# Research on Rights Management of Blockchain Data with Symmetric Encryption

Jun Wang [1,*,a] , Zhipeng Li [1,b] , Ping Du [2,c], Jun Yu [2,d] , Xiaolong Zhang [2,e]

*[a]wangjun17@lzu.edu.cn; [b]1158852782@qq.com; [c]2438396213@qq.com; [d]2864974919@qq.com; [e]2135144459@qq.com

[1]State Grid Gansu Electric Power Company, Digital Division, Lanzhou 730000, China
[2]Sichuan Zhongdian Qimingxing Information Technology Co., Ltd. Information Enterprise Platform Business Unit, Chengdu, Sichuan 610000, China

**Abstract:** Traditional symmetric encryption algorithms have certain limitations in terms of blockchain data security and permission management due to their decentralization and openness. Therefore, this study aims to explore a method of blockchain data rights management that integrates symmetric encryption algorithm, and proposes a blockchain data rights management framework based on symmetric encryption by analyzing the application potential of symmetric encryption algorithm in blockchain. The framework utilizes symmetric encryption algorithms to protect sensitive data in the blockchain and enables controlled and secure data access through authorization and authentication mechanisms. The results show that the fusion symmetric encryption method has a significant improvement in protecting data privacy and improving data access efficiency. In conclusion, this study proposes an approach to blockchain data rights management that incorporates symmetric encryption and aims to address challenges in blockchain data security and rights management. This method can not only effectively protect the security of sensitive data, but also improve the controllability and efficiency of data access. This study provides a useful reference for further research and practice in the field of blockchain data rights management.

**Key words:** blockchain; Data permissions; Symmetric encryption

## 1 Introduction

With the rapid development of blockchain technology, it has become an important tool for data management and security. However, due to the decentralized and open characteristics of blockchain, traditional symmetric encryption algorithms have some limitations in the management of blockchain data rights. As a result, researchers began exploring ways to incorporate symmetric encryption to improve the security and rights management of blockchain data. Blockchain is a distributed ledger technology that ensures the security and integrity of data through the use of cryptographic algorithms. However, the application of symmetric encryption algorithms in blockchain is still relatively limited. Symmetric encryption algorithm is a method of encryption and decryption using the same key, which has the advantage of high efficiency and fast operation speed. However, due to the sharing of keys, symmetric encryption algorithms face some challenges in data rights management. Current approaches to blockchain data rights management rely primarily on asymmetric encryption algorithms, which include techniques such as public key encryption and digital signatures. These methods ensure data confidentiality

ICEMBDA 2023, October 27-29, Tianjin, People's Republic of China

DOI 10.4108/eai.27-10-2023.2341930

and authentication, but are less efficient when dealing with large amounts of data. Therefore, the research of fusion symmetric encryption algorithm is of great significance in order to improve the efficiency of data access and the ability of processing large-scale data. This study aims to explore a blockchain data rights management approach that incorporates symmetric encryption to solve the current challenges in blockchain data rights management. The research will analyze the application potential of symmetric encryption algorithms in blockchain by reviewing existing research and technologies, and propose a framework for blockchain data rights management based on symmetric encryption. By designing and implementing a prototype system and comparing it with traditional asymmetric encryption methods, the study will evaluate the performance and feasibility of methods that incorporate symmetric encryption in terms of data security and rights management. The results of this study will help drive further development in the field of blockchain data rights management and provide useful references for practical applications. By fusing symmetric encryption algorithms, research can improve the security, controllability and efficiency of blockchain data, leading to innovative solutions for data management and permission control.

## 2 Research status at home and abroad

Decisions recorded on a blockchain cannot be changed and there is the risk of majority attack (also known as 51% attack). Seeking to mitigate these limitations, (Zhu et. al., 2019)[1] propose a controllable blockchain data management (CBDM) model that can be deployed in a cloud environment. The previous blockchain data transmission techniques in industrial Internet of Things (IoT) have low security, high management cost of the trading center, and big difficulty in supervision. To address these issues (Liang et. al., 2019) [2]propose a secure FaBric blockchain-based data transmission technique for industrial IoT. (Tan et. al., 2019) [3]examine the prediction that blockchain technology will transform accounting and the profession because transactions recorded on a blockchain can be aggregated into financial statements and confirmed as true and accurate. (Paik et. al., 2019) [4]aim to increase the level of understanding of blockchain technology as a data store and to promote a methodical approach in applying it to large software systems. The lack of well-processed up-to-date blockchain datasets impedes big data analytics of blockchain data. To fill this gap (Zheng et. al., 2019) [5]collect and process the up-to-date on-chain data from Ethereum, which is one of the most popular permission-less blockchains. With rapid development of computing technologies, large amount of data are gathered from edge terminals or Internet of Things (IoT) devices, however data trust and security in edge computing environment are very important issues to be considered, especially when the gathered data are fraud or dishonest, or the data are misused or spread without any authorization, which may lead to serious problems. A blockchain-based trusted data management scheme (called BlockTDM) in edge computing is proposed to solve the above problems, in which (Zhaofeng et. al., 2020)[6] propose a flexible and configurable blockchain architecture that includes mutual authentication protocol, flexible consensus, smart contract, block and transaction data management, blockchain nodes management, and deployment. (Nicolas et. al., 2021) [7]study blockchain system defensive overview for double-spend and selfish mining attacks: a systematic approach. It presents a comparison framework for existing and future research on blockchain security. (Luo et. al., 2021)[8] present the Impact-Score metric, an efficient framework that attempts to quantify the impact of events on the Bitcoin blockchain.

This specific threat to the reliability of blockchain data is known as the oracle problem. (Sheldon, 2021) [9]argue that they should be viewed as service organizations under the auditing standards from the AICPA and PCAOB. Other influential work includes (Fu et. al., 2019)[10].

## 3 Application system architecture based on blockchain

The system architecture is shown in Table 1. Iot facilities monitor their surroundings, acquire perceptual data, and then broadcast that data in a farm of edge servers. The edge server packages and mines the data, and these perceptual data are stored in the blockchain ledger in the form of blocks, and finally each edge server stores a copy of the ledger locally and synchronously updates the ledger content in real time. Iot facilities synchronize the header content of each block in the ledger in real time and do not store the specific content of the transactions contained in the block. If the iot facility wants to query the specific content of the ledger, it needs to download the relevant content from a nearby edge server, and verify the downloaded content with the block header content that has been stored locally to ensure the correctness of the obtained content. External customers want to obtain the contents of the ledger, they need to query the contents of the ledger by accessing the edge server. The backup ledger of all edge servers is updated synchronously in real time, and its content is consistent, so that customers and edge servers can only access the data in the ledger, and cannot change the ledger. Since every edge server in the system can query any content of the ledger, including the perceptual data stored in the ledger, which may contain some users' private data, access to that data needs to be controlled.

**Table 1** System architecture

| Administrative management | Cloud computing center | Edge server | Iot facility |
|---|---|---|---|
| Office link | Data analysis | blockchain | sensor |
| | Facility management | Public key | NB-loT |
| | Authority management | Real-time interaction | Private key |
| Security decision | Information security | Identity authentication | RFID |

Malicious behaviors in the system can be divided into: 1) Malicious nodes steal data sent by iot facilities; 2) Malicious nodes forge identities and impersonate other nodes to send and request data to any other node in the system; 3) The malicious node intercepts the data sent by the iot facility, then impersonates its identity and sends false data to the edge server; 4) Malicious nodes query the data in the ledger and illegally use or expose the private data therein.

## 4 Specific scheme

Blockchain ensures the validity of data through transparent transmission. In smart cities, there is a large amount of sensing data that is broadcast in a blockchain network. The encryption scheme based on the elliptic curve digital signature algorithm prevents data from being tampered during transmission by verifying the consistency of plaintext and ciphertext. However, due to the lack of effective plaintext encryption, there is still the risk of data leakage. In addition, private data will also be exposed to the blockchain network during the broadcast process, without effective protection. Symmetric encryption is a lightweight and efficient encryption method, which is very suitable for the limited resources of iot facilities. This paper combines symmetric encryption algorithm and elliptic curve digital signature algorithm to propose a blockchain data rights management scheme, which prevents data from being stolen by malicious nodes during transmission, and provides a secure transmission mode of symmetric keys to ensure that the receiving node can correctly interpret the data content. According to the proposed system model, the system is built based on the license chain, and each node in the system holds a pair of public and private keys (Pk,Sk) as a unique identity. The specific encryption process of the scheme is shown in Figure 1. The sender uses the symmetric secret key K to encrypt the plaintext in SIG {·}, which can be expressed as:

$$SIG_{D=Sk,}\{T\} = \left\{ENC_{Sk,}(Sha(T))\|ENC_K(T)\right\}$$

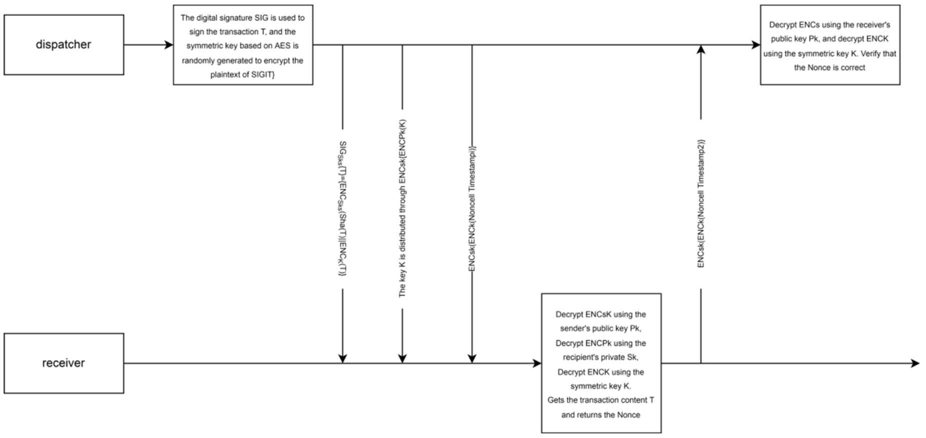
dispatcher
The digital signature SIG is used to sign the transaction T, and the symmetric key based on AES is randomly generated to encrypt the plaintext of SIGIT}
Decrypt ENCs using the receiver's public key Pk, and decrypt ENCK using the symmetric key K. Verify that the Nonce is correct
SIG_Sks{T}={ENC_Sks(Sha(T))||ENC_K(T)}
The key K is distributed through ENCsk{ENCPk(K)}
ENCsk{ENCk(Noncell Timestampi)}
ENCsk{ENCk(Noncell Timestamp2)}
receiver
Decrypt ENCsK using the sender's public key Pk, Decrypt ENCPk using the recipient's private Sk, Decrypt ENCK using the symmetric key K. Gets the transaction content T and returns the Nonce

**Figure 1** Solution flow

Where Sks is the private key of the sender, ENC represents encryption, ENCSks represents the encryption of the content using the private key Sks, T represents the message sent, and Sha(T) represents the summary of the message T generated using a hash algorithm. Next, the symmetric key K is sent using the sender's public key Pkr, which can be represented as ENCSks{ENCPkr(K)}. Finally, the timestamp Timestamp1 and the check code Nonce are sent. If the receiver returns the correct check code, the sender considers that the receiver has received the correct symmetric key and successfully decrypted the transaction information. The ciphertext encrypted with the receiver's Pk can only be decrypted by the corresponding Sk, which provides a secure way for the key distribution of symmetric encryption algorithms that does not rely on a centralized trust authority. Using the sender's public key to sign the message prevents malicious nodes from impersonating other nodes and ensures that the receiver can determine the identity of the sender. By using a dynamic symmetric key to encrypt the plaintext in the digital signature, only the node holding the receiver's private key can obtain the plaintext content, preventing data from being stolen during transmission. Through the above encryption scheme, the private data is effectively protected and the rights are managed. Symmetric keys are randomly generated by iot facilities, and since the amount of sensitive data can be huge, this way of obtaining keys can reduce the efficiency of data queries. Therefore, the generation mode of the symmetric key can be adjusted by the device operator according to the actual situation, for example, the symmetric key can be replaced regularly.

## 5 Experimental analysis

The experiment mainly evaluates the operation cost of the designed data rights management scheme. AES and ECDSA are used as symmetric encryption algorithm and digital signature algorithm respectively, and SHA256 is used as hash algorithm. The experiment simulated STM32 virtual machine as an iot facility on Keil uVision5 based on RT-Thread, and set RT_TICK_PER_SECOND to 2000, that is, the number of beats per second of the system clock was increased by 2000, and the clock beat was 0.5ms. AES and ECDSA algorithms are implemented on virtual machine based on C language.

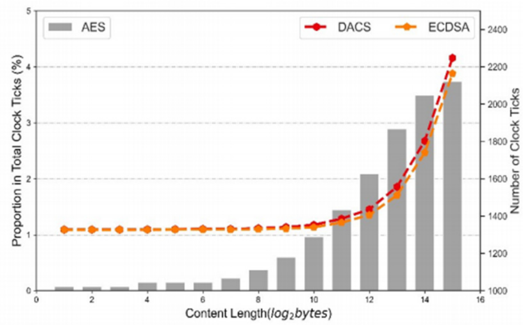

**Figure 2** Calculation cost consumption comparison

Due to the limited resources of iot facilities, running complex encryption algorithms can greatly affect the efficiency of iot facilities uploading data. This paper introduces symmetric encryption (AES) on the basis of ECDSA. Compared to ECDSA, DACS is more expensive to compute. The experiment compared DACS with ECDSA to analyze the computational cost of DACS encrypting private data on iot facilities. As shown in Figure 2, with the increase in the amount of data transmitted, the time consumption required by DACS and ECDSA increases, in which ECDSA increases from 1327 beats at 21Bytes of data to 2146 beats at 215Bytes of data. DACS increased from 1328 beats at 21Bytes to 2248 beats at 215Bytes. The growth rate is slow within 26Bytes and gradually increases after 26Bytes. In DACS, ECDSA takes up most of the run time, especially in the case of small content lengths. In contrast, AES was very efficient, accounting for 0.7% at 21Bytes and 3.7% at 215Bytes. In smart cities, the amount of data uploaded by iot facilities is usually smaller. When the data volume is less than 210Bytes, AES accounts for less than 1% of the total time cost. Therefore, DACS sacrifices a small amount of computing costs, but brings high security and access control capabilities.

## 6 Conclusions

This research focuses on blockchain data rights management with symmetric encryption, aiming to address the application limitations of traditional symmetric encryption algorithms in blockchain and the challenges of data security and rights management. By reviewing the existing researches and technologies, this paper proposes a framework for data rights management of blockchain based on symmetric encryption, and verifies the effectiveness of this framework by designing a prototype system. The experimental results show that the fusion symmetric encryption method can significantly improve the efficiency of data access and protect the security of sensitive data. Compared with traditional asymmetric encryption methods, this method can process large-scale data faster and reduce the computation and storage overhead. At the same time, authorization and authentication mechanisms based on symmetric encryption can achieve control over data access, ensuring that only authorized users can access and modify data. In addition, the blockchain data rights management method that incorporates symmetric encryption can also provide higher data privacy protection compared to traditional asymmetric encryption methods. Symmetric encryption algorithm reduces the complexity of key management by using the same key for encryption and decryption, thus reducing the potential risk of attack. Therefore, the method of integrating symmetric encryption shows better performance and security in protecting data privacy. Overall, the blockchain data rights management approach that incorporates symmetric encryption brings innovative solutions for data security and rights management in the blockchain space. By improving the efficiency of data access, protecting data security and providing data privacy protection, the approach helps drive further development and application of blockchain technology. Future research could further explore and optimize ways to fuse symmetric encryption to meet the growing demand for data management and drive the practical application of blockchain in various fields.

## References

[1] Zhu, L., Wu, Y., Gai, K., Choo, K. R. "Controllable and Trustworthy Blockchain-based Cloud Data Management". Future Gener. Comput. Syst., 2019.

[2] 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.

[3] Tan, B. S., Low, K. Y. "Blockchain As The Database Engine in The Accounting System". Aust. Account. Rev., 2019.

[4] Fu, Y., Zhu, J. "Big Production Enterprise Supply Chain Endogenous Risk Management Based on Blockchain". IEEE Access, 2019.

[5] Paik, H. Y., Xu, X., Bandara, H. M. N. D., Lee, S. U., Lo, S. K. "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance". IEEE Access, 2019.

[6] Zheng, P., Zheng, Z., Dai, H.-n. "XBlock-ETH: Extracting And Exploring Blockchain Data From Ethereum". arXiv preprint arXiv:cs.CR, 2019.

[7] 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.

[8] Nicolas, K., Wang, Y., Giakos, G. C., Wei, B., Shen, H. "Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach". IEEE Access, 2021.

[9] Luo, A., Xu, D. "Quantifying Event Impact on The Bitcoin Blockchain". In 2021 IEEE 45th Annual Computers, Software, and Applications... (CONFERENCE), 2021.

[10] Sheldon, M. D. "Auditing The Blockchain Oracle Problem". J. Inf. Syst., 2021.