# Industrial Internet Security Protection Strategy Based on the Blockchain

**Hua Sun, Jiale Wu*, Yirang Yin**
*Industrial Information Security (Sichuan) Innovation Center Co., Ltd (ICICS), Chengdu, Sichuan, China*
**Corresponding Author*

**Abstract: With the rapid development and wide application, the industrial Internet integrates a large number of industrial equipment and systems, and involves massive data exchange and processing, which brings security risks such as data leakage, illegal access and system attacks, while improving the production efficiency. The blockchain technology can provide a secure and reliable network environment with its unique decentralization characteristics, data immutability and high transparency. Therefore, based on the blockchain technology, this paper discusses the security protection strategy of industrial Internet, in order to provide theoretical references for the healthy development of industrial Internet.**

**Keywords: Blockchain; Industrial Internet; Safety Protection**

## 1. Introduction

With the deep integration of information technology and industrial production, the industrial Internet has led the digital and intelligent revolution of the manufacturing industry, realized the seamless flow of data and the decision optimization, and improved the production efficiency and economic benefits by connecting machines, equipment and systems[1]. However, the highly networked and systematic characteristics make the industrial Internet face security risks such as external attacks, internal data leakage, and malware infringement, which seriously hinder the wide application of industrial Internet technology. In this context, the application of blockchain technology in the industrial Internet can enhance the security and transparency of data with its unique decentralization feature, data immutable through encryption and the traceability of transactions; and it can automatically manage network access through the functions such as smart contracts to improve the overall security of the system. Therefore, this paper will discuss the security protection strategy of industrial Internet based on the blockchain, in order to provide theoretical references for the security management of industrial Internet.

## 2. Security Requirements of the Industrial Internet

As an advanced network platform connecting equipment, data and personnel, the industrial Internet undertakes the taskS of optimizing production processes, promoting the operation and maintenance efficiency and improving the product quality. To this end, the security requirements of the industrial Internet include ensuring the data integrity, protecting data from unauthorized access, and preventing service interruptions. The data integrity means that the data will not been tampered, deleted or damaged in any way during the transmission or storage to ensure the accuracy of the production process and quality control. Protecting data from unauthorized access requires the industrial Internet to implement strict access control policies to ensure that only authorized users and devices can access specific network resources and data. Preventing service interruption requires the industrial Internet to monitor the operating status of the system in real time, detect abnormal behavior early, and respond quickly to security incidents to ensure the continuous and stable operation of the industrial Internet. These security requirements are the basis for effectively improving the security protection capability, stability and sustainable development of the industrial Internet[2].

## 3.Application of Blockchain Technology in Industrial Internet

 

### 3.1 The selection and Architecture Design of Blockchain Technology

Due to the decentralized nature, the blockchain technology provides a unique way to enhance the integrity and security of data, and its principle diagram is the Figure 1. The public chain in blockchain technology provides the highest level of transparency and security and is suitable for application scenarios that require a high degree of decentralization. The private chain operates under the control of a single organization and is suitable for internal business processes with high privacy and control requirements. The consortium chain is somewhere between the public and private chain, is jointly managed by multiple organizations, and is suitable for industrial applications where multiple trusted parties are required to work together. Therefore, the choice of blockchain technology needs to choose the right type of blockchain based on the specific business needs and security requirements of the industrial Internet. In the architecture design of blockchain, it is need to consider the compatibility of blockchain technology with existing industrial control systems, and to establish a stable data interface between traditional industrial data processing systems and blockchain platforms to ensure that data can be safely and accurately transmitted between various systems, and necessary security enhancement functions can be provided without interfering with existing operations, so as to further optimize the business process and improve the operational efficiency[3].

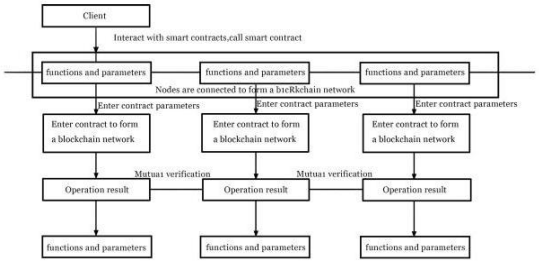


**Figure 1. Principle Diagram of Blockchain Technology**

### 3.2 Data Protection and Privacy Guarantees

Due to the data immutability, the application of blockchain technology in the industrial Internet can ensure the integrity and accuracy of the data generated in the production process, ensure the security of the data in the storage and transmission process, so that every data transaction is encrypted through a complex algorithm. It prevents the data from being stolen, ensures the privacy of the data and is beneficial to ensure the reliability of the production quality and process control. In the context of the industrial Internet, an identity authentication system that does not rely on a single centralized entity can be created based on the blockchain technology, so that every access request needs to be verified by a majority of nodes in the network. It reduces the risks of identity falsification, enhances the resistance of the entire system to fight against internal and external security threats, promotes the continuous operation of the system and supports the transformation of the industrial Internet to higher security standards.

### 3.3 Access Control and Identity Authentication

By utilizing the decentralization and immutability features of blockchain, a transparent and secure identity authentication system can be built, so that every device, sensor and user can have a unique identity, and all identity information and corresponding access rights records are stored on the blockchain. It enhances the security of identity information, improves the transparency of the system management, and further ensure the legality and correctness of the operation. In the industrial Internet environment, dynamic access control policies can be implemented by deploying smart contracts. When the equipment needs to be maintained or upgraded, the smart contracts can automatically update the access rights of the equipment to ensure that only authorized technicians can access the relevant equipment, which can reduce the need for manual intervention, improve the efficiency of the operation, reduce the security risks caused by human error or abuse of authority, and provide a reliable guarantee for the safe operation of the industrial Internet.

## 4.Industrial Internet Security Protection Strategy Based on Blockchain

### 4.1Enhanced Device-level Security Protocols

The industrial Internet environment usually includes a variety of sensors, control systems and intelligent machines. In order to improve the security of these devices, blockchain-based

 

security protocols can be used to ensure that only verified and authorized devices can access and operate the network by taking advantage of the immutablility and encryption of the blockchain, so as to reduce the security risks caused by tampering or unauthorized access to the equipment, which can ensure the stability and security of the entire production network. Based on the blockchain technology, the process of each device status check and update can be automatically recorded and verified, and once the software version of the device is detected to be backward or there is a security vulnerability, the smart contracts can automatically trigger the update program to ensure that all devices are running the latest and most secure software version. It can help the industrial Internet maintain a high degree of security and reliability in the increasingly complex environment of network threats, improve the overall security of the industrial system, reduce the burden of manual equipment maintenance, and ensure the transparency and correctness of industrial Internet activities[4].

### 4.2 On-chain Data Activity Monitoring

In the industrial Internet environment, based on the transparency and immutablility of the blockchain technology, a comprehensive monitoring system can be established, so that every data transmission, modification or access event can be recorded on the blockchain, and a permanent and irreversible history for real-time tracking and recording of all data interactions and operations in the industrial Internet can be generated. When the system detects abnormal data access or potential data leakage behavior, the security team can quickly track the relevant data operation records, determine the source of the problem, and take appropriate security measures to strengthen the prevention and control of data leakage and abuse, which is conducive to the smooth progress of security audit and compliance inspection. In industrial Internet operations, smart contract programming can be used to define specific security rules and conditions. When the system monitors data activities that violate security rules, preset response measures can be automatically implemented such as restricting user access rights, notifying system administrators or initiating security protection procedures to reduce the delay of manual intervention and improve the accuracy and efficiency of handling security incidents. Therefore, the industrial Internet can effectively improve the control and protection of complex data environments and ensure the security and continuity of business operations.

### 4.3 Decentralized Threat Intelligence Sharing

In the traditional threat intelligence sharing model, information is often concentrated in some specific centers or platforms, which increases the risk of data attack and has the trust risk of information flow. Based on the blockchain technology, it is possible to create a decentralized platform that allows multiple trusted entities to collaborate, in which each participant can contribute and receive the latest threat data including malware fingerprints, IP addresses, web-sites, and other details about security threats, and exchanging information directly without going through a central authority. It can facilitate the sharing of security information between different organizations, make participant respond to emerging threats quickly, and enhance the security of the entire industry. Through the smart contracts of blockchain technology, the validity of information can be verified without disclosing specific details to realized the anonymization of data processing and access control, and the sensitive data or personal information of any enterprise will not be disclosed when sharing sensitive threat information, which is conducive to ensuring the security and privacy of information sharing and encouraging more enterprises to participate in the threat intelligence sharing network. It further changes the limitations of traditional security protection, provides a more dynamic and interactive defense mechanism, and brings broader and deeper security to the industrial Internet environment.

### 4.4 Persistent Transaction Auditing

The industrial Internet uses the immutable and complete audit tracking capabilities of blockchain technology to persist the details of each transaction to the blockchain. In this way, all operation records will be permanently preserved and open to all participants to provide a fully transparent operation history, so that the source of transactions can be quickly tracked when a security incident occurs. It can

 

enhance the compliance, help to prove that the operation and processing of data are in accordance with relevant regulations and standards, and ensure that the integrity and accuracy of data can be maintained in complex networks with multiple parties. On this basis, each node participates in the verification process of data in the blockchain network. Such decentralization ensures that the audit system will not be affected by a single point of failure, improves the anti-attack capability of the system. The immutable nature of the audit log reduces internal risks and increases the strictness of the internal control of the enterprise, so as to provide an additional layer of the protection against internal abuse and fraud. In addition, in practical applications, the persistent transaction audit of blockchain can record the data interaction from sensors, robots and other industrial equipment in real time. When a violation or abnormal transaction is found, smart contracts can automatically issue an alarm and take preset countermeasures such as suspending the transaction, restricting user rights or reporting it directly to security managers. It improves the efficiency of audit, effectively prevents the spread of problems, and enhances the response ability of defense system to internal threats and external attacks. This shows that the industrial Internet platform based on blockchain technology can provide a more secure and reliable network environment to provide security guarantees for the continuous operation and data management of enterprises.

## 5. Conclusion

Based on the security requirements of the industrial Internet, this paper analyzes the application of blockchain technology in the industrial Internet, including the selection and architecture design, data protection and privacy assurance, access control and identity authentication of blockchain technology, and puts forward security protection strategies such as enhanced device-level security protocols, on-chain data activity monitoring, decentralized threat intelligence sharing, and persistent transaction auditing, so as to improve the security of the industrial Internet, enhance the data transparency and operational traceability, support more efficient and secure industrial operations, ensure the continuity of business operations and integrity of data, and promote the sustainable development and innovation of the industrial Internet.

## Acknowledgments

This paper is supported by Chengdu Science and Technology Innovation Project“Research on Industrial Internet Data Security Sharing and Privacy Protection Technology ”(2021-YF08-00151-GX).

## References

[1] CHEN Dapeng. Research on Identity Analysis System of Industrial Internet Based on Blockchain [J]. Intelligent Computers and Applications, 2019,14(03):218-222.

[2] YANG Jing. Research on Optimal Allocation of Industrial Internet Resources by Integrating Edge Computing and Blockchain [J]. Network security and Informatization,2024,(2):71-73.

[3] XIANG Yanjie, ZhANG Huan. Research on Blockchain Distributed Identity Authentication Model for Internet of Things [J]. Wireless Internet Technology,2024,21(1):118-121.

[4]Liu Y D，Hua Y H，Chen Q R. Research on Key Technologies of Data Security and Privacy Protection in Internet of Things Group Intelligence[J]. Optical and Quantum Electronics , 2024(56) .

 