


Article

Research on Trusted Management of Industrial Internet Identity Analysis Data Based on Blockchain

Zhibo Qi ^{1,2}, Tao Huang ^{1,*} , Boyang Zhang ³, Yue Li ³ and Xin Zhang ³

¹ State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; qizhibo@caict.ac.cn

² Department of Industrial Internet Institute, China Academy of Information and Communication, Beijing 100083, China

³ Key Laboratory of Industrial Internet and Big Data, China National Light Industry, Beijing Technology and Business University, Beijing 100048, China; 2130062075@st.btbu.edu.cn (B.Z.); 2130062057@st.btbu.edu.cn (Y.L.); zhangxin@btbu.edu.cn (X.Z.)

* Correspondence: htao@bupt.edu.cn

Abstract: As an important part of the industrial internet, identity analysis data are growing with the expansion of the field involved in the industrial internet. The management of industrial internet identity analysis data faces many problems, such as complex types, a wide range of information, rapid growth, reduced security, etc. In view of the above problems, a trusted management model of industrial internet identity analysis data based on blockchain is first designed. Meanwhile, the identity analysis data information is analyzed and classified, and industrial data are divided into three levels according to the degree of privacy for hierarchical encryption. Secondly, the “on-chain + off-chain” storage model combining the blockchain main-slave chain and the off-chain database is designed to improve the efficiency of the whole model. Then, a collaborative consensus mechanism suitable for the main-slave multi-chain of the industrial internet is also designed, including slave-chain CIPBFT consensus, inter-chain cross-chain transmission protocol and main chain KZKP consensus. Finally, a prototype system is built to analyze the correctness, security, scalability and consensus efficiency of the model proposed in this study. The results show that the model proposed in this study can be applied to trusted management of data information for industrial internet identity analysis, and also provides an optimized solution for the same problem in fields of the industrial internet.

Keywords: industrial internet; identity resolution data; blockchain; main-slave multi chain; privacy security; trusted management



Citation: Qi, Z.; Huang, T.; Zhang, B.; Li, Y.; Zhang, X. Research on Trusted Management of Industrial Internet Identity Analysis Data Based on Blockchain. *Symmetry* **2023**, *15*, 2102. <https://doi.org/10.3390/sym15122102>

Academic Editor: Alice Miller

Received: 18 September 2023

Revised: 2 November 2023

Accepted: 21 November 2023

Published: 23 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent years, with the continuous growth of the world economy, a new round of scientific and technological revolution as well as industrial transformation are progressing fast. The internet has rapidly extended from the consumption field to the production field, and the industrial economy has expanded in depth from digitization to networking and intelligence. The innovative development of the internet interacts with the new industrial revolution in a historical way. In this context, the industrial internet was born [1]. Industrial internet identity analysis empowers objects with a unique identity through bar codes, QR codes, radio frequency identity tags, etc. The service goal of the identity analysis data is to carry out industrial identity data management and cross-enterprise, cross-industry, cross-region and cross-country data sharing and using with the help of identity coding resources and identity resolution system [2–4].

However, as the industrial internet constantly evolves, people’s demand for the interconnection of everything is also increasing [5]. The industrial internet identity analysis data contains a wide range of industries, including production, design, manufacturing,

procurement, warehousing, sales, after-sales and other processes that require the participation of industrial internet identity analysis data. Therefore, the management of industrial internet identity analysis data faces many problems, such as complex types, a wide range of information, rapid growth, low security, etc. [6,7]. For this reason, a safe and efficient management method is urgently needed to solve the problems existing in the current identity analysis data of the industrial internet [8].

Blockchain technology is defined as a chain data structure that connects and combines data blocks in chronological order. It is a distributed infrastructure that uses cryptographic methods to avoid data from being tampered with and forged, uses consensus algorithms to transmit and update data, and uses smart contracts composed of automated script code to operate on data [9–13].

In recent years, many scholars have studied the security management of industrial internet data. With the development of blockchain technology with its characteristics of decentralization, difficulty to be tampered with, distributed storage, etc., many scholars have applied it to the information management of various industries and the security management of industrial internet data. Jeong et al. proposed a blockchain-based industrial Internet of Things (IIoT) information enhancement model, which can ensure the data integrity of the IIoT generated by the industrial site. The model can process the data that may occur at the end of the industrial site into the blockchain by independently processing the data generated by the same IIoT device, effectively ensuring the security of data information [14]. In order to solve the problem of missing data collection in the industrial internet platform, Yu et al. proposed a rule-based optical gradient elevator (LightGBM) algorithm to fill the missing data of the industrial internet according to the operation mechanism of the industrial internet platform. They used examples to verify that the algorithm fills the data faster with smaller errors and better performance [15]. Sergii et al. proposed a new blockchain structure called “blockchain tree” and hence created a multi-level protection system, which not only stores information from ID cards but also improves the level of security and access control for that information [16]. Ding et al. designed a complete copyright registration protection application system by combining blockchain technology with digital copyright registration technology. The system emphasizes copyrighted data storage and embodies the security and credibility of blockchain technology [17]. Wang et al. constructed a blockchain-based rice supply chain information supervision model and adopted a variety of encryption algorithms to protect the sensitive data of enterprises in the supply chain, meeting the need for efficient supervision by regulatory authorities and effectively improving the security of rice supply chain data information [18]. Xu et al. proposed the concept of blockchain and industrial internet connector suitable for data traceability in the grain and oil industry, and hence built a grain and oil quality and safety traceability model. They also designed a wheat quality and safety traceability system to provide a solution for the traceability of wheat supply chain data information [19]. Peng et al. researched the information control on a rice supply chain based on multi-chain collaboration and designed a multi-chain collaboration model of “blockchain + child chain”, in which the trusted chain mechanism, multi-level sub-chain encryption mechanism, trusted supervision mechanism, and hierarchical consensus mechanism were designed to realize trusted management and control of the rice supply chain [20]. Through the analysis of the above research, scholars have made a preliminary study on the application of blockchain technology in the security management of the industrial internet and studied the trustworthy management of data security in the industrial internet or other areas in terms of information security. However, this research is mostly based on the single-chain structure of blockchain without involving specific methods of data privacy circulation. Faced with complex industrial multi-source scenarios, the increase in nodes in the blockchain network and the accumulation of ledger data pose great pressure on the storage capacity and system efficiency of the blockchain.

Considering that the management of the industrial internet identify resolution data faces many problems, such as complex types, large amounts of information, wide range, rapid growth, and reduced security [21,22], this study proposes a trusted management

model of the industrial internet identify resolution data based on blockchain multi-chain, which provides a common model for the industrial internet across industries on the whole, which divides sub-chains of different industries. In this way, data autonomy across industries can be realized while data from different industries can be isolated. Each industry contains redundant links from R&D, production, manufacturing, supply, inventory, sales, operation and maintenance, etc.; therefore, the main-slave multi-chain model is applicable to various industries. By dividing different links from the slave chain, information collaborative verification within the industry through the main chain is achieved. Blockchain technology can effectively defuse the centralized risk of traditional models. The main-slave multi-chain architecture reduces the storage pressure of traditional blockchain while isolating data in plaintext, thus improving the overall collaborative authentication efficiency of the model. In addition, the step-by-step consensus mechanism and cross-chain transmission protocol proposed in this study not only ensure data privacy across industries but also realize the cross-industry information collaborative consensus certification of the industrial Internet data. The main-slave multi-chain architecture and data flow mode in this study offer a set of general solutions for trusted management of cross-industry analysis data in the industrial Internet.

This paper makes the following specific contributions:

(1) It comprehensively analyzes the characteristics of various information of the industrial internet, and classifies industrial data according to the degree of privacy, which realizes hierarchical governance within the data chain.

(2) A trusted management model of industrial internet identity analysis data based on blockchain multi-chain is designed, and data trusted management is realized through hierarchical encryption, cross-chain transmission and dual-mode storage.

(3) The multi-chain consensus mechanism of industrial internet based on CI-PBFT, cross-chain transmission protocol and KZKP is designed, which realizes intra-chain trusted consensus, cross-chain trusted transmission and global security collaborative consensus.

(4) A trusted management model of industrial internet identity analysis in this study is universally applicable in various application fields of industrial internet.

The article structure of this paper is as follows. Firstly, in the relevant work part, trusted management of industrial internet data and the application of blockchain technology to trusted management of data in recent years are investigated. Secondly, a blockchain-based trusted management model of industrial internet identity analysis data is designed. The identity analysis data information is analyzed and classified at the same time, and the information is classified into three levels for hierarchical encryption. The “on-chain + off-chain” storage model combining the blockchain main-slave chain and the off-chain database is designed to improve the efficiency of the whole model. In addition, a collaborative consensus mechanism suitable for main-slave multi-chain of the industrial internet is also designed. Then, the correctness, security and scalability analysis of the model is carried out, and a prototype system is built to verify the model by example. Finally, in the results and outlook section, the whole research is summarized, and the next research is planned.

2. Related Work

In this section, the application status of data security management in industrial internet-related fields, data trusted management based on blockchain technology, and cutting-edge research on data trusted management combined with the two are investigated and summarized, as shown in Table 1.

Table 1. Preliminary Research Work Investigation.

Research Content	References
Data security management research of industrial internet	[23–27]
Data trusted management research based on blockchain	[28–35]
Data Trusted Management research of industrial internet data based on blockchain	[36–41]

In terms of data security management research of industrial internet, Misra et al. [23] explored the security risks existing in four major industries of IIoT: medical, transportation, mining and manufacturing; analyzed the existing solutions and challenges, and discussed the research gaps to mitigate these risks. In addition to minimizing the harm and risk to personnel, it is the current research hotspot to improve the security and privacy of the data environment and to enhance data management by interconnecting various units. Gebremichael et al. [24] pointed out that the complexity of the IIoT infrastructure makes it difficult to guarantee the availability, confidentiality and integrity of data. They tried to provide a comprehensive overview of security and privacy in the IIoT according to the recommendations from well-known standardization agencies, comprehensively analyzed various security protocols and solutions, highlighted the existing security weaknesses and vulnerabilities, and outlined possible directions for further research to solve some of the security and privacy issues currently facing IIoT data. Al-Rakhami et al. [25] proposed ProChain, a traceability framework based on the Internet of Things (IoT) supply chain system aiming at the complexity of the storage, accessibility and multi-participant of industrial data in the IIoT. The framework relies on the IOTA Tangle network. It collects industrial data through IoT sensors, enhances the model scalability through DLTiota distributed ledger technology, and verifies the processability, transparency and security of the framework through examples, providing feasible research ideas for enhancing the credible traceability management of industrial data. Boudagdigue et al. [26] proposed a dynamic trusted architecture H-IIoT suitable for industrial environments to enhance trusted management in industrial equipment in view of the security and privacy of data integrated into industrial processes. Based on this, the Tm-IIoT dynamic trusted management model was proposed to monitor the trusted measurement of nodes in the architecture, and finally, the simulation proved that the model has good adaptability and trusted management capabilities to ensure that the industrial equipment is protected from malicious attacks. Saqlain et al. [27] pointed out that in the industrial environment, the quantity, heterogeneity, timeliness and other characteristics of industrial data bring great challenges to data collection, processing and decision-making. For this reason, they proposed an industrial data management system IDMS based on the IoT. The system realizes the retrieval and collection of huge industrial data through the middleware layer and realizes the distributed storage and rapid transmission of data through communication channels and metadata modules. The verification results show that the framework can effectively support huge industrial data collection, providing the basis for the secure management of industrial data. Through the analysis of the above research, it can be seen that most research on data security management of the industrial internet has focused on the overall architecture, while studies on how to enhance trust among multiple participants in the industrial internet, the industrial data privacy protection and the data security and credibility are urgently needed.

As a decentralized distributed ledger technology, blockchain ensures safe and trustworthy value transfer among participants and provides a good application environment for data-trusted management. Based on characteristics of the off-chain database OCBS to improve scalability, reduce storage burden and enhance data privacy, Miyachi et al. [28] proposed a hybrid privacy protection framework hOCBS by combining with blockchain technology to make the model better meet the needs of the medical and health industry. The framework improves medical and health information management by realizing sharing, sovereignty and enhancing trust. Jiang et al. [29] proposed a multi-chain network architecture of the Internet of Vehicles based on blockchain technology, which provides a feasible solution for the centralized management of the Internet of Vehicles data through the decentralized distributed storage of the blockchain. With the development of computing technology, data trust and security problems emerge in the large amount of data collected by edge terminals and IoT devices. Ma et al. [30] proposed a blockchain-based edge computing trusted data management scheme, BlockTDM, which provides sensitive data security protection and trusted management through mutual authentication protocols, flexible consensus, smart contracts, data management and node deployment. Address-

ing the lack of data integrity and data privacy in transportation networks, Li et al. [31] proposed a decentralized location-aware architecture integrating a modular blockchain network and non-interactive zero-knowledge range proof to solve the data trust problem in transportation systems. Chen et al. [32] designed a blockchain-based personnel information management system according to the tamper-proof and traceability of blockchain technology, which avoids personnel information leakage, information tampering and trust loss, as well as verified the feasibility of applying blockchain technology to personnel information management. Song et al. [33] designed a low-energy dual-chain structure suitable for agricultural scenarios by combining blockchain with IoT technology, providing transparent and sustainable management methods for traditional agriculture. Relying on the tamper-proof and traceable characteristics of blockchain technology. Okegbile et al. [34] proposed a sharing scheme for blockchain data in IoT networks based on cloud edge computing and designed the BeHDS system in the cloud edge environment, as well as demonstrated the ability to compensate for each other's limitations of the integrated blockchain and the cloud edge computing-based technology, so as to improve PBFT consensus for system performance evaluation. The results show that the analysis proposed in this study can be used to study the performance of any data-sharing system supporting blockchain, which enhances security for data sharing under blockchain technology. Okegbile et al. [35] analyzed the performance of the blockchain data-sharing framework in terms of delay and data age and studied the applicability of blockchain technology in the data-sharing system. They also proposed an enhanced blockchain data-sharing system with PBFT consensus and captured the verification of the PBFT scheme by using Erlang sequential distribution. Finally, through experiments, it is verified that when using blockchain technology in time-sensitive data-sharing applications, various influential system parameters must be carefully considered. The study has improved researchers' understanding of the blockchain PBFT consensus algorithm.

The above research provides a trusted research method among multiple participants for blockchain information management.

In terms of the application of blockchain in industrial internet data management, as a key element in the industrial Internet, the security of industrial data has always been taken seriously. Considering scattered equipment and difficulty in connection to the industrial internet, Zhang et al. [36] proposed a trusted management scheme for industrial data based on the editable blockchain of the industrial internet, which reduces the system operation cost while effectively responding to malicious behaviors, thus enhanced the security of trusted management of industrial system data. With the development of information technology and personalized needs, manufacturing service collaboration based on industrial internet has become the main method of manufacturing collaboration, but the trust issue among participants hinders the development of information technology. Tao et al. [37] proposed a DT-BC (digital twin-blockchain) enhanced manufacturing collaboration mechanism for industrial internet platforms to improve data accuracy and trust among participants, as well as enhance manufacturing service management. In order to solve problems of low blockchain data transmission security, high transaction management cost and difficult supervision in the past industrial IoT, Liang et al. [38] proposed an IIoT data transmission security technology based on Fabric blockchain, which realizes a reliable trading center with the power blockchain sharing model, and realizes the secure matching of power data transmission by designing a power data consensus mechanism and dynamic link storage, and realizes the secure matching of power data transmission. In view of the heterogeneity of industrial infrastructure, Ceccarelli et al. [39] proposed a software platform called FUSION that combined blockchain with SDN and container-based orchestration, which intends to flexibly configure terminal devices or edge nodes around FESN as a trusted industrial IoT node and to verify that it can make the access edge devices accessed in railway business cases more trusted to manage trust information, even if operators do not trust each other. Given the high latency and easy failure of the traditional identity resolution architecture based on handle analysis, Huo et al. [40] proposed a trusted identifier co-governance archi-

texture applied to the IIoT and designed a decentralized identifier service framework based on blockchain. Based on the identifier life cycle management of smart contracts and the data storage mechanism of trusted identifiers, the whole architecture avoids single-point failure, data tampering, governance deviation, etc., which reduces the cost of trust in data circulation. Singh et al. [41] proposed a cloud-based centralized cross-domain data-sharing platform that involves multiple secure gateways. The secure gateways store information in a centralized cloud through blockchain, and the device authentication is enhanced through temporary elliptic curves Diffie-Hellman (ECDHE) and identity-based signatures (IBS). Through a comparison between the experiment results and existing studies, they found that the proposed security and privacy framework helps maintain trust among industries that collaborate across fields and facilitates secure movement of data between different domains worldwide, providing an optimized solution to data sharing.

By analyzing the above research, it can be seen that most researchers started with the infrastructure in the industrial scenario to increase trust among devices and enhance data credibility with the distributed feature of the blockchain. However, there is little research on the application of blockchain technology to the entire industrial Internet. Therefore, this study will focus on how to achieve cross-industry data management, data privacy protection and data collaboration in the industrial scenario.

3. Trusted Management Model of Industrial Internet Identity Analysis Data

3.1. Construction of Trusted Management Model of Industrial Internet Identity Analysis Data Based on Blockchain

A trusted management model of industrial internet identity analysis data is constructed based on the main-slave blockchain and smart contracts, as shown in Figure 1. The model generally consists of three parts. Firstly, the industrial internet involves industries such as raw materials, manufacturing, construction, consumer goods, food and agriculture. The public traceability data and industrial confidential data in the identity analysis data are stored in the off-chain database and blockchain network, respectively, through the dual-mode storage mechanism. Secondly, the blockchain network is composed of the slave chain corresponding to different industries of the industrial internet and a main chain responsible for completing cross-industry and cross-chain consensus. In the industrial internet, the correlation of information in different industries is low, and there is privacy data corresponding to their respective industries. Therefore, different child chains are set up to facilitate data autonomy between different industries. Each slave chain is composed of nodes corresponding to typical links in their respective industry. The slave chain first completes the intra-chain consensus in its respective industry, and after the data are cross-chained to the main chain, the main chain completes the industrial internet global collaborative consensus. Finally, the smart contract part is responsible for data storage, data hierarchical encryption and data cross-chain interaction functions among chain networks so as to realize trusted management of industrial internet identity analysis data.

3.2. Information Analysis and Classification of Industrial Internet Identity Analysis Data

The industrial internet is the product of deep integration of a new generation of information and communication technology and modern industrial technology, and an important carrier of being intelligent, networked and data-based of the manufacturing industry, as well as one of the important areas of China's new infrastructure. Industrial internet identify resolution data are to give each entity or virtual object a unique identity code through bar codes, two-dimensional codes and radio frequency identify tags, etc. It carries relevant data information that enables positioning, connection and dialogue of entities and virtual objects, therefore, serves as the data basis for intelligent interconnection and interoperability of data between different systems [42]. Industrial internet identity analysis data refers to the data generated, collected, transmitted, stored, used, shared or archived by industrial internet-related enterprises when carrying out R&D, design, manufacturing, operation, management, application and service to meet customers' needs

for orders, plans, R&D, design, technology, manufacturing, procurement, supply, inventory, sales, delivery, after-sales, operation and maintenance, scrapping or recycling and other industrial production and operation links and processes under the new model and format of the industrial internet.

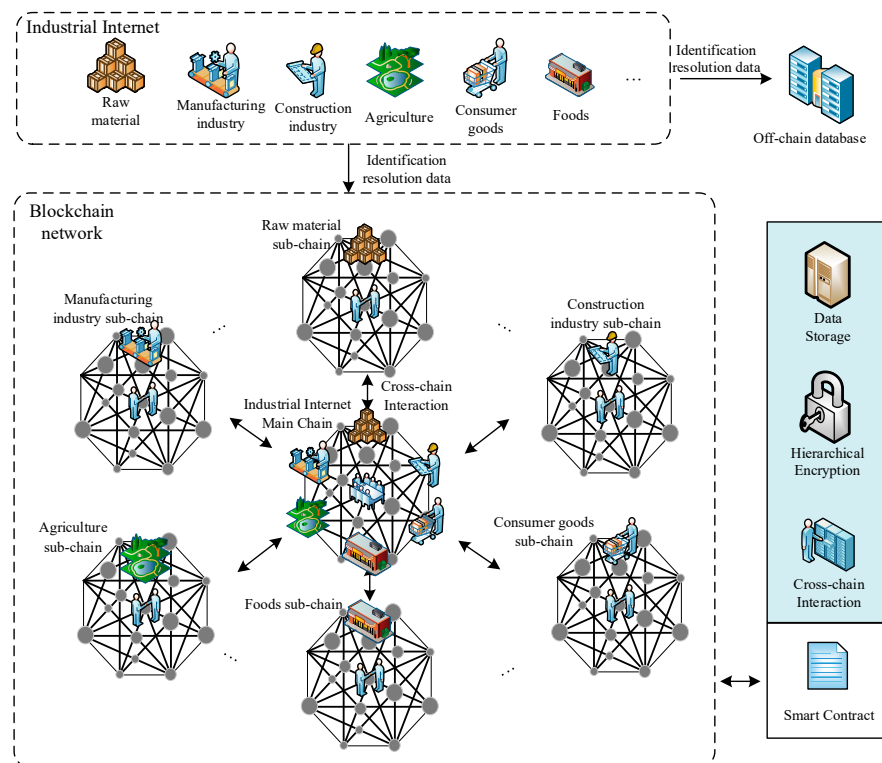


Figure 1. Trusted Management Model of Industrial Internet Identity Analysis Data Based on Blockchain.

With the continuous development of the industrial internet, identity analysis data has characteristics of rapid growth, large volume, wide variety, large collection range, multiple flow directions, wide transmission path, complex storage location, etc., and data security faces more complex and variable risks. Therefore, it is of great significance to ensure the security of industrial internet identity analysis data to maintain further development of the industrial internet.

3.2.1. Information Characteristics Analysis

Based on the information flow characteristics of relevant enterprises, life cycle links of the industrial internet identity analysis data can be abstracted into six typical links: data collection, data transmission, data storage, data processing, data exchange and sharing, and data archiving and deletion. Combined with actual business scenarios, the main identity analysis data are divided into R&D data domain, production data domain, operation and maintenance data domain, management data domain, external data domain and application service data domain, as shown in Table 2.

The R&D data domain mainly includes R&D design test data and development test data, etc.; the production data domain mainly includes control information, process parameters, and system logs during the production; the operation and maintenance data domain mainly includes operation and maintenance data related to the product life cycle, such as logistics and after-sales data, etc.; the management data domain mainly includes data related to equipment, customers, products and business; the external data domain mainly includes data shared with other entities; the application service data domain mainly includes equipment maintenance data, platform operation data, digital models and product information, etc.

Table 2. Classification of Industrial Internet Identity Analysis Data.

Data Domain	Content Included
R&D data domain	R&D design test data, development test data, etc.
Production data domain	Control information, working status, process parameters and system logs, etc.
Operation and maintenance data domain	Logistics and after-sales service data, etc.
Management data domain	System equipment asset information, customer and product information, product supply chain data, business statistics, etc.
External data domain	Data shared with other entities, etc.
Application service data domain	Equipment operation and maintenance data, knowledge mechanism, digital model, IoT collection data, platform application and service data, platform operation data, identity operation data, data product information, transaction information, etc.

3.2.2. Identity Analysis Data Classification

According to the requirements of policies and standards such as the “Guidelines for Classification and Grading of Industrial Data” and “Guidelines for the Grading of Network Security Level Protection”, industrial internet identity analysis data can be divided into three levels: first, second, and third level, among them the third-level data requires the highest security. The third-level data are core industrial data, which has the highest authority requirements. It is not allowed to be shared in principle. The scope of knowledge must be strictly controlled and even allowed to be shared. It will have a serious impact on the national economy, industry development, public interests, social order and even national security once leaked. Therefore, it must be capable of defending against large-scale malicious attacks from hostile national-level organizations. The second-level data are important industrial data, which is only open to authorized institutions and related personnel who really need to obtain this level of data, so it needs to be able to resist large-scale and strong malicious attacks. The first-level data are general industrial data, which has little impact on normal production and operation of industrial control systems and equipment, industrial internet platforms, etc. It also has little negative impact on enterprises, small direct economic losses with a small number of affected users and enterprises, a small range of production and living areas, short duration, and a small price required to restore industrial data or eliminate negative effects. Hence, it needs to be able to resist general attacks.

According to the above data level standards, the industrial internet identity data are classified as combined with actual application to achieve differentiated management and use of data information, which lays the foundation for the following research. Table 3 shows the industrial internet identity data classification.

Table 3. Authority Classification of Industrial Internet Identity Data.

Data Level	Data Domain	Data Content
Third level	R&D data domain	R&D design test data, development test data, etc.
Second level	Production data domain, operation and maintenance data domain, management data domain, application service data domain	Control information, working status, process parameters and system logs, logistics and after-sales service data, system device asset information, customer and product information, product supply chain data, business statistics data, device operation and maintenance data, knowledge mechanism, digital model, IoT collection data, platform application and service data, platform operation data, identity operation data, data product information, transaction information, etc.
First level	External data domain	Data shared with other entities, etc.

The R&D data domain possesses the core industrial data, which has the highest authority and security requirements; the production data domain, operation and maintenance data domain, management data domain, and application service data domain have important data in the industrial production, so they are defined as second-level data with

relatively high-security requirements; the external data domain mainly owns data shared with other entities, so it is defined as first-level general industrial data.

3.3. Hierarchical Encryption Mechanism Design

In the aforementioned research based on the trusted management model of blockchain-based industrial internet identity analysis data, each industrial internet slave chain stores the plain text of the identity analysis data within its respective industry, and the publicly traceable identity data are stored in the off-chain database. In order to achieve a collaborative consensus on the global identity analysis data of the industrial internet and to ensure the data privacy of each slave chain in each industry at the same time, a hierarchical encryption method is adopted to implement hierarchical encryption of the identity analysis data of the industrial internet. The identity analysis data classification encryption mechanism is shown in Figure 2.

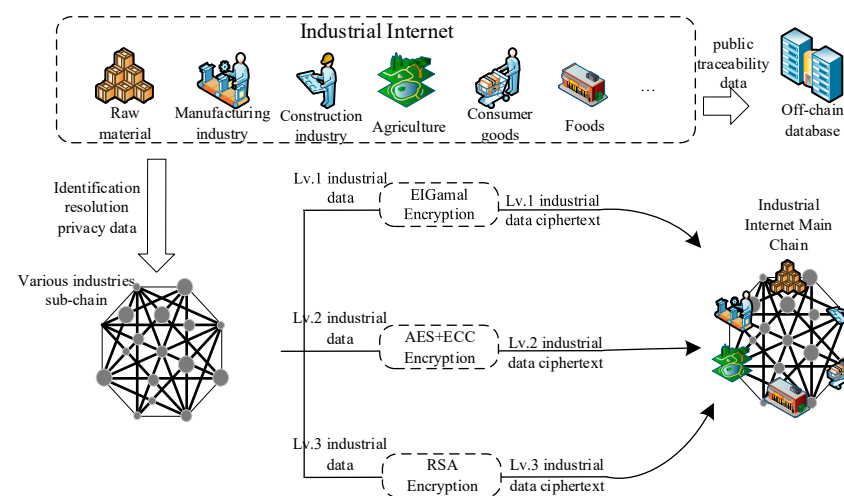


Figure 2. Classification Encryption Mechanism of Identity Analysis Data.

(1) The third-level industrial data are core data of the industrial internet, which has the highest requirements for data privacy and security with moderate data volume. Therefore, for the third-level industrial data, the RSA algorithm is chosen to encrypt the data plaintext.

First, the key required for encryption is generated by the system parameters, and two large prime numbers are randomly generated. $(n_3, \phi(n_3))$ is calculated according to Formulas (1) and (2). The positive integer e_3 is randomly selected. There exists $1 < e_3 < \phi(n_3)$, and the greatest common divisor of e_3 and $\phi(n_3)$ is 1. d_3 is calculated according to Formula (3).

$$n_3 = p_3 q_3 \quad (1)$$

$$\phi(n_3) = (p_3 - 1)(q_3 - 1) \quad (2)$$

$$d_3 = e_3^{-1} \bmod \phi(n_3) \quad (3)$$

By calculation, the public key is (n_3, e_3) , and the private key is (n_3, d_3) . The plain text of the third-level industrial data is encrypted by using the public key, and the private key is transmitted to the main chain of the industrial internet along with the cipher text of the third-level industrial data through cross-chain interaction and destroyed $(p_3, q_3, \phi(n_3))$. The encryption process is shown in Formula (4). The plaintext of the third-level industrial data is encrypted by using the public key (n_3, e_3) . The decryption process is shown in Formula (5); the plain text of the third-level industrial data is decrypted by using the private key (n_3, d_3) .

$$c_3 = E(m_3) = m^{e_3} \bmod n_3 \quad (4)$$

$$m_3 = D(c_3) = c_3^{d_3} \bmod n_3 \quad (5)$$

Since the generation parameters of the key pair are destroyed after the key pair is generated, the key cannot be decomposed. It is difficult to decompose large prime numbers, so the privacy and security of third-level industrial data are guaranteed.

(2) Second-level industrial data are important industrial data that cover a wide range, require relatively high data privacy and security, and have a large amount of data. Traditional asymmetric encryption methods cannot take into account both data security and encryption efficiency. In the face of redundant second-level industrial data, the AES symmetric encryption algorithm is first adopted to quickly encrypt the data. Secondly, in order to ensure the privacy and security of the data, the symmetric key is encrypted the second time through the ECC elliptic curve encryption. The specific process is as follows.

According to Formula (6), firstly, the AES algorithm is used to encrypt the plaintext of the second-level industrial data, where m_2 is the plain text of the second-level industrial data, k_A is the symmetric key for the encryption process and c_2 is the cipher text of the second-level industrial data.

$$c_2 = Enc_{AES}(m_2, k_A) \quad (6)$$

Set F_p as a finite field. p_2 is the characteristic of the field F_p , and p_2 is a prime number that cannot be factorized. E is an elliptic curve based on F_p , G is the base point of E , and n_2 is the order of F_p . A large prime number is selected randomly as the private key ($k_2 < n_2$) in the first-level main chain. The public key of the elliptic curve E is calculated by Formula (7). The first-level main chain sends (G, K_2) to the second-level slave chain through the cross-chain protocol. The second-level slave chain encodes k_A via BCH to point M on the elliptic curve. An integer r_2 less than an integer n_2 is randomly selected. The transmitted point M is encrypted by Formulas (8) and (9), and the second-level slave chain will send (C_1, C_2, c_2) to the first-level main chain.

$$K_2 = k_2 * G \quad (7)$$

$$C_1 = M + r_2 K_2 \quad (8)$$

$$C_2 = r_2 G \quad (9)$$

After the first-level main chain of the industrial internet receives (C_1, C_2, c_2) , the private key k_2 is used to decrypt M point, as shown in Formula (10). The symmetric key k_A is obtained by the decoding point M , and the cipher text of the second-level industrial data are decrypted to get the plain text by Formula (11).

$$C_1 - k_2 C_2 = M + r_2 K_2 - k_2(r_2 G) = M \quad (10)$$

$$m_2 = Dec_{AES}(c_2, k_A) \quad (11)$$

In data interaction, the second-level industrial data are transmitted through ciphertext, the symmetric key A is encoded on the elliptic curve for secondary encryption, and the ECC discrete logarithmic problem effectively guarantees the key security line so that the key cannot be cracked, thereby ensuring data security.

(3) The first-level industrial data are mainly industrial data shared with other entities with moderate data volume and moderate privacy and security requirements, so ElGamal homomorphic encryption is selected for plain text encryption. ElGamal is a public-key cryptosystem based on the discrete logarithm problem in finite fields. Since discrete logarithmic solving is difficult, the algorithm has relatively high security, which can effectively guarantee the security of shared industrial data.

In the key generation stage, set G_{Z_p} as a multiplicative group of finite fields Z_p , a large prime number p_1 is randomly generated, and the generating element g_1 is selected

$g_1 \in Z_p^*$. The private key $k_1 \in [1, p_1 - 1]$ is randomly selected. The public key is calculated by Formula (12), the public key (y_1, g_1, p_1) is publicized, and the private key k_1 is saved.

$$y_1 = g_1^{k_1} \bmod p_1 \quad (12)$$

In the encryption stage, the random number $r_1 \in [1, p_1 - 1]$ is selected from the second-level slave chain, and the first-level industrial data are encrypted by using the system parameters and the public key y_1 . The cipher text of the first-level industrial data is calculated by Formula (13).

$$c_1 = E(m_1) = (g_1^{r_1} \bmod p_1, m_1 y_1^{r_1} \bmod p_1) \quad (13)$$

In the decryption stage, after receiving the cipher text c_1 , the first-level main chain of the Industrial internet uses the private key k_1 to decrypt, and the plain text of the first-level industrial data are calculated by Formula (14).

$$m_1 = D(E(m_1)) = \frac{m_1 y_1^{r_1} \bmod p_1}{(g_1^{r_1} \bmod p_1)^{k_1}} \bmod p_1 \quad (14)$$

The encryption process of ElGamal algorithm is random, and the ciphertext is affected by both plaintext and the key, and $p_1 - 1$ possible ciphertext may be generated for the same key, thereby ensuring the privacy and security of the data.

3.4. “On-Chain + Off-Chain” Storage Model

If all data information is stored in the blockchain database, the storage cost will be greatly increased, and its efficiency and throughput will gradually decrease due to the increasing amount of data. In order to solve this problem, this study proposes an “on-chain + off-chain” dual-mode storage model. This is shown in Figure 3. Public traceable data with a large amount of data information is stored in an off-chain cloud database, and then the data are hashed and stored in the blockchain network in the form of hash values. If you need to query the data in the off-chain cloud database, the hash function is used to find the hash value uploaded to the blockchain network to ensure the security of the data information. The combination of storing industry confidential data in a blockchain network according to privacy degree and dual-mode storage model effectively reduces storage cost and improves operational efficiency.

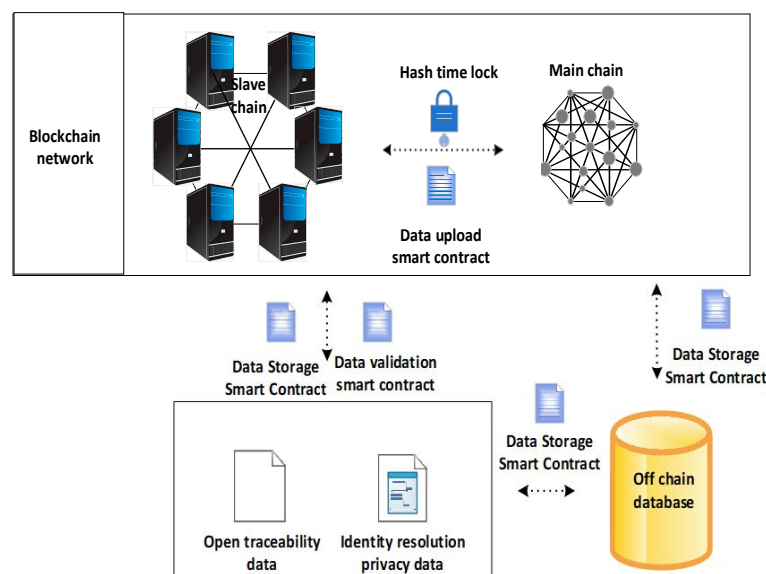


Figure 3. “On-chain + Off-chain” Storage Model.

4. Design of Main-Slave Multi-Chain Consensus Algorithm

In this section, a global collaborative consensus mechanism suitable for complex industrial internet applications is proposed by combining PBFT, hash locking, smart contracts, zero-knowledge proof and Kafka, the mechanism of which includes three stages—CI-PBFT consensus within the chain, cross-chain transmission protocol between the main chain and the slave chain, and KZKP main chain global consensus.

4.1. Design of Slave Chain Consensus Algorithm Based on CI-PBFT

In the actual application of the industrial internet, there are differences in various industry links, and the process is complex. In the case of a large number of nodes, the traditional consensus algorithm will seriously affect the efficiency of the slave chain consensus in the face of faults or malicious nodes. As a consensus algorithm that supports Byzantine fault tolerance, PBFT can accommodate the existence of faulty or malicious nodes under certain conditions, providing flexibility and security for the system, which is more suitable for complex and variable industrial internet applications. The algorithm process is shown in Figure 4.

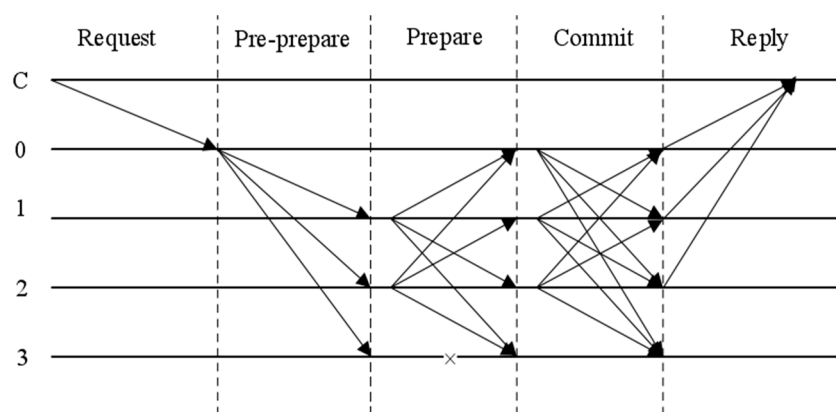


Figure 4. Consensus Process.

The process is as follows:

- (1) Client C sends a request to Master Node 0.
- (2) Master Node 0 assigns an integer value to the request and broadcasts a message containing that integer value to all other replica nodes.
- (3) Upon receiving the message, each replica node sends a broadcast message to all other nodes except itself.
- (4) All nodes broadcast throughout the entire network to acknowledge the assigned serial number of the master node.
- (5) Each node acknowledges the message and sends a reply to C.
- (6) Client C judges that the reply has been received and acknowledges the result.

To improve the trusted management of industrial internet identity analysis data and enhance the security and reliability of identity analysis data within the slave chain based on traditional PBFT, the CI (credible information degree) standard is added, and the CI-PBFT consensus algorithm is designed to solve the information security problem. If the information uploaded to the slave chain is malicious information, trusted information can be effective against criminals from malicious uploads, while the speed and success rate of information transmission is significantly reduced. m Byzantine nodes are set to participate in the CI-PBFT consensus algorithm, and the total number of nodes is N . All nodes are divided into consensus nodes CN (Consensus Node) and preset nodes PN (Preset Node) in a certain proportion. The consensus nodes participate in the consensus, while the preset nodes are used as a backup to save the consensus result without participating in the consensus. Before the CI-PBFT consensus starts, all nodes are ordinary nodes. If a node

wants to enter the consensus node group, it needs to submit an application and broadcast identity registration to the entire network. Upon approval, it will enter the consensus node group. Too many CN nodes will affect the entire consensus, while too few will affect the consensus results. Therefore, 70% of nodes are selected to form the CN cluster, and the remaining 30% are used as the PN cluster. When the CN node meets its set threshold, the rest of the ordinary nodes enter the PN cluster according to the order of joining the network. The CN node cluster is denoted as C_{CN} and the PN node cluster is denoted as C_{PN} , both of which should meet the requirements of Formula (15).

$$N = C_{CN} + C_{PN} \quad (15)$$

In the consensus, the initial score of all ordinary nodes is 0. In a certain round of consensus, when the consensus master node initiates consensus, and the consensus slave node is verified, the score of the master node increases by 1, and the score of all slave nodes increases by 1. When the consensus master node crashes or consensus fails due to a malicious node, the score of the master node that initiated the consensus request decreases by 2. When the score reaches a negative number, nodes will automatically exit the consensus and be replaced by preset nodes. The CI-PBFT consensus algorithm can effectively reduce the occurrence of malicious data uploaded by criminals, thereby ensuring the trusted ingestion of industrial data.

4.2. Design of Cross-Chain Transmission Protocol Based on Hash Lock and Smart Contract

For data interaction between the main chain and the slave chain, a cross-chain transmission protocol based on the combination of hash locking and smart contracts is designed. The schematic diagram of the transmission protocol is shown in Figure 5. It is assumed that data A on the main chain interacts with data B on the slave chain.

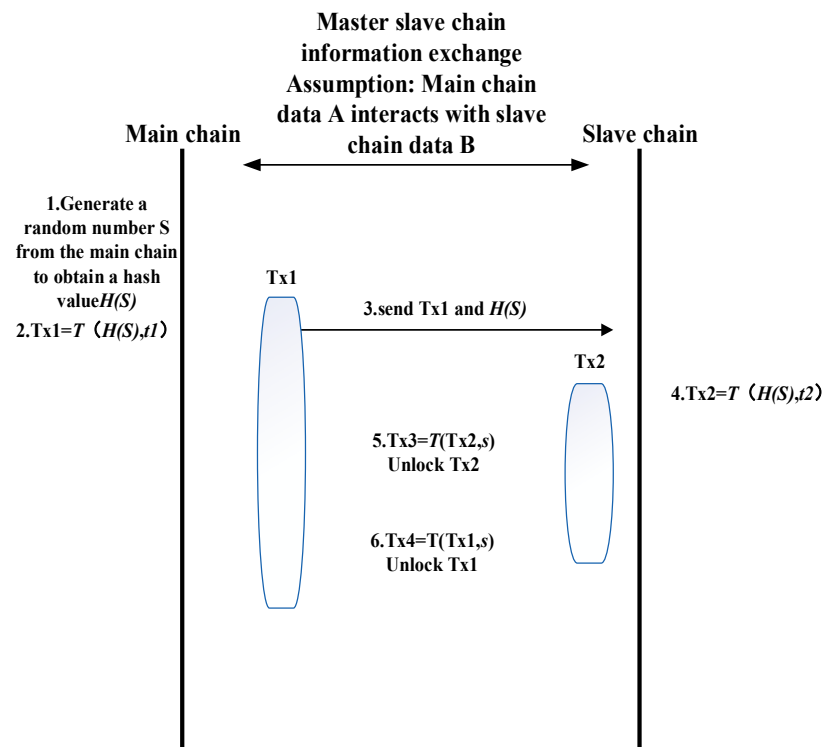


Figure 5. Schematic Diagram of the Transmission Protocol.

The specific process is as follows:

- (1) The main chain generates a random number s and calculates the hash value $H(s)$;

- (2) The main chain uses $H(s)$ and a time t_1 to generate a contract transaction $Tx_1 = T(H(s), t_1)$ on the main chain. Tx_1 will lock data A that the main chain needs to interact with, and the locking time is t_1 ;
- (3) The main chain sends the calculated $H(s)$ to the slave chain and sends transaction Tx_1 to the main chain, proving that data A has been locked;
- (4) The slave chain uses $H(s)$ and time t_2 to lock data B that needs to be interacted with and uplink the transaction to the chain, where the lock time is t_2 ($t_2 < t_1$);
- (5) The main chain uses s to construct Tx_3 to unlock the contract transaction Tx_2 on the slave chain and obtain data B locked by Tx_2 . At this time, the random number s is exposed;
- (6) The slave chain uses the public s to construct Tx_4 to unlock Tx_1 on the main chain and obtain data A locked by Tx_1 .

The cross-chain transmission protocol algorithm based on hash locking and smart contract is shown in Algorithm 1.

Algorithm 1: Cross-chain Transmission Protocol

Input: main chain data A

Output: slave chain data B

1: input A

2: $H(S) = H(\text{generate } S)$ (the main chain generates a random number S and obtains the hash value $H(s)$)

3: if time $\leq t_1$

4: locking A and send $H(S)$ send $H(S)$ to the slave chain

5: if time $\leq t_2$ ($t_2 < t_1$)

6: locking& Up chain B (lock the data B and uplink it to the chain)

6: obtain $B \rightarrow S$ (obtain slave chain data B through random number S)

7: return B

8: else

9: else

10: else return nonce

Algorithm 1 shows the way the main chain obtains data from the slave chain. If the slave chain needs to obtain data from the main chain, it only needs to unlock data A with the public random number S when the main chain obtains data B, which is not shown here.

4.3. Design of Main Chain Consensus Algorithm Based on Zero-Knowledge Proof and Kafka Cluster

In the aforementioned research, the industrial internet identity analysis data are successfully uplinked to the chain after the credible information degree consensus judgment, and then the hierarchically encrypted industrial data cipher text is transmitted to the industrial internet main chain through the cross-chain transmission protocol for global collaborative consensus. The main chain of the industrial internet involves different levels of industrial data cipher text in various industries. Once leaked, it will cause immeasurable losses.

Zero-knowledge proof is a cryptographic means to solve data confidentiality verification. The interactive zero-knowledge proof achieves the proof effect by completing several rounds of interaction between the two communicating parties. However, in the complex application of the industrial internet, frequent interactions among multiple nodes will cause serious network congestion or service denial. Therefore, the simple non-interactive zero-knowledge proof protocol Groth16 is selected to complete the zero-knowledge verification of the data. Concise, non-interactive zero-knowledge proof meets the application requirements of high throughput and high privacy of blockchain with lower communication and verification complexity. The partitioning feature of Kafka enables rapid orchestration of the verification evidence, and each node verifies the evidence generated by the remaining nodes in the corresponding partition, achieving a one-to-many complex verification process. And a Kafka-based zero-knowledge proof consensus algorithm KZKP (Kafka-based Zero-Knowledge Proof Consensus algorithm) is designed, as shown in Figure 6. KZKP consensus algorithm enables rapid orchestration of the zero-knowledge proof evidence through the Kafka cluster, and the evidence effectively reduces the amount of verification

of original information, which achieves secure collaborative authentication of data while ensuring data privacy.

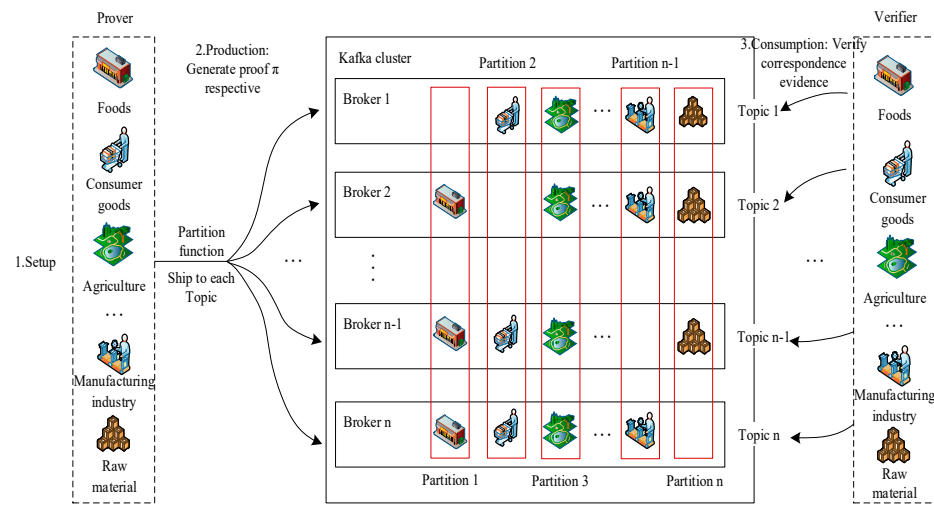


Figure 6. KZKP Consensus Process.

KZKP consensus consists of three stages: trusted initialization, generating evidence, and verifying evidence. The system parameters are first generated by a trusted third party. During the trusted initialization, the public input of the system needs to be introduced: the domain \mathbb{F} , arithmetic circuit $\mathbb{C} : \mathbb{F}^{|x|+|w|} \rightarrow \mathbb{F}^{|y|}$, where $(x, y) = (c_1, c_2, \dots, c_N)$, $|x| + |y| = N$; the secret input of the prover node: $w = (c_{N+1}, c_{N+2}, \dots, c_m)$, mark the set $I_{mid} = \{N+1, N+2, \dots, m\}$, there is $|w| = |I_{mid}|$.

(1) Trusted Initialization Process Setup

a. An arithmetic circuit \mathbb{C} on finite field \mathbb{F} is generated by a trusted third party. The QAP string is constructed according to the circuit \mathbb{C} , whose degree is d and size is m .

b. Corresponding parameters are created by a trusted third party. The generating group $\mathbb{G}_1, \mathbb{G}_2$ corresponds to the generator g, h , and the group of bilinear maps \mathbb{G}_T . The mapping e is defined as $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Mark $[a]_1$ as g^a , $[b]_2$ as h^b , $[c]_T$ as $e(g, h)^c$. $\alpha, \beta, \gamma, \delta, s \xleftarrow{\$} \mathbb{F}$ is randomly selected.

c. The public reference string $\sigma = ([\sigma_1]_1, [\sigma_2]_2)$ and the simulated trapdoor $\tau = (\alpha, \beta, \gamma, \delta, s)$ are generated by the trusted third-party module. $[\sigma_1]_1$ are elements on the elliptic curve \mathbb{G}_1 , and $[\sigma_2]_2$ are elements on the elliptic curve \mathbb{G}_2 . (σ_1, σ_2) is calculated by Formulas (16) and (17).

$$\sigma_1 = \left(\alpha, \beta, \delta, \{s^i\}_{i=0}^{d-1}, \left\{ \frac{\beta u_i(s) + \alpha w_i(s) + y_i(s)}{\gamma} \right\}_{i=0}^N, \left\{ \frac{\beta u_i(s) + \alpha w_i(s) + y_i(s)}{\delta} \right\}_{i=N+1}^m, \left\{ \frac{s^i t(s)}{\delta} \right\}_{i=0}^{d-2} \right) \quad (16)$$

$$\sigma_2 = \left(\beta, \gamma, \delta, \{s^i\}_{i=0}^{d-1} \right) \quad (17)$$

According to the formula, the common reference string σ is obtained, and the toxic wastes σ_1, σ_2 are destroyed in order to prevent them from being used by malicious attackers to generate forgeries and to avoid hidden dangers to system security.

(2) Prover Node P Generates Evidence Process

In the consensus of the first-level main chain of the industrial internet, the first-level nodes of each industry not only generate evidence as prover nodes but also serve as verifier nodes to verify evidence during the verification. Each prover node $P_j (j = 1, \dots, n)$ randomly selects $r_{1j}, r_{2j} \xleftarrow{\$} \mathbb{F} (j = 1, \dots, n)$, and calculates their respective evidences $(\pi_1, \pi_2, \dots, \pi_k, \dots, \pi_n)$ according to Formula (18), where the calculation formula (A_j, B_j, C_j)

is shown in (19)–(21). Each node calls the Producer API as a prover to send the specified Topic information, and the specified partition function sends the evidence generated by each node to different Broker proxy nodes with $n - 1$ pieces for each group. The partition function defines that each group of messages contains $n - 1$ pieces of n evidence except itself: Broker1 receives $(\pi_2, \dots, \pi_{n-1}, \pi_n)$, Broker2 receives $(\pi_1, \pi_3, \dots, \pi_n)$, and similarly, Broker $n - 1$ receives $(\pi_1, \dots, \pi_{n-2}, \pi_n)$, and Broker n receives $(\pi_1, \dots, \pi_{n-2}, \pi_{n-1})$. The cluster is vertically divided into n Partitions, and each partition contains $n - 1$ copies of proof evidence generated by the same node, which are distributed among different Brokers to achieve high parallel data processing for subsequent verification.

$$\pi_j = ([A_j]_1, [C_j]_1, [B_j]_2) \quad (18)$$

$$A_j = \alpha + \sum_{i=0}^m c_i u_i(s) + r_{1j} \delta \quad (19)$$

$$B_j = \beta + \sum_{i=0}^m c_i w_i(s) + r_{2j} \delta \quad (20)$$

$$C_j = \frac{\sum_{i=N+1}^m c_i (\beta u_i(s) + \alpha w_i(s) + y_i(s)) + h(s)t(s)}{\delta} + A_j r_{2j} + B_j r_{1j} - r_{1j} r_{2j} \delta \quad (21)$$

(3) Verifier Node V Verifies Evidence Process

After the partition function divides the evidence into partitions, all prover nodes P will change their identities to verifier nodes V , and the evidence π will be verified and checked by Formula (22). After the verification, the bit b_o will be output. If and only if the verifier passes the verification of the evidence π , $b_o = 1$ will be output, and $b_o = 0$ will be output if the verification fails.

$$e([A_j]_1, [B_j]_2) \stackrel{?}{=} e([a]_1, [\beta]_2) e\left(\sum_{i=0}^N c_i \left[\frac{\beta u_i(s) + \alpha w_i(s) + y_i(s)}{\gamma}\right]_1, [\gamma]_2\right) e([C_j]_1, [\delta]_2) \quad (22)$$

During the verification, after each prover node converts to a verifier node, each node pulls the verification evidence generated by the remaining nodes in the corresponding partition to determine whether the zero-knowledge proof formula is true and gives feedback on the verification result. The node that first completes the evidence verification in the corresponding partition will serve as the master node in this round of consensus. In order to avoid over-centralization of the system, each node cannot serve as the master node consecutively multiple times. When the replica of each partition is successfully verified by the corresponding node by more than 51%, it is deemed that the partition reaches a consensus within the partition and, at the same time, gives feedback to the master node and broadcasts to nodes that fail to verify. When all partitions complete the evidence verification, a round of consensus is reached.

5. Results and Analysis

5.1. Theoretical Analysis

5.1.1. Correctness Analysis

The research on trusted management of industrial internet identity analysis data based on blockchain mainly includes two parts: the design of trusted management architecture of industrial internet identity analysis data and the design of main-slave multi-chain consensus algorithms. This study first divides the industrial internet identity analysis data into different industrial grades according to the degree of privacy and security and adopts a hierarchical encryption method for different levels of industrial data according to the authority division so as to perform hierarchical management of private data with different authority levels. Secondly, the industrial internet multi-chain network architecture based on the main-slave multi-chain is designed. The business links of different industries form their

own slave chain for data autonomy and, at the same time, include a main chain to complete the global information collaborative certification of the industrial internet. The “on-chain + off-chain” dual-model storage mechanism can effectively bear the storage burden on the blockchain, thereby improving system efficiency. Finally, at the consensus level, a cross-industry main-slave multi-chain collaborative consensus mechanism is designed that is suitable for complex industrial internet applications. It includes a trusted information consensus within the chain CI-PBFT to ensure the trusted uplink process of the data. In terms of interaction between the main chain and the slave chain, a cross-chain interaction protocol based on hash locking is designed to ensure the trusted transmission of the data. When the encrypted industrial data are transmitted to the main chain, the KZKP consensus algorithm completes the collaborative consensus of the global encrypted data. The whole model guarantees the integrity and reliability of data information in identity analysis data uplink, cross-chain transmission and collaborative consensus, which is of great significance to trusted management of identity analysis data.

5.1.2. Security Analysis

In the network layer, industrial data of each industry is stored in a corresponding slave chain, separated from industrial data in other slave chains, which facilitates data autonomy in each industry chain. In the data layer, industrial data are hierarchically encrypted according to their privacy level and the amount. The industrial data interact in the form of ciphertext to ensure its security. Among them, the third-level industrial data adopts the RSA asymmetric encryption with the highest security. Since it is difficult to decompose large prime numbers, the privacy and security of the third-level industrial data are guaranteed. The second-level industrial data has a large amount. It is encrypted by AES symmetric encryption for fast encryption. ECC is used to re-encrypt the key that encrypts the data plaintext. The difficulty of solving the discrete logarithm effectively guarantees the security of the second-level industrial data and the key. The first-level industrial data adopts ELGamal homomorphic encryption. Its security is based on the difficulty of discrete logarithmic solving, which guarantees the security of industrial data. In data cross-chain transmission, the transmission protocol combined with the hash lock and smart contract adopted in this study can effectively guarantee the security of data information. The data must be transmitted within the specified time; otherwise, the information interaction will not be completed. At the same time, smart contracts are used for interactions to avoid artificial operations in the blockchain network. When the preset conditions are met, the data will automatically interact, which effectively reduces the possibility of criminals destroying data information during the transmission process. For the storage of data information, this study adopts the “on-chain + off-chain” storage model, which effectively improves storage efficiency. At the same time, the hash value of the off-chain data is stored in the blockchain network. When the data in the off-chain database needs to be called, the call must be responded to when the data matches the hash value in the blockchain network so as to ensure the security of the data information in the off-chain database. In the consensus layer, the CI-PBFT consensus mechanism based on trusted information is designed for the slave chain. Compared with the PBFT consensus, the consensus node and the preset node are classified by a ratio of 7:3. Once the blockchain network is tampered with or destroyed in the consensus, the points of the consensus node will be reduced until it withdraws from the consensus, and the preset nodes will take their place, so as to reduce destruction of the blockchain network by criminals and to effectively improve the security of the slave chain consensus. The main chain is designed with the KZKP consensus, which combines Kafka with zero-knowledge proof. Zero-knowledge proof selects the Groth16 protocol. Based on the unfalsifiable assumption, zero-knowledge proof ensures that the corresponding nodes on the main chain are the knowledge masters of industrial data in their respective industries, and the rest of the nodes are honest verifiers which will not disclose any relevant knowledge of industrial data cipher text during the proof. Relevant parameters in the consensus are destroyed immediately after generation, preventing illegal

and malicious personnel from obtaining relevant system parameters, which ensures the security of industrial data cross-industry global collaborative consensus.

5.1.3. Scalability Analysis

This blockchain-based research on trusted management of industrial internet identity analysis data is widely applicable in manufacturing, light industry, food industry, agriculture, consumer goods and other fields involved in the industrial internet. Different industries can set their corresponding nodes according to their characteristics to generate the slave chain for data autonomy. On the main chain, corresponding industry nodes are also generated to participate in the global collaborative consensus. The KZKP consensus algorithm on the main chain can effectively guarantee the privacy and security of identity analysis data in various industries, and the introduced message processing mechanism can also effectively deal with large-scale data verification.

5.2. Prototype System Verification

5.2.1. System Architecture Design

Combined with the actual application of various industries of the industrial internet, based on the trusted management model of the industrial internet identity analysis data, the system architecture of trusted management of the industrial internet identity analysis data is constructed. The designed overall system architecture is shown in Figure 7, which mainly includes five layers: application layer, acquisition layer, data layer, contract layer and consensus layer.

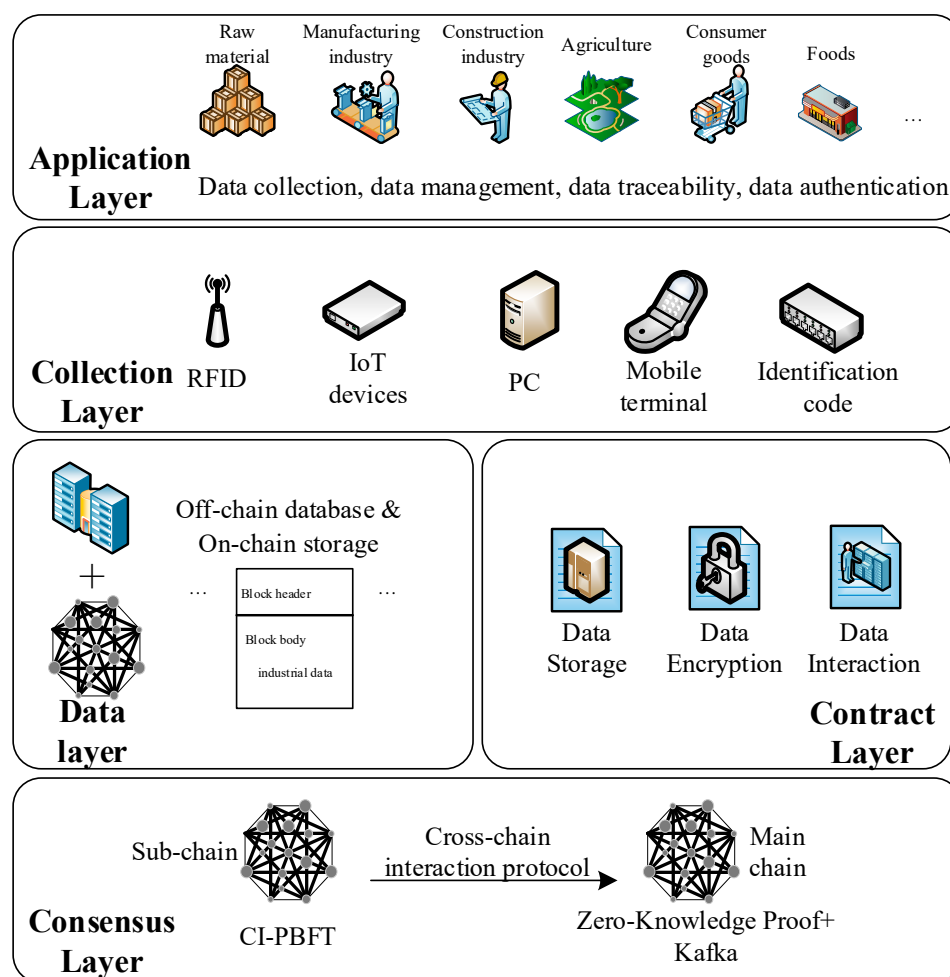


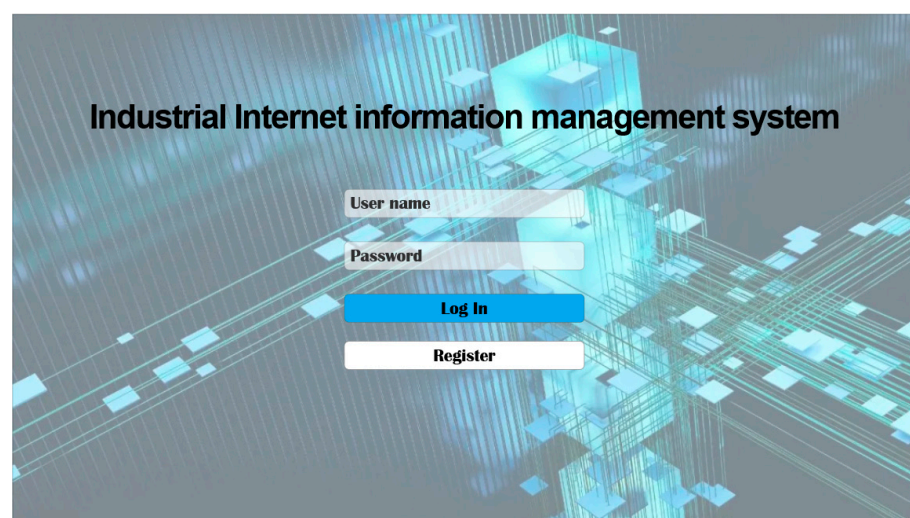
Figure 7. System Architecture Diagram.

The application layer provides management services of industrial internet identity analysis data for raw materials, manufacturing, construction, consumer goods, food, agriculture and other industries through a visual interface. The data collection layer consists of RFID devices, IoT devices, identity codes, PC terminals and mobile terminals. The data layer is composed of a blockchain main-slave multi-chain storage network and an off-chain database; by establishing a distributed ledger and an off-chain database to store data, the data interaction among multiple chains adopts hash locking and smart contracts. In this way, the data cannot be easily tampered with so as to improve data security. The contract layer is mainly achieved through codes and is mainly composed of smart contracts for data storage and data verification. When the execution conditions are met, it is automatically executed, which can effectively improve the overall efficiency of the model. The consensus layer consists of main chain consensus based on zero-knowledge proof and Kafka cluster, slave chain CI-PBFT consensus and hash time lock.

5.2.2. Prototype System Realization

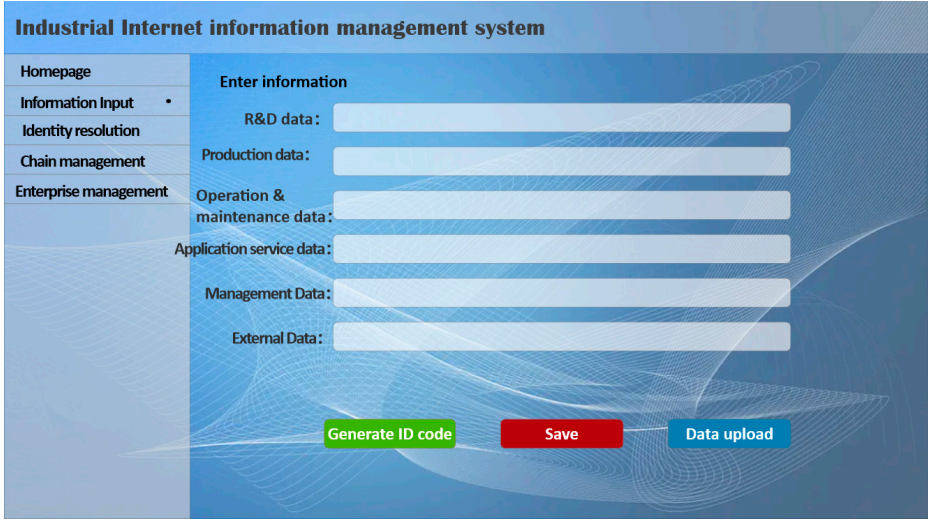
This paper implements a prototype system based on trusted management research of industrial internet identity analysis data of the blockchain, with the development environment of Ubuntu version 20.04.1 and Linux version 16.0.0. The Docker version is 20.10.7. The super book Fabric 2.1 is adopted as the open-source framework. The go language version is 1.17.2. Six slave chains are set, namely slave chains of six industries of raw materials, manufacturing, construction, consumer goods, food, and agriculture. In addition, a main chain responsible for the global consensus work of the industrial internet is also set. Consumers can query off-chain traceability information, and enterprises can make private data access, encrypted interaction and other functions through the prototype system. The specific implementation interface is shown in Figure 8.

Figure 8a shows the system platform login interface. After the enterprise logs in to the system, the operation interface is shown in Figure 8b. Corresponding industrial data can be input according to different data domains. The identity analysis interface is shown in Figure 8c. Data that have been input and generated an identity code can be decoded by the decoding tool of the system platform to obtain the specific content corresponding to the identity code, and the corresponding file certificate can be viewed. Enterprises can manage their slave chains within the chain through the platform, including the dynamic management of nodes, organizations, certificates, etc., as shown in Figure 8d.



(a) Platform Login Interface

Figure 8. Cont.



Industrial Internet information management system

Homepage
Information Input •
Identity resolution
Chain management
Enterprise management

Enter information

R&D data:

Production data:

Operation & maintenance data:

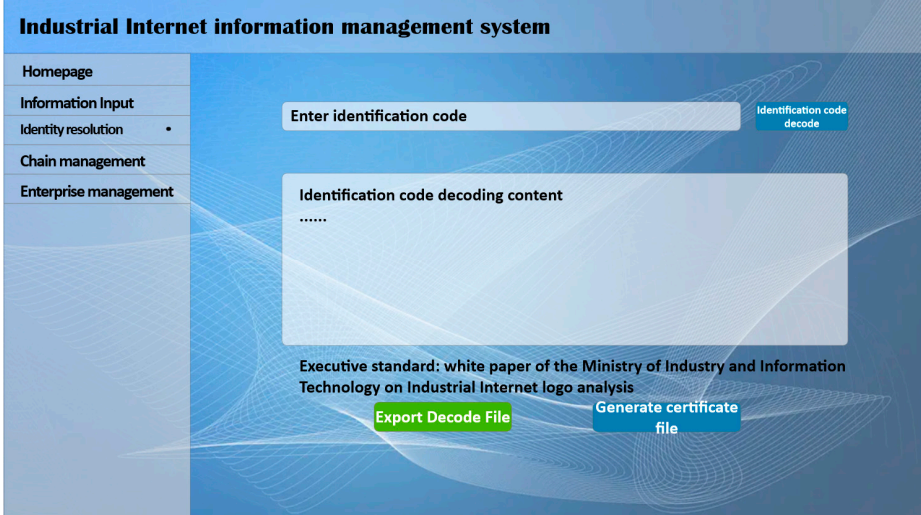
Application service data:

Management Data:

External Data:

Generate ID code Save Data upload

(b) Information Input Interface



Industrial Internet information management system

Homepage
Information Input
Identity resolution •
Chain management
Enterprise management

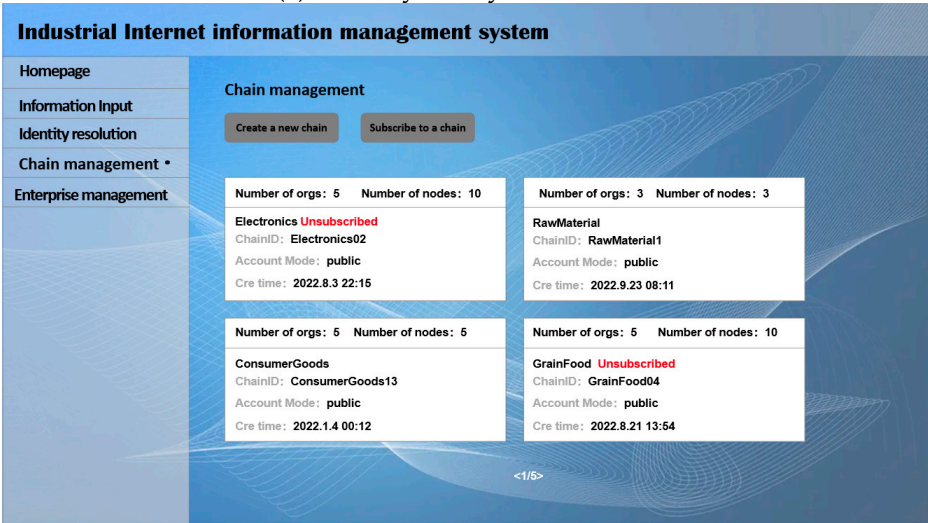
Enter identification code Identification code decode

Identification code decoding content
.....

Executive standard: white paper of the Ministry of Industry and Information Technology on Industrial Internet logo analysis

Export Decode File Generate certificate file

(c) Identity Analysis Interface



Industrial Internet information management system

Homepage
Information Input
Identity resolution
Chain management •
Enterprise management

Chain management

Create a new chain Subscribe to a chain

Number of orgs: 5 Number of nodes: 10 Electronics Unsubscribed ChainID: Electronics02 Account Mode: public Cre time: 2022.8.3 22:15	Number of orgs: 3 Number of nodes: 3 RawMaterial ChainID: RawMaterial1 Account Mode: public Cre time: 2022.9.23 08:11
Number of orgs: 5 Number of nodes: 5 ConsumerGoods ChainID: ConsumerGoods13 Account Mode: public Cre time: 2022.1.4 00:12	Number of orgs: 5 Number of nodes: 10 GrainFood Unsubscribed ChainID: GrainFood04 Account Mode: public Cre time: 2022.8.21 13:54

<1/5>

(d) Chain Management Interface

Figure 8. Trusted Management System of Industrial Internet Identity Analysis Data.

In order to verify the efficiency, security, scalability and other indicators of the model proposed by our institute, we collaborated with an industry company in Beijing to obtain

data for the first quarter of 2023 to verify its security, transaction throughput, and ciphertext query time. During the verification process, we selected 9750 pieces of data from the company for security authentication in the first quarter. The results in Figure 9 shows that in the experiment, there were only four pieces of unsafe data due to missing data and incomplete records, which verifies the safety of the model proposed in this study.

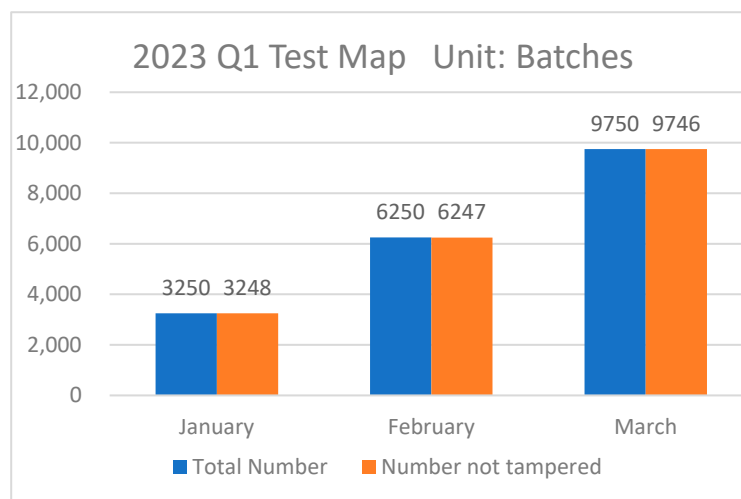


Figure 9. Data Security Test Diagram.

Meanwhile, to verify the efficiency of the model, this study tested the transaction throughput, which refers to the number of transactions completed per unit time. This study conducted experimental verification on the main-slave multi chain model using PBFT, CI-PBFT consensus. In the experiment, 500 requests were sent to the client, recording the number of transactions that can be completed per second, and different node numbers were used for testing. As the number of nodes increases, the throughput of both consensus shows a downward trend. However, the main-slave multi-chain model using CI-PBFT consensus has higher throughput, as shown in Figure 10. In addition, query efficiency of the second-level as well as the third-level industrial data in the industrial internet blockchain network was tested. In order to ensure the authenticity and reliability of the experimental data, the test results were adopted as the average value of the results of 50 executions. As shown in Figure 11, the average query time of the third-level industrial data is 0.8582 s, and the average query time of the second-level industrial data is 0.4193 s. This test result is also similar to the computational resources consumed by the corresponding encryption and decryption algorithms of the two kinds of industrial data, and the present model has a good querying efficiency of the data, which is able to meet the querying requirements of industrial data.

5.3. Comparative Analysis of Consensus Performance

This study conducted a performance comparison analysis on PoW, PoS, Raft, PBFT, CI-PBFT and KZKP proposed by this model in terms of four aspects: decentralization, security, consensus efficiency, and scalability. The analysis results are shown in Table 4. Compare the degree of decentralization based on the number of consensus nodes participating in the blockchain network, how to select the main node and the weight of consensus nodes. The weight of consensus nodes means the possibility of each consensus node being elected as the main node during the consensus. In the consensus, the more nodes participate, the more dispersed rights each node receives, and the more dispersed the system becomes. Security analysis includes supply cost, diversity of attacks, and fault tolerance. Fault tolerance refers to the percentage of malicious nodes that can be tolerated by the entire consensus, provided that the consensus is completed. Consensus efficiency consists of two indicators: transaction throughput and transaction latency. Transaction throughput

refers to the total number of transactions processed per unit time, and transaction delay refers to the total time required for a block to generate and complete consensus. Scalability includes two indicators: resource consumption and communication complexity. Resource consumption refers to the degree of consumption of network resources, such as computing power and storage, by nodes during the consensus. Consensus algorithm with higher resource consumption requires higher network performance.

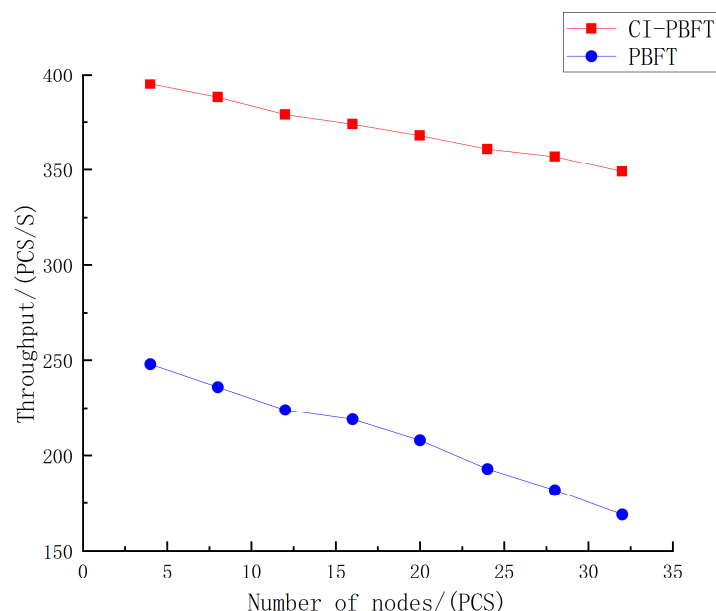


Figure 10. Transaction Throughput Test.

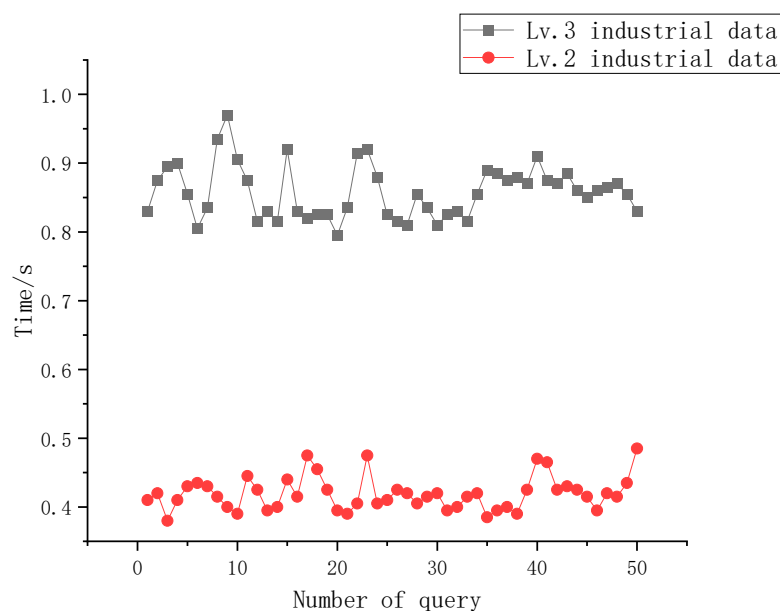


Figure 11. Query efficiency.

In terms of decentralization, in the slave chain CI-PBFT consensus, all common node points in the initial state are 0. In a certain round of consensus, when the consensus master node initiates the consensus and the consensus slave node passes the verification, the score of the master node increases by one and the score of all slave nodes increases by one. When the consensus master node is down or the consensus fails due to some malicious nodes, the score of the master node that initiates the consensus request decreases by 2. So, in each

round of consensus, the master node will be changed according to the success rate of the verification so as to change the master node to improve the capability of decentralization. The main chain is based on KZKP consensus. The node that first completes the evidence verification in the corresponding partition serves as the master node of the consensus round, and it cannot serve as the master node consecutively to avoid centralization. In terms of security, it is costly and difficult to launch an attack on PoW and PoS competition consensus based on the public chain. The Raft consensus only supports fault-tolerant nodes but cannot support malicious nodes in the network, so it is unable to resist Byzantine node attacks. CI-PBFT consensus is based on PBFT consensus. It can tolerate the existence of faulty nodes and malicious nodes under certain conditions, providing security or flexibility for the system. It also adds trusted information to participate in the consensus. When points decrease to negative, the nodes will automatically exit the consensus and the preset nodes will take the place. This algorithm can greatly increase the cost of criminals attacking the blockchain, which effectively improves the security of the consensus. The security of KZKP consensus is based on public reference strings. The strings will be destroyed once corresponding parameters are generated, which effectively avoid perjury generated from strings by malicious nodes. Moreover, it is costly and difficult to attack zero-knowledge proof evidence, effectively ensuring the security of industrial data consensus. In terms of consensus efficiency, the consensus of traditional public chains and consortium chains is not suitable for huge industrial data applications because their special block structure lowers the block generation efficiency. CI-PBFT consensus classifies all its nodes into preset nodes and consensus nodes. When points decrease to negative, the nodes will automatically exit the consensus and be supplemented by preset nodes, which can ensure the high efficiency of transaction throughput. At the same time, although KZKP needs to go through the evidence phase corresponding to the initialization and generation of data, it can effectively meet the application requirements of multi-party interactive verification in the industrial internet through the high parallel processing characteristics of the Kafka cluster. In terms of scalability, the resource consumption of PoW and PoS consensus is large, which limits the performance of nodes. CI-PBFT consensus, based on PBFT adding the evaluation standard of trusted information, does not increase its resource consumption, and its communication complexity can basically meet the application of this study. KZKP consumes relatively large network computing resources in zero-knowledge verification, but the communication complexity meets the requirements of the application due to the partitioning characteristics of Kafka.

Table 4. Comparison and Analysis of Consensus Performance.

Performance Indicator		PoW	PoS	Raft	PBFT	CI-PBFT	KZKP
Decentralization	No. Consensus node	whole network	whole network	whole network	whole network	whole network	whole network
	Selection method of master node	compete	compete	select	select	compete	compete
	Weight of consensus node	not equal	not equal	not equal	not equal	not equal	not equal
Security	Fault tolerance rate	<50%	<50%		<1/3	<1/3	<50%
	Attack variety	high	high	low	medium	medium	high
	Attack cost	high	high	low	medium	high	high
Consensus Efficiency	Transaction throughput	low	low	high	medium	high	medium
	Transaction delay	high	high	low	medium	medium	medium
Scalability	Resource consumption	high	medium	low	low	low	high
	Communication complexity	O(N)	O(N)	O(N)	O(N ²)	O(N ²)	O(N)

At present, the management of industrial internet data has been studied by many scholars, but traditional technologies can no longer solve the problems of low efficiency

and poor sharing caused by the wide variety of industrial internet data and complex participation links. Although blockchain technology can solve some of the problems, the transaction throughput, delay and other problems of single-chain architecture are becoming increasingly prominent; therefore the application of multi-chain architecture to the industrial internet data trusted management industry is not yet mature. In order to demonstrate the advantages of the model proposed in this study, a comparative analysis is conducted between this study and existing literature, as shown in Table 5.

Table 5. Comparative Analysis of Models.

Performance	Indicators	Literature [15]	Literature [19]	Research in This Paper
Security	Data Security	Medium	High	High
	Vulnerability	High	Medium	Low
Model Efficiency	Timeliness	Low	Medium	High
	Throughput	Medium	High	High
	Delay	High	Medium	Low
Scalability	Resource consumption	Medium	Relatively Low	Low

6. Summary and Outlook

In view of inconsistent industrial links of the industrial internet, complex identity analysis data, and difficulty in defining privacy authority, etc., this research first classifies the identity analysis data of the industrial internet according to industrial data classification and security level protection. Secondly, this paper constructs a blockchain-based trusted management model of industrial internet identity analysis data, which realizes the separation of industrial data among various industries through the main-slave multi-chain design. Then, a hierarchical encryption method is designed for the classification of industrial data privacy authority to ensure the privacy and security of industrial data transmission; meanwhile, in order to improve system efficiency, a dual-model storage mechanism of blockchain + off-chain database is adopted, which effectively reduces the blockchain storage burden. Fourthly, a main-slave multi-chain consensus mechanism suitable for the industrial internet is designed, which includes three processes: slave chain consensus, cross-chain protocol and main chain consensus. The slave chain is based on the trusted information consensus CI-PBFT, which greatly reduces the possibility of uploading malicious data in various industries. In terms of the cross-chain interaction between the slave chain and the main chain, a cross-chain interaction protocol based on hash locking is designed to realize the trusted interaction of data. On the main chain, the KZKP consensus algorithm is designed with the combination of Kafka and zero-knowledge proof. While improving verification efficiency, it can realize zero-knowledge verification of industrial data in different industries and effectively protect the privacy and security of industrial data. Finally, the correctness, security and scalability of the trusted management model are theoretically analyzed, and a prototype system is developed and realized. The analysis and verification results show that this research can be well applied to the research of related fields of the industrial internet and has great significance for fields involved in the industrial internet. In the meantime, this study ensures the security and trusted management of industrial data while ensuring data privacy in uplink and verification of industrial internet identity analysis data information.

However, although this research proposes a model that can effectively ensure the security and trusted management of industrial internet data information, it does not involve whether the data source is credible, which is also an obstacle to the current blockchain project—the last mile development. In the future, how to achieve trusted collection and transmission of industrial internet data sources and how to achieve full-process and holographic security and trusted management of data information will continue to be explored. On the other hand, this research aims to construct a main-slave multi-chain-based industrial

internet identity analysis data information management method in the industrial internet. However, at the current stage, it is relatively difficult to completely achieve the main-slave multi-chain model and a multi-chain collaborative consensus mechanism in the Fabric network. Therefore, in the analysis, the prototype system and relevant theoretical methods need to be achieved in a streamlined way. But it turns out that this study has certain limitations through streamlined feedback and verification. In this way, the proposed theoretical model is fully verified and supported through theoretical analysis and experimental simulation in this study. In addition, algorithm complexity of the cryptographic algorithm for hierarchical encryption of industrial data is at the polynomial level, so the encryption algorithm is less affected with the growth of encrypted text. However, compared with the encryption and decryption stage, the generation of the parameter of the encryption algorithm requires a relatively long time. But once the key is generated, it can be applied to subsequent data encryption and decryption. For the main-slave multi-chain collaborative consensus algorithm proposed in this study, the slave chain consensus enhances the credibility of the model to a certain extent. But as the number of nodes in the network gradually increases, the consensus efficiency becomes low correspondingly. For the main chain consensus, during the parameter generation of zero-knowledge proof, the time consumption reaches the second level. Once the system parameters are generated, they can be applied to subsequent verification, and zero-knowledge proof evidence also effectively reduces the amount of verification of the original information of the data. This paper is mainly a preliminary exploration of blockchain multi-chain technology and collaborative consensus in the field of the industrial internet. In future research, detailed network models and consensus algorithms will be further implemented, and the integrity test of consensus algorithm will be strengthened.

Author Contributions: Conceptualization, Z.Q. and T.H.; methodology, B.Z. and Y.L.; software, X.Z.; validation, Z.Q. B.Z. and Y.L.; formal analysis, X.Z.; investigation, T.H.; resources, Z.Q.; data curation, T.H.; writing—original draft preparation, B.Z. and Y.L.; writing—review and editing, Z.Q. and X.Z.; visualization, T.H.; supervision, X.Z.; project administration, Z.Q.; funding acquisition, Z.Q. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (No. 92267301), and partially supported by the Open Project Program of Key Laboratory of Industrial Internet and Big Data, China National Light Industry, Beijing Technology and Business University.

Data Availability Statement: Data available on request due to restrictions eg privacy or ethical. The data presented in this study are available on request from the corresponding author. The data are not publicly available due to data protection protocol for authorized projects.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Li, J.-Q.; Yu, F.R.; Deng, G.; Luo, C.; Ming, Z.; Yan, Q. Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 1504–1526. [\[CrossRef\]](#)
2. Xiao, Y.; Pei, E.; Wang, K.; Zhou, W.; Xiao, Y. Design and Research of M2M Message Transfer Mechanism of Looms for Information Transmission. *IEEE Access* **2022**, *10*, 76136–76152. [\[CrossRef\]](#)
3. Robison, P.; Sengupta, M.; Rauch, D. Intelligent Energy Industrial Systems 4.0. *IT Prof.* **2015**, *17*, 17–24. [\[CrossRef\]](#)
4. Zhao, J.; Wu, D. The risk assessment on the security of industrial internet infrastructure under intelligent convergence with the case of G.E.'s intellectual transformation. *Math. Biosci. Eng.* **2022**, *19*, 2896–2912. [\[CrossRef\]](#) [\[PubMed\]](#)
5. Wang, L.; Ye, Z.; Zhang, R.; Lin, J.; Chen, F.; Tang, F. The Growth Model of Industrial Internet Platform in Industrial 4.0. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5145641. [\[CrossRef\]](#)
6. Dou, K.; Li, J.; Zhou, Y. Research on Design and Monitoring of a Development Index of an Industrial internet Platform Based on a Fixed-Base Index Method. *Electronics* **2022**, *11*, 274. [\[CrossRef\]](#)
7. Jung, M.; Min, B.-W. A highly selective UWB bandpass filter using stepped impedance stubs. *Int. J. Microw. Wirel. Technol.* **2018**, *10*, 301–307. [\[CrossRef\]](#)
8. Zikria, Y.B.; Kim, S.W.; Afzal, M.K.; Wang, H.; Rehmani, M.H. 5G Mobile Services and Scenarios: Challenges and Solutions. *Sustainability* **2018**, *10*, 3626. [\[CrossRef\]](#)

9. Wang, L.; He, Y.; Wu, Z. Design of a Blockchain-Enabled Traceability System Framework for Food Supply Chains. *Foods* **2022**, *11*, 744. [\[CrossRef\]](#)
10. Lee, S.B.; Park, A.; Song, J. Blockchain Technology and Application. *J. Korea Soc. Comput. Inf.* **2021**, *26*, 89–97. [\[CrossRef\]](#)
11. Wei, Q.; Li, B.; Chang, W.; Jia, Z.; Shen, Z.; Shao, Z. A Survey of Blockchain Data Management Systems. *ACM Trans. Embed. Comput. Syst. (TECS)* **2021**, *21*, 1–28. [\[CrossRef\]](#)
12. Li, X.; Russell, P.; Mladin, C.; Wang, C. Blockchain-Enabled Applications in Next-Generation Wireless Systems: Challenges and Opportunities. *IEEE Wirel. Commun.* **2021**, *28*, 86–95. [\[CrossRef\]](#)
13. Guo, H.; Yu, X. A Survey on Blockchain Technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [\[CrossRef\]](#)
14. Jeong, Y.-S. Secure IIoT Information Reinforcement Model Based on IIoT Information Platform Using Blockchain. *Sensors* **2022**, *22*, 4645. [\[CrossRef\]](#)
15. Yu, Q.; Guan, X.; Zhai, Y.; Meng, Z. The missing data filling method of the industrial internet platform based on rules and lightGBM. *IFAC-PapersOnLine* **2020**, *53*, 152–157. [\[CrossRef\]](#)
16. Kushch, S.; Baryshev, Y.; Ranise, S. Blockchain Tree as Solution for Distributed Storage of Personal ID Data and Document Access Control. *Sensors* **2020**, *20*, 3621. [\[CrossRef\]](#) [\[PubMed\]](#)
17. Ding, Y.; Yang, L.; Shi, W.; Duan, X. The Digital Copyright Management System Based on Blockchain. In Proceedings of the 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 16–18 August 2019; pp. 63–68. [\[CrossRef\]](#)
18. Wang, J.; Zhang, X.; Xu, J.; Wang, X.; Li, H.; Zhao, Z.; Kong, J. Blockchain-Based Information Supervision Model for Rice Supply Chains. *Comput. Intell. Neurosci.* **2022**, *2022*, 2914571. [\[CrossRef\]](#)
19. Xu, J.; Han, J.; Qi, Z.; Jiang, Z.; Xu, K.; Zheng, M.; Zhang, X. A Reliable Traceability Model for Grain and Oil Quality Safety Based on Blockchain and Industrial internet. *Sustainability* **2022**, *14*, 15144. [\[CrossRef\]](#)
20. Peng, X.; Zhang, X.; Wang, X.; Li, H.; Xu, J.; Zhao, Z. Multi-Chain Collaboration-Based Information Management and Control for the Rice Supply Chain. *Agriculture* **2022**, *12*, 689. [\[CrossRef\]](#)
21. Zhu, K.; Chen, W.; Jiao, L.; Wang, J.; Peng, Y.; Zhang, L. Online training data acquisition for federated learning in cloud–edge networks. *Comput. Netw.* **2023**, *223*, 109556. [\[CrossRef\]](#)
22. Wang, P.; Wu, X.; He, X. Vibration-Theoretic Approach to Vulnerability Analysis of Nonlinear Vehicle Platoons. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 11334–11344. [\[CrossRef\]](#)
23. Misra, S.; Roy, C.; Sauter, T.; Mukherjee, A.; Maiti, J. Industrial internet of Things for Safety Management Applications: A Survey. *IEEE Access* **2022**, *10*, 83415–83439. [\[CrossRef\]](#)
24. Gebremichael, T.; Ledwaba, L.P.I.; Eldefrawy, M.H.; Hancke, G.P.; Pereira, N.; Gidlund, M.; Akerberg, J. Security and Privacy in the Industrial internet of Things: Current Standards and Future Challenges. *IEEE Access* **2020**, *8*, 152351–152366. [\[CrossRef\]](#)
25. Al-Rakhami, M.S.; Al-Mashari, M. ProChain: Provenance-Aware Traceability Framework for IoT-Based Supply Chain Systems. *IEEE Access* **2022**, *10*, 3631–3642. [\[CrossRef\]](#)
26. Boudagdigue, C.; Benslimane, A.; Kobbane, A.; Liu, J. Trust Management in Industrial internet of Things. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3667–3682. [\[CrossRef\]](#)
27. Saqlain, M.; Piao, M.; Shim, Y.; Lee, J.Y. Framework of an IoT-based Industrial Data Management for Smart Manufacturing. *J. Sens. Actuator Netw.* **2019**, *8*, 25. [\[CrossRef\]](#)
28. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf. Process. Manag.* **2021**, *58*, 102535. [\[CrossRef\]](#)
29. Jiang, T.G.; Fang, H.; Wang, H.G. Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis. *IEEE Internet Things J.* **2019**, *6*, 4640–4649. [\[CrossRef\]](#)
30. Ma, Z.; Wang, X.; Jain, D.K.; Khan, H.; Gao, H.; Wang, Z. A Blockchain-Based Trusted Data Management Scheme in Edge Computing. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2013–2021.
31. Li, W.; Guo, H.; Nejad, M.; Shen, C.C. Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. *IEEE Access* **2020**, *8*, 181733–181743. [\[CrossRef\]](#)
32. Chen, J.; Lv, Z.H.; Song, H.B. Design of personnel big data management system based on blockchain. *Future Gener. Comput. Syst.-Int. J. Esci.* **2019**, *101*, 1122–1129. [\[CrossRef\]](#)
33. Song, L.; Wang, X.; Wei, P.; Lu, Z.; Wang, X.; Merveille, N. Blockchain-Based Flexible Double-Chain Architecture and Performance Optimization for Better Sustainability in Agriculture. *CMC-Comput. Mater. Contin.* **2021**, *68*, 1429–1446. [\[CrossRef\]](#)
34. Okegbile, S.D.; Cai, J.; Alfa, A.S. Performance Analysis of Blockchain-Enabled Data-Sharing Scheme in Cloud-Edge Computing-Based IoT Networks. *IEEE Internet Things J.* **2022**, *9*, 21520–21536. [\[CrossRef\]](#)
35. Okegbile, S.D.; Cai, J.; Alfa, A.S. Practical Byzantine fault tolerance-enhanced blockchain-enabled data sharing system: Latency and age of data package analysis. *IEEE Trans. Mob. Comput.* **2022**, 1–17. [\[CrossRef\]](#)
36. Zhang, C.; Ni, Z.; Xu, Y.; Luo, E.; Chen, L.; Zhang, Y. A trustworthy industrial data management scheme based on redactable blockchain. *J. Parallel Distrib. Comput.* **2021**, *152*, 167–176. [\[CrossRef\]](#)
37. Tao, F.; Zhang, Y.; Cheng, Y.; Ren, J.; Wang, D.; Qi, Q.; Li, P. Digital twin and blockchain enhanced smart manufacturing service collaboration and management. *J. Manuf. Syst.* **2022**, *62*, 903–914. [\[CrossRef\]](#)
38. Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K.C. A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3582–3592. [\[CrossRef\]](#)

39. Ceccarelli, A.; Cinque, M.; Esposito, C.; Foschini, L.; Giannelli, C.; Lollini, P. FUSION-Fog Computing and Blockchain for Trusted Industrial internet of Things. *IEEE Trans. Eng. Manag.* **2022**, *69*, 2944–2958. [[CrossRef](#)]
40. Huo, R.; Zeng, S.; Di, Y.; Cheng, X.; Huang, T.; Yu, F.R.; Liu, Y. A Blockchain-Enabled Trusted Identifier Co-Governance Architecture for the Industrial internet of Things. *IEEE Commun. Mag.* **2022**, *60*, 66–72. [[CrossRef](#)]
41. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT. *J. Parallel Distrib. Comput.* **2021**, *156*, 176–184. [[CrossRef](#)]
42. Li, Y.; Cheng, Q.; Shi, W. Security Analysis of a Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for IIoT Environments. *Secur. Commun. Netw.* **2021**, *2021*, 5573886. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.