Journal of Electronics and Information Science (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2022.070204
ISSN 2371-9524 Vol. 7 Num. 2

Blockchain-Based Information Security Management: A Brief Review

Wenxin Zhao

Taiyuan University of Technology, Taiyuan, China
zhaowenxin1154@163.com

Keywords: Blockchain, Data management, Information security

Abstract: Blockchain integrates P2P network, cryptography, consensus mechanism, smart contract and other technologies, realizing the functions of reliable information transfer between nodes in decentralized transactions, security of trading accounts, and information transfer between nodes will not be tampered with. Block chain technology uses distributed data management technology to store data in chain structure. It plays an important role in information security management and, to a certain extent, ensures user information security. From the perspective of data security management, this paper describes and analyzes the problems existing in data storage security, privacy security, data access security and data sharing security, and the solutions proposed by scholars. In data storage, it mainly introduces on-chain storage and on-chain collaborative storage, introduces privacy security from identity privacy and transaction privacy, and focuses on identity authentication and access control for data access security. Finally, it introduces data sharing security. In the future research, the application of blockchain in information security management is still worthy of attention.

1. Introduction

Blockchain is essentially a peer-to-peer, decentralized, tamper-evident and traceable distributed data ledger. Its birth is the inevitable result of the convergence of cryptography, distributed technology, Internet governance and digital economy development. Blockchain in a narrow sense can be described as a kind of peer-to-peer network environment based on transparent and trustworthy rules to build forgery-proof, tamper-proof and traceable blockchain data structure. In a broad sense, blockchain can be described as a new multicentric infrastructure and distributed computing paradigm that uses cryptographic chain-like block structure to store and verify data, distributed consensus algorithms to add and update data, and code running on the blockchain to ensure the automatic enforcement of business logic.

The characteristics of blockchain include peer-to-peer, decentralization, immutability, transaction anonymity, traceable distributed data storage, etc. Among them, decentralization is the most prominent and essential feature of blockchain. Blockchain technology does not rely on additional third-party management agencies or hardware facilities, and there is no central control, except for the self-contained blockchain itself, and through distributed accounting and storage, each node realizes self-verification, transmission and management of information. Blockchain can be classified into

licensed and unlicensed chains in terms of categories, and the differences in terms of access restrictions, number of participants, consensus algorithms used, and application scenarios are summarized in the Table 1.

Table 1: Difference between licensing chain and non-licensing chain

	Unlicensed chain	License chain
Access restrictions	No access restrictions	There are access restrictions
Consensus algorithm	POW, POS	BFT
Blockchain performance	Good	Bad
Application scenario	Cryptocurrency Trading System	Inter-company contracts, intra-company affairs management

2. Related work

As a distributed data management technology that combines cryptography technology and uses chain structure to store data, the data security management and privacy protection technology within the blockchain system is crucial. From the perspective of data security management, it can be divided into data storage security, privacy security, data access security and data sharing security, as shown in Figure 1.

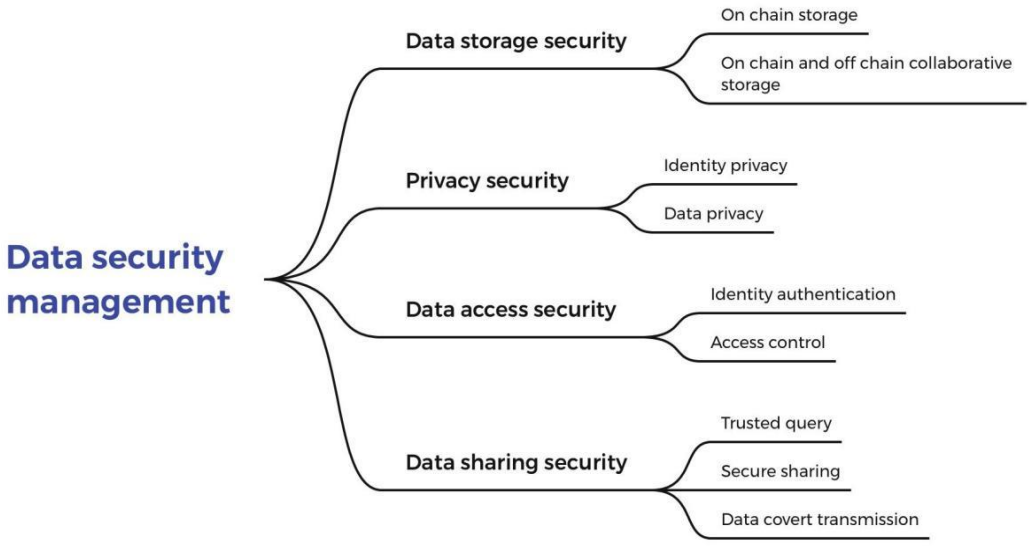

Figure 1: Classification of data security management

2.1 Data Storage Security

Blockchain system data is stored within a database system, such as EL-HINDI et al. [1] designed a blockchain-based shared database using a relational database. The cost of on-chain storage is much higher than the general database, so the form of storing part of the data offline has been developed, and two kinds of data storage methods, on-chain storage and off-chain cooperative storage, are gradually formed. Ali et al. [2] designed a blockchain-based data storage framework, which uses the on-chain and off-chain cooperative approach to store a small amount of metadata of daily files on the chain to achieve the management of identity and access control. This framework uses a collaborative on-chain approach to store a small amount of metadata of daily files on the chain to achieve the management of identity and access control, and store files off-chain. Considering the security of off-chain data uploading to the chain, Xiao et al. [3] proposed Privacy Guard, an access control system

for private data, and its TEE-based off-chain contract execution engine ensures secure data uploading.

2.2 Privacy Security

When using blockchain, privacy security issues arise when the blocks are publicly verified to reach consensus, the relevant data are made available to all nodes involved in the verification. Blockchain privacy is often divided into identity privacy and transaction privacy. For protecting identity privacy often use coin mixing mechanism.

For centralized coin mixing based mechanism, BONNEAU et al. [4] proposed Mixcoin - a centralized coin mixing mechanism which requires senders to mix coins with the same amount at the same time to improve anonymity; and through the mechanism that intermediary nodes sign the transactions and users view the signature information, it prevents the intermediary nodes from being evil, but there is still a risk of transaction information leakage.

The decentralized coin mixing mechanism solves some limitations of centralized coin mixing mechanism to some extent, such as high latency when waiting for enough online participants, susceptibility to DOS attacks, and high user payment for mixing fees, etc. Maxwell et al. [5] proposed the first decentralized coin mixing mechanism, Coin join. Relationship between the sender and receiver accounts, and all transaction participants need to sign the transactions and merge them.

2.3 Data Access Security

In the information security management of blockchain, data access security mainly includes identity authentication and permission access control.

One research direction of identity authentication is blockchain-based distributed PKI system. Fromknecht et al. [6] first proposed a blockchain-based decentralized PKI system Cert coin, which associates user identity with certificate public key, and stores user certificate in the blockchain, and implements identity registration, public key operation, and identity authentication on this basis. Another research direction is to improve the CA-centric PKI system, which is a distributed transformation of CA to record the CA-related operations on the blockchain. Matsumoto et al. [7] proposed IKP, a PKI framework that can automatically respond to unauthorized certificates, with the idea of improving the CA-centric PKI system.

Blockchain-based access control is generally classified into two types: smart contract-based access control and on-chain off-chain collaborative access control. Smart contract-based access control takes advantage of the automatic operation of smart contracts. Cruz et al. [8] proposed a smart contract-based role access control model RBAC-SC, which specifies user roles and other information through smart contracts and assigns reasonable permissions to users. In on-chain off-chain collaborative access control, some systems store data authorization information on the chain to ensure the traceability of data access history, and off-chain stores the accessed resources. ouaddah et al. [9] used on-chain off-chain data collaborative data access control technology to store data authorization information on the blockchain to achieve traceability of data access history off-chain.

2.4 Data Sharing Security

The demand for data sharing has continued to rise in recent years and it is crucial to ensure data integrity and prevent data leakage. Blockchain-based data sharing systems enable secure data query, multi-party data exchange and reliable data transmission.

There is no guarantee that each node on the blockchain is trusted when users query the relevant data, and there are problems with the privacy of blockchain data queries. In response, JIANG Peng et al. [10] designed Searchain, which achieves private search for authorized keywords through

blockchain for keyword queries. In the case of secure multi-party data sharing while needing to safeguard the privacy of users, Shen et al. [11] proposed a blockchain-based support vector machine training model for protecting the privacy of IoT data, which provides a secure data sharing platform. Data covert transmission hides the data to be shared in the actual communication data, which is often achieved by dynamic tags and secret channels, etc. Gao et al. [12] proposed a secret data transmission mechanism, i.e., a secret channel in an open blockchain network.

3. Challenges for Blockchain-Based Security Management

In information management, for data on-chain storage, if all nodes provide enough storage space to store block data, the memory burden of nodes in the network will be too heavy, resulting in wasted storage space and data redundancy problems. JIA et al. [13] designed the Elastic Chain model and used the repetition ratio adjustment algorithm to slice the complete blockchain data to solve the node memory of blockchain system burden problem of blockchain system.

While solving the problem of heavy node burden, it leads to the reduction of the number of full nodes, which reduces the difficulty of full nodes to do evil and affects the reliability of nodes, currently, it is often solved by consensus algorithms. In the blockchain system with on-chain and off-chain cooperative storage, the problem of data integrity and data reliability arises because the original on-chain data is cut off. Ali et al. [14] designed a blockchain-based data storage framework to guarantee the integrity and reliability of data.

The problem of CA man-in-the-middle attack exists in improving CA-centric PKI systems. Matsumoto et al. [7] proposed IKP, a PKI framework that can automatically respond to unauthorized certificates, which uses an economic mechanism to encourage reporting of illegal certificates and punishes CAs that illegally issue certificates. Blockchain technology has some outstanding advantages in privacy protection, which can solve the privacy leakage problem faced by some centralized servers. The advantages and disadvantages of blockchain technology in privacy protection are shown in Table 2.

Table 2: Advantages and disadvantages of blockchain technology in privacy protection

Layer	Advantages	Disadvantages
Network	P2P network is difficult to monitor.	Nodes in blockchain network have a low performance and are vulnerable to being taken over.
Transaction	Blockchain technology supports anonymous transactions.	The correlation among transactions can be used to derive sensitive information.
Application	Decentralized application can effectively counter cyber attacks.	Blockchain applications face various security vulnerabilities.

4. Future work

In terms of blockchain-based data storage, the current research direction is in the direction of on-chain storage, and there are a large number of theoretical results to solve the problems such as heavy memory burden of nodes encountered by using on-chain storage, such as sharding technology [13], B-M tree storage structure and network coding technology.

In the management of privacy security, one of the key research directions is to protect the privacy of identity data and business data. In this regard, cryptographic techniques such as homomorphic encryption, group ring signatures and zero-knowledge proofs are often used, or hybrid coin mechanisms [4-5], and lightning networks are used in these directions to secure the user's identity privacy; for data privacy, data hashing on-chain schemes, off-chain encryption on-chain storage schemes, etc. are mainly studied.

For using blockchain to realize data security access, it usually includes two parts: authentication and permission access control technology. Among them, the main research direction of identity authentication lies in distributed PKI system [6] and improvement of CA-centered PKI system [7], which is the future research direction; for permission access control technology, the current research direction lies in the use of smart contracts [8] or on-chain off-chain collaborative technology [9] means based on blockchain to implement some classical access control models to guarantee secure data access.

Blockchain is applied to data sharing, and in terms of trusted query, the main research direction lies in combining database technology with blockchain; in terms of secure sharing of multi-party data, it is usually solved by encryption technology; for the covert transmission of data, research directions include dynamic tags, secret channels and other schemes [12].

5. Conlusion

Blockchain, as a peer-to-peer, decentralized, tamper-evident and traceable distributed data ledger, is particularly suitable for information security management nowadays.

In this paper, the important role of blockchain technology in data security management is explained from four aspects: data storage management, privacy security management, data access security management, and data sharing security management, and the related challenges and main research directions are listed. The data traceability, anti-tampering and invisibility of data available in blockchain technology are extremely clever to make up for the deficiencies in data security management and greatly enhance its security and reliability.

Nowadays, with the continuous application of blockchain system in various fields, its security issue is becoming more and more pivotal. In response to the new problems and challenges brought about by the widespread application of blockchain in information security management, further research and innovation are also required.

References

[1] EL-HINDI M, BINNIG C, ARASU A, et al. BlockchainDB: a shared database on blockchains [C]// Proceedings of the VLDB Endowment. Los Angeles: VLDB, 2019: 1597–1609.

[2] ALI S, WANG G, WHITE B, et al. A blockchain-based decentralized data storage and access framework for pinger [C]//Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering. New York: IEEE, 2018: 1303–1308.

[3] XIAO Yang, ZHANG Ning, LI Jin, et al. PrivacyGuard:enforcing private data usage control with blockchain and attested off-chain contract execution [C]// Proceedings of the European Symposium on Research in Computer Security. Cham: Springer, 2020: 610–629.

[4] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes [C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 486–504.

[5] MAXWELL G. CoinJoin: Bitcoin privacy for the real world [EB/OL]. (2013-08-22). https://bitcointalk.org/index.php?topic=279249.0.

[6] FROMKNECHT C, VELICANU D, YAKOUBOY S. Certcoin: a namecoin based decentralized authentication system 6.857 class project [EB/OL]. (2014-03-14). http://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov- certcoin.pdf.

[7] MATSUMOTO S, REISCHUK R. IKP: turning a PKI around with decentralized automated incentives [C]// Proceedings of 2017 IEEE Symposium on Security and Privacy. San Jose: IEEE, 2017: 410–426.

[8] CRUZ J, KAJI Y, YANAI N. RBAC-SC: role-based access control using smart contract [J]. IEEE Access, 2018, 6: 12240–12251.

[9] OUADDAH A, ABOU E A, AIT O A. FairAccess: a new blockchain-based access control framework for the Internet of things [J]. Security and Communication Networks, 2016, 9(18): 5943–5964.

[10] JIANG Peng, GUO Fu-chun, LIANG Kai-tai, et al. Searchain: blockchain-based private keyword search in decentralized storage [J]. Future Generation Computer Systems, 2020, 107: 781–792.

[11] SHEN Meng, TANG Xiang-yun, ZHU Lie-huang, et al. Privacypreserving support vector machine training over blockchain-based encrypted IoT data in smart cities [J]. IEEE Internet of Things Journal, 2019, 6(5): 7702–7712.
[12] GAO Feng, ZHU Lie-huang, GAI Ke-ke, et al. Achieving a covert channel over an open blockchain network [J]. IEEE Network, 2020, 34(2): 6–13.
[13] JIA Da-yu, XIN Jun-chang, WANG Zhi-qiong, et al. ElasticChain: support very large blockchain by reducing data redundancy [C]// Proceedings of the Asia-Pacific Web and Web-Age Information Management Joint International Conference on Web and Big Data. Cham: Springer, 2018: 440–454.
[14] ALI S, WANG G, WHITE B, et al. A blockchain-based decentralized data storage and access framework for pinger [C] //Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering. New York: IEEE, 2018: 1303–1308.