cloud computing and storage resources. In addition, edge intelligence can also utilize the idle computing resources of edge devices for security defense tasks, improving the utilization rate of resources and thereby reducing the overall security cost.

5.4 Promote the Innovative Development of Blockchain Technology

The integration of edge intelligence and blockchain security defense provides new impetus for the innovative development of blockchain technology. On the one hand, a secure and reliable blockchain network can attract more users and enterprises to participate, promoting the application and popularization of blockchain technology in more fields. On the other hand, the application of edge intelligence also prompts blockchain technology to innovate and optimize in aspects such as architecture design, consensus mechanism, and smart contracts, in order to better adapt to the environment and demands of edge intelligence. For instance, in order to work better in coordination with edge intelligence, blockchain networks may need to design more efficient lightweight consensus mechanisms to enhance the processing capacity and response speed of nodes.

6. Development Trends and Challenges of Edge Intelligence in Blockchain Security Defense

6.1 Development Trends

Integration with 5G technology: 5G technology features high speed, low latency, and large capacity. When combined with edge intelligence, it can provide stronger support for blockchain security defense. For instance, 5G networks can offer more stable edge device connections, enhancing the efficiency and reliability of data transmission.

Cross-chain security defense: With the continuous development of blockchain technology, cross-chain applications are becoming increasingly widespread. Edge intelligence can play a significant role in cross-chain scenarios, enabling security monitoring and collaborative defense among different blockchain networks.

The degree of intelligence is constantly improving: In the future, edge intelligence will continuously introduce more advanced artificial intelligence algorithms, such as reinforcement learning and federated learning, to enhance the intelligence level of blockchain security defense and achieve more autonomous and efficient security defense.

6.2 Challenges Faced

Limited resources of edge devices: Edge devices typically have limited computing resources and storage capacity. How to achieve efficient security defense under limited resources is a challenge. It is necessary to optimize artificial intelligence algorithms, reduce their complexity and enhance the processing capabilities of edge devices.

Data security and privacy protection: Edge intelligence involves a large amount of data collection and processing. How to ensure the security and privacy of data on edge devices is an important issue. It is necessary to enhance the application of security technologies such as data encryption and access control.

Lack of standard norms: Currently, the application of edge intelligence in blockchain security defense still lacks unified standard norms, and there are compatibility issues among edge devices and solutions from different manufacturers. It is necessary to formulate relevant standards and norms to promote the healthy development of edge intelligence in the field of blockchain security defense.

7. Conclusion

Edge intelligence, as an emerging technology, provides new approaches and methods for blockchain security defense. Through application scenarios such as real-time security monitoring, abnormal behavior detection, and enhanced privacy protection, edge intelligence can effectively improve the security of blockchain networks and reduce security risks. Meanwhile, the integration of edge intelligence and blockchain security defense brings numerous values such as enhancing security response speed, improving the comprehensiveness of defense, reducing security costs, and promoting technological innovation and development. Although edge intelligence still faces some challenges in blockchain security defense, with the continuous development and improvement of technology, its application prospects are broad. In the future, efforts should be made to further enhance the research on the integration of edge intelligence and blockchain technology, and promote the wide application of edge intelligence in blockchain security defense.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[2] Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of information management, 39, 80-89.
[3] Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, 13938-13959.
[4] Habiba, M., Islam, M. R., Muyeen, S. M., & Ali, A. S. (2023). Edge intelligence for network intrusion prevention in IoT ecosystem. Computers and Electrical Engineering, 108, 108727.
[5] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE internet of things journal, 3(5), 637-646.
[6] Zhang, K., Zhu, Y., Maharjan, S., & Zhang, Y. (2019). Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things. IEEE network, 33(5), 12-19.
[7] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.
[8] Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019, October). SoK: Consensus in the age of blockchains. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (pp. 183-198).
[9] Szabo, N. (1997). Formalizing and securing relationships on public networks. First monday.
[10] Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95-102.
[11] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, July). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual international cryptology conference (pp. 357-388). Cham: Springer International Publishing.

[12] Atzei, N., Bartoletti, M., & Cimoli, T. (2017, March). A survey of attacks on ethereum smart contracts (sok). In International conference on principles of security and trust (pp. 164-186). Berlin, Heidelberg: Springer Berlin Heidelberg.
[13] Karame, G. O., Androulaki, E., & Capkun, S. (2012, October). Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 906-917).