DOI: 10.23977/jeis.2024.090219
ISSN 2371-9524 Vol. 9 Num. 2

Application of Blockchain Technology in Data Security and Privacy Protection

Xiuni Li

Xi'an Kedagaoxin University, Xian, Shaanxi, China
4070183@qq.com

Keywords: Blockchain Technology; Data Security; Privacy Protection; Access Control

Abstract: In recent years, with the frequent occurrence of data leakage incidents, data security and privacy protection have become hot topics of public concern. Blockchain technology is widely regarded as an effective solution to enhance data security due to its unique immutability and decentralization characteristics. This article explores the practical application of a blockchain based data management framework in data security and privacy protection by constructing it. In the access control experiment during the experimental phase, the success rate of administrators accessing the system was 100%, and the success rates for both regular and unauthorized users were 0%. In the evaluation experiment of privacy protection effectiveness, the success rate of 100 decryption attempts was 100%, and the average decryption time was 0.0025 seconds. From the above data conclusions, it can be seen that blockchain technology is effective and reliable in improving data security and privacy protection.

1. Introduction

In today's rapidly developing digital world, data security and privacy protection issues are becoming increasingly prominent, bringing huge security risks and economic losses to society. Blockchain technology, due to its natural immutability and decentralized nature, provides new possibilities for solving these problems. Although blockchain technology has been widely applied in fields such as cryptocurrencies, its potential in data security and privacy protection has not been fully explored and applied. Therefore, studying the application of blockchain technology in this field is of great significance.

This article explores the effectiveness of a blockchain based data security management system in protecting data from tampering and illegal access. The main contributions of the article include: designing a blockchain data management framework that combines smart contracts and advanced encryption technology, improving the efficiency of secure storage and access control of data; through a series of experiments, the actual operating effect of the system was verified, demonstrating its ability to prevent data leakage and illegal access in actual environments. These contributions not only enrich the application research of blockchain technology, but also provide valuable references for solving data security problems in reality.

The article is organized as follows: first, the experimental methods and steps are described, including the processes of data generation, encryption, transmission and decryption. Then, the implementation of each experiment and the analysis of results are described in detail. Finally, the research findings are summarized and the potential challenges and future research directions of blockchain technology in practical applications are discussed.

2. Related Works

In recent years, many scholars have studied the application of blockchain technology in data security and privacy protection. For example, Anna Chor combined blockchain technology with interstellar file system, used blockchain technology to store the hash value and index address of medical data, constructed the logical structure between the data, and realized the traceability, tamper-proof, and solidified deposit of medical data [1]. Li Yang et al. proposed a multi-key homomorphic encrypted transaction scheme based on digital promises, which improved the problem that the transaction process needed to be executed by a full-featured bookkeeping node and the multiple transmissions of the transaction parameters and amounts lead to data leakage, making the transaction process more decentralized and secure [2]. Traditional centralized data management systems are often vulnerable to attacks and breaches. To address these challenges, Raparthi M studied the application of blockchain and artificial intelligence to create a decentralized data management system that prioritized privacy and security [3]. As a promising alternative to cloud storage, decentralized storage networks are expected to evolve and reshape the market in the future. Du Y et al. proposed a fine-grained storage audit design based on custom zero-knowledge protocols in a revised security model to provide mitigation options [4]. Liang W et al. proposed a blockchain based secure data storage and recovery scheme by improving the eccentricity, tamper resistance, real-time monitoring and management of the storage system. The scheme supports dynamic storage, fast repair and update of distributed data in industrial node data storage systems [5]. Khalaf O I has constructed a node identification system based on the data storage requirements of wireless sensor networks using blockchain technology [6]. The traditional blockchain technology is not suitable for modern in-vehicle systems due to high data update overhead, fragile raw data storage strategy and inflexible consensus algorithm. For this reason, Yin Y et al. proposed a blockchain data storage system that supported incremental data updates [7]. However, most of these studies focus on the technical level of exploration and lack detailed analysis and verification of practical application scenarios. In addition, although some studies have proposed blockchain-based privacy protection schemes, their effectiveness and feasibility have not been fully verified. Therefore, the current exploration of blockchain technology in data security and privacy protection still faces many challenges and deficiencies.

To make up for the shortcomings of existing research, some scholars have attempted to combine blockchain technology with other security technologies. For example, Xu G et al. proposed an efficient attribute homomorphic encryption privacy protection scheme based on blockchain [8]. In order to solve the problem of low security and threatened user privacy in connected vehicles, Xu C et al. proposed a blockchain-based privacy protection scheme [9]. Since cloud computing transactions are usually asynchronous, the data privacy and online payment issues involved often lead to a trust crisis. For this reason, Wu X et al. proposed a privacy-preserving cloud computing fair payment scheme based on blockchain and homomorphic encryption that achieves correctness, fairness, compatibility, and lightweight clients [10]. However, these schemes still face problems such as high computational complexity and performance bottlenecks in practical applications. In this paper, we propose a new blockchain-based data security and privacy protection scheme by introducing smart contract technology, aiming to solve the deficiencies in existing research and improve the feasibility and practical application of the scheme.

3. Methods

3.1 Blockchain Infrastructure Design

In this study, we designed a dedicated blockchain infrastructure to enhance data security and privacy protection levels. Firstly, we have selected a suitable blockchain platform to ensure the scalability and efficiency of the system. We choose to use private blockchain because it maintains the core features of blockchain, such as immutability and transparency, while providing faster transaction speeds and better privacy protection [11].

Data layer: The data layer mainly consists of block data and chain structure, and also includes the signature algorithm, hash function, asymmetric encryption algorithm, and Merkle tree structure used in the data layer. Among them, the block head and block body form a complete block. The block header stores the version number, timestamp, hash value of the previous block, difficulty value, random number, and Merkle tree root value generated from transaction data; stores all transaction data of the current block in the block body. When generating new blocks, the blocks are arranged in chronological order through the hash value of the previous block, forming a chain structure.

Network layer: The network layer mainly includes the networking method of blockchain. Blockchain uses P2P networks for peer-to-peer transmission, where nodes receive transactions and verify them before storing them in blocks. Nodes in the blockchain network ensure the consistency of the blockchain through consensus mechanisms.

Consensus layer: The consensus layer mainly adopts the PoW mechanism to achieve data consistency, which requires nodes to perform a certain amount of operations.

Incentive layer: The incentive layer stipulates the issuance and distribution system of economic incentives (usually tokens), which is equivalent to an economic constraint. Through the set incentive system, certain economic incentives are given to nodes participating in the accounting work in the blockchain, and punishment strategies are implemented for nodes that do not follow rules or commit evil.

Application layer: The application layer mainly implements the transaction application of digital currency, including accounting and transfer functions.

3.2 Application of Smart Contracts

Smart contracts were first proposed by Ether, with the aim of achieving Turing completeness and maximizing the demands of real-world application scenarios. In different blockchain systems, smart contracts are also known as chain codes, and this article uniformly uses smart contracts for description. Smart contracts are essentially executable computer programs that define the transaction functions or business logic of contracts and terms between non trusted parties. Compared to traditional digital contracts, smart contracts can be automatically executed by any blockchain participating node, without relying on trusted endorsement institutions, and have better reliability, fairness, and efficiency.

Taking the Ethereum platform, which was the first to support smart contracts, as an example, participating nodes all have sandbox environments, namely Ethereum Virtual Machine (EVM), which can compile and run smart contracts written in Solidity language. In addition, Solidity language is Turing complete, allowing developers to customize business logic to achieve different types of decentralized applications.

Overall, the introduction of blockchain technology into IoT systems will bring two major innovations. On the one hand, it is the innovation of storage modes. Distributed ledgers have replaced traditional centralized databases, and IoT data or transaction transactions will be stored through a blockchain data structure, which is jointly stored and maintained by multiple parties. Not only can it address security issues such as data integrity and privacy protection, but it can also ensure the traceability, integrity, and transparency of data. On the other hand, blockchain technology has also changed the data processing mode. Thanks to the clear hierarchical structure of the Internet of Things, the computing and storage capabilities available at the edge layer have been further explored. Based on smart contracts, many edge devices can process massive amounts of data without relying on third parties, and can ensure the quality and efficiency of services. Through innovation in storage and computing, blockchain technology has brought many security advantages to the Internet of Things, such as decentralization, privacy protection, immutability, high availability, and high error tolerance, and has been widely applied in various fields [12].

3.3 Combination of Data Encryption Techniques

Homomorphic encryption is also a commonly used cryptographic technique in blockchain privacy protection. Homomorphic encryption allows for direct computation of ciphertext data without decryption, enabling multiple complex operations while protecting data privacy. Therefore, in blockchain, in order to protect the privacy of transaction amounts, homomorphic encryption algorithms can be used to encrypt transaction amounts, so that transactions can be operated in a ciphertext state. The property of this process satisfies the Equation (1):

$$\mathrm{E}(\mathrm{m}_1) \cdot \mathrm{E}(\mathrm{m}_2) = \mathrm{E}(\mathrm{m}_1 + \mathrm{m}_2) \tag{1}$$

In equation (1), let $\mathrm{E}(\mathrm{m})$ be a cryptographic function and both m_1 and m_2 be plaintext data.

While implementing homomorphic encryption technology, we also introduced zero knowledge proof technology. Zero knowledge proof, as a two party cryptographic protocol, can convince the verifier of a statement without disclosing any information related to the statement. In blockchain, it is the block production node that convinces other nodes that the current global state transition is effective without leaking transaction information. The proof process is shown in Equation (2):

$$\mathrm{P}(\mathrm{x}) \Rightarrow \mathrm{V}(\mathrm{x}) \tag{2}$$

In equation (2), x is the content to be verified. This approach not only guarantees the privacy of the data, but also effectively prevents unauthorized access and ensures the security and compliance of data operations.

To ensure the security of data during transmission, we have adopted end-to-end encryption technology. The end-to-end forward encryption scheme driven by blockchain is implemented based on the Java language environment, which includes the following steps: system public and private key initialization, private key update, data trusted root calculation, electrical energy data encryption, encrypted information signing, block chain endorsement node verification, data center decryption of electrical energy data, and data integrity verification. The encryption and decryption processes can be represented by equations (3) and (4):

$$\mathrm{C} = \mathrm{E}(\mathrm{K}, \mathrm{P}) \tag{3}$$

$$\mathrm{P} = \mathrm{D}(\mathrm{K}, \mathrm{C}) \tag{4}$$

In equation (3) and equation (4), P denotes plaintext, C is ciphertext, K is key, and D denotes decryption function. This method prevents data from being intercepted or tampered with during transmission and ensures the integrity and confidentiality of data transmission. End-to-end encryption combined with the decentralized nature of the blockchain allows the entire system to maintain a high level of security in the face of cyberattacks [13-14].

4. Results and Discussion

4.1 Data Integrity Evaluation Experiment

In our data integrity evaluation experiment, we first generated a set of 1000 bytes of random data and calculated its initial hash value. Next, we simulated the storage and transmission process of these data in the blockchain system. Specifically, we repeatedly retrieved and recalculated the hash value of the data on multiple nodes to ensure that the data remained unchanged throughout the entire process. We use Matlab to draw charts and display the original data and the transmitted data, as shown in Figure 1:

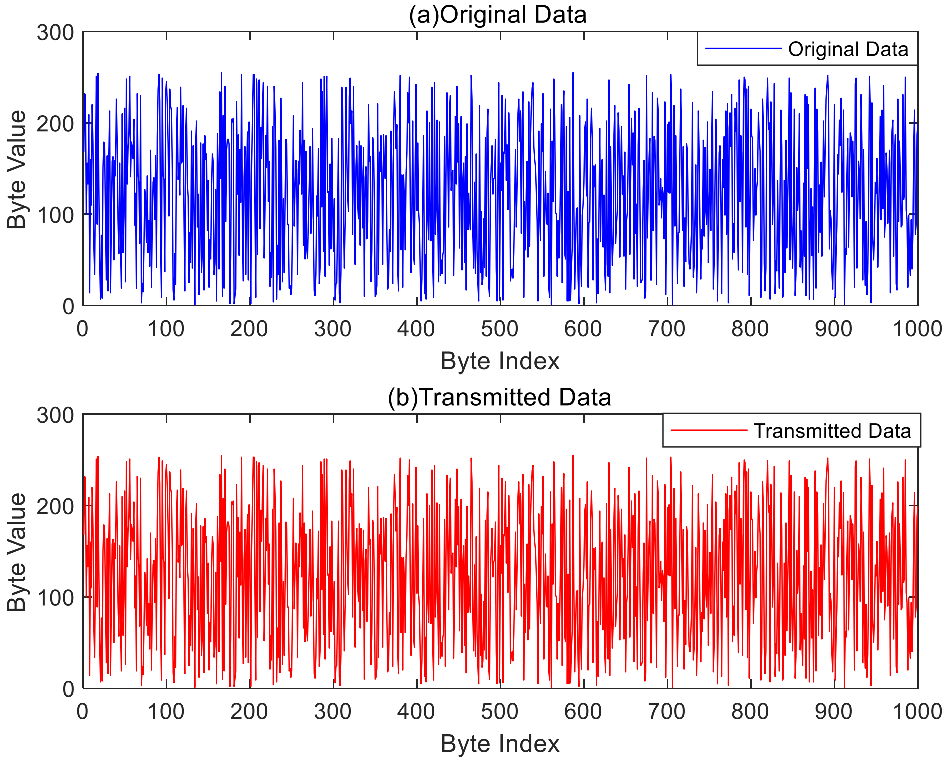

Figure 1: Data integrity assessment

In Figure 1 (a-b), the raw data is represented in blue, and the transmitted data is represented in red. In Figure 1, the initial hash value is b7199bafc769daa60881f7e258ca5187. By simulating the data storage and transmission process in a blockchain system, we retrieved data with hash values of b7199bafc769daa60881f7e258ca5187 across multiple nodes, which are completely consistent with the initial hash values. From the data conclusion, it can be seen that the data remains intact during transmission and storage without any tampering.

4.2 Access Control Effectiveness Evaluation Experiment

In the experiment of evaluating the effectiveness of access control, we evaluated the privacy protection effectiveness of data encryption technology in blockchain systems. Generating a set of sensitive data through blockchain technology and performing encryption and decryption operations to simulate practical application scenarios. The experimental steps include data encryption, decryption attempts, recording decryption time and success rate. By analyzing the decryption results, the specific data situation is shown in Table 1:

Table 1: Assessment of access control effectiveness

User Type	Attempts	Successful Attempts	Success Rate (%)
Admin	100	100	1
Regular User	100	0	0
Unauthorized User	100	0	0

In Table 1, we set up three types of users: administrators, regular users, and unauthorized users, and conducted 100 access attempts each. The success rate of access for administrators is 100%, and the success rates for both regular and unauthorized users are 0%. In the above data conclusion, the access control strategy implemented by smart contracts in blockchain systems effectively prevents unauthorized users from accessing sensitive data, while ensuring the normal access of authorized users.

4.3 Experiment to Evaluate the Effect of Privacy Protection

In the privacy protection effectiveness evaluation experiment, we evaluated the privacy protection effectiveness of data encryption technology in blockchain systems. A set of randomly sensitive data with a length of 1000 bytes was generated in the experiment and encrypted using a symmetric encryption algorithm. Next, recording the time of each decryption operation through 100 decryption attempts.

In the 100 decryption tests in Figure 2, the success rate of decryption is 100%, and the average decryption time is 0.0025 seconds. In the above data conclusions, our encryption technology is very effective in protecting data privacy, and the decryption process is also very efficient and stable. The line graph of decryption time in Figure 2 further illustrates the time of each decryption operation and verifies the reliability and consistency of the encryption method. The specific data situation is shown in Figure 2:

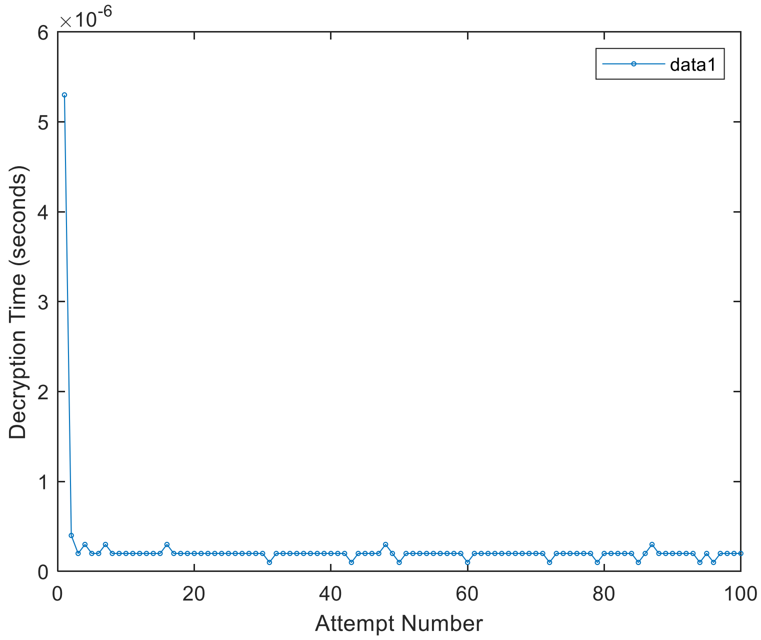

Figure 2: Evaluation of privacy protection effectiveness

4.4 System Performance Evaluation Experiment

In our system performance evaluation experiment, we simulated a series of data operations to test the response time and processing capability of the blockchain system. The specific operations include writing and reading data, as well as executing smart contracts. We conducted 100 tests and recorded the response time of each operation to analyze the average processing speed and efficiency of the system. The specific performance is shown in Figure 3:

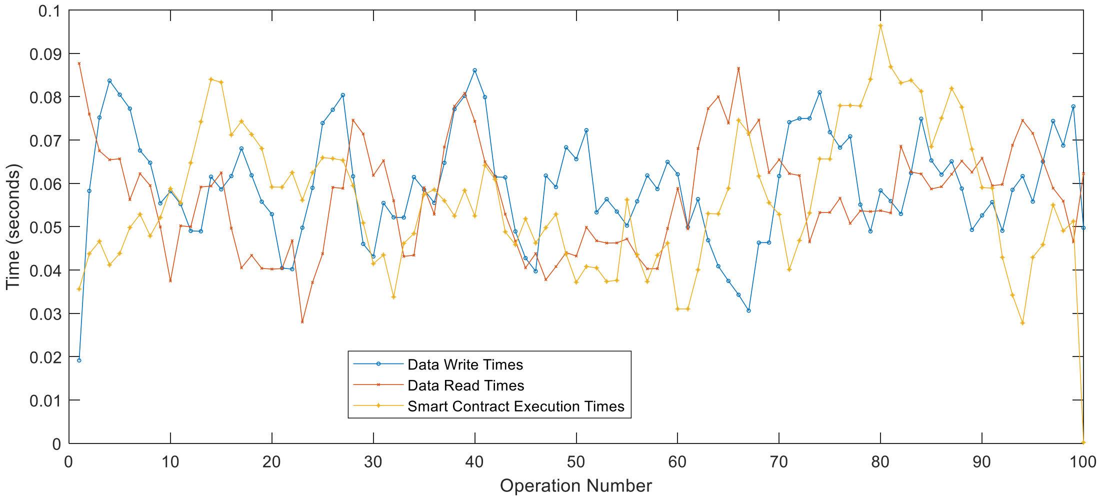

Figure 3: System performance evaluation

In Figure 3, there are 100 data write, read, and smart contract execution operations. The average response time for data writing is 0.059 seconds, the average response time for data reading is 0.056 seconds, and the average response time for smart contract execution is 0.056 seconds. In the above data conclusions, blockchain systems have shown high efficiency and stability in processing data operations and executing smart contracts.

5. Conclusion

In the digital age, the importance of data security and privacy protection is becoming increasingly prominent, especially in key areas such as healthcare and finance where data leakage incidents occur frequently. Blockchain technology, with its immutable and decentralized characteristics, provides a new solution for strengthening data protection. This article explores the application of blockchain in data security and privacy protection, aiming to improve the security of data storage and access control by designing and implementing a blockchain data management system that combines smart contracts and encryption technology. The study validated the effectiveness of the system through experiments, demonstrating its ability to effectively prevent data tampering and unauthorized access. In addition, the article also discusses the challenges that may be encountered when promoting blockchain technology, providing valuable suggestions and development directions for further research and application of blockchain technology.

References

[1] Chu Jingjing, Dong Ruiyin. Research on Distributed Storage Scheme for Medical Data Based on Interstellar File System [J]. China Digital Medicine, 2022, 17 (11): 52-57.

[2] Li Yang, Wan Hongyu, Zhu Jianming, et al. A decentralized blockchain transaction scheme based on digital commitment [J]. Journal of Lanzhou University of Technology, 2023, 49 (4): 95-101.

[3] Raparthi M. Privacy-Preserving IoT Data Management with Blockchain and AI-A Scholarly Examination of Decentralized Data Ownership and Access Control Mechanisms [J]. Internet of Things and Edge Computing Journal, 2021, 1(2): 1-10.

[4] Du Y, Duan H, Zhou A, et al. Enabling secure and efficient decentralized storage auditing with blockchain[J]. IEEE

Transactions on Dependable and Secure Computing, 2021, 19(5): 3038-3054.

[5] Liang W, Fan Y, Li K C, et al. Secure data storage and recovery in industrial blockchain network environments [J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6543-6552.

[6] Khalaf O I, Abdulsahib G M. Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks [J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2858-2873.

[7] Yin Y, Li Y, Ye B, et al. A blockchain-based incremental update supported data storage system for intelligent vehicles [J]. IEEE Transactions on Vehicular Technology, 2021, 70(5): 4880-4893.

[8] Xu G, Zhang J, Cliff U G O, et al. An efficient blockchain-based privacy-preserving scheme with attribute and homomorphic encryption [J]. International Journal of Intelligent Systems, 2022, 37(12): 10715-10750.

[9] Xu C, Wu H, Liu H, et al. Blockchain-oriented privacy protection of sensitive data in the internet of vehicles[J]. IEEE Transactions on Intelligent Vehicles, 2022, 8(2): 1057-1067.

[10] Wu X, Yu F, Wang J, et al. Bpf-payment: Fair payment for cloud computing with privacy based on blockchain and homomorphic encryption [J]. Peer-to-Peer Networking and Applications, 2023, 16(5): 2649-2666.

[11] Liu J, Zhao J, Huang H, et al. A novel logistics data privacy protection method based on blockchain[J]. Multimedia Tools and Applications, 2022, 81(17): 23867-23887.

[12] Zubaydi H D, Varga P, Molnár S. Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: a systematic literature review [J]. Sensors, 2023, 23(2): 788-792.

[13] Elisa N, Yang L, Chao F, et al. A framework of blockchain-based secure and privacy-preserving E-government system [J]. Wireless networks, 2023, 29(3): 1005-1015.

[14] Fang S, Liu Q, Zhang F, Chen N, & Li X. Application of Internet of Things and Blockchain in Information Security and Privacy Protection of Global Organizations. Journal of Organizational and End User Computing, 2023, 35(3), 1-16.