Advances in Computer and Communication, 2024, 5(2), 135-140
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Research on the Potential of Blockchain in Building Medical Information Systems

Guanlin Fan

North China University of Science and Technology, Tangshan, Hebei, China.

How to cite this paper: Guanlin Fan. (2024) Research on the Potential of Blockchain in Building Medical Information Systems. *Advances in Computer and Communication*, 5(2), 135-140.
DOI: 10.26855/acc.2024.04.007

Received: March 22, 2024
Accepted: April 19, 2024
Published: May 16, 2024

***Corresponding author:** Guanlin Fan, North China University of Science and Technology, Tangshan, Hebei, China.

Abstract

The healthcare industry has long struggled to ensure the integrity, security, and traceability of patient data. Traditional medical information systems often encounter issues such as single-site failure, data forgery, and inadequate data traceability. Due to the privacy of medical information and the limitations of the current storage methods for medical records, most patients have a very limited understanding of their medical information, making it difficult to access and utilize effectively. This is also the main factor that affects the quality and development of medical treatment. Safe sharing and use of medical information are also major concerns for the medical industry. In recent years, blockchain technology has emerged as a viable solution to these problems. Especially in the epidemic era, personal information in the medical supply network is shared among providers of medical services, including examination items, treatment items, medical facility utilization items, and consumption record items. Based on the practices and applications of predecessors, this paper discusses the utilization of blockchain technology in constructing robust and dependable medical information systems and its significant potential.

Keywords

Chunk chain, medical information systems, trust, complex privilege management with multiple private keys, traceability

1. Advantages of blockchain: trust, transparency and security

1.1 High reliability

One of the motivations for the use of blockchains in medical information systems is the rapidly increasing demand for the high security and reliability of these critical systems. In addition, the blockchain systems emphasize reliable, decentralized account books to store important information. The need for reliability and data integrity has continued to increase in recent years. With the help of distributed databases and corresponding security algorithms, a variety of persistent information can be securely stored on a public ledger such as ethernet. The encryption procedure for block generation and connection improves the security of individual blockchain transactions. Data records on the blockchain are immutable and cannot be changed once the data is generated, which greatly improves the reliability of the data.

1.2 Exceptional transparency

For a long time, it has been recognized that it is difficult for patients and clinicians to access medical records. Due to the privacy of medical information and the limitations of the current storage methods of medical information records, most patients do not understand and use their medical information records adequately. This is an obstacle to making health care transparent and efficient. This lack of interoperability is increasingly apparent when complex patients

come into contact with caregivers from different medical jurisdictions [1]. Blockchain-based systems are a possible solution, which can eliminate the asymmetry of medical information to a certain extent. Break the "data island" phenomenon.

1.3 Superior safety

The sharing security of medical information is the most popular problem in today's data age. The purpose is to not disclose the authenticity, integrity, and privacy of the user as much as possible when the normal data communication with each other [2]. In today's world where the ability of computers to be used for malicious purposes has been greatly enhanced, cyber attacks have become very cheap and easy. Therefore, there is a need for more efficient and effective methods to ensure security and protect the data privacy of personal information. With the support of the blockchain, higher security and the required privacy level can be brought. The medical information sharing scheme based on blockchain utilizes blockchain technology to realize the safe storage and efficient sharing of medical information, and at the same time fully protect the privacy of patients and the ownership of personal medical data.

2. Irreplaceable place of blockchain in medical information systems: complex privilege management with multiple private keys

2.1 The role of multi-private key complex privilege management and its advantages

Complex privilege management with multiple private keys is a method to enhance the security of digital assets. It is based on multi-signature technology and needs multiple private keys to authorize transactions or operations, in order to ensure the security and controllability of assets. In complex rights management with multiple private keys, each private key can be assigned to a different user or entity, which means that multiple authorizations are required to complete an operation. In the medical information systems based on the blockchain, the advantages of the complex authority management of multiple private keys are mainly reflected in the following aspects:

A. Data security and privacy protection: In medical information systems, the personal health information of patients is extremely sensitive, and confidential data, needs to be strictly protected. Through the complex privilege management of multiple private keys, only authorized users can access and operate specific data, which can effectively prevent unauthorized access and data disclosure and improve the security of data.

B. Data integrity: The integrity of medical information is critical to ensuring the accuracy and reliability of data. Through multi-private key privilege management, you can limit the modification and deletion of data. only authorized users can modify the data, thus ensuring the integrity and reliability of the data.

C. Audit and tracing: multi-private key permission management can record each user's access to and operation of data, thus realizing the audit and tracing of data. This helps monitor data usage, track data sources and flows, detect unusual operations and data breaches in a timely manner and improve transparency and traceability in data management.

D. Improving the reliability and stability of the systems: through the complex privilege management with multiple private keys, a set of perfect data access control mechanisms can be established to effectively prevent malicious access and operation, improve the stability and reliability of the systems, and ensure the normal operation of the medical information systems and data security.

E reducing the risk of data leakage: strict rights management can reduce the risk of data leakage and avoid data leakage and abuse caused by unauthorized access and operation. Multi-private key rights management systems can effectively reduce the occurrence of data leakage events and protect data security in medical information systems.

2.2 The realization method of complex privilege management of multiple private keys

Through the consideration of combining blockchain-related technology with the uniqueness of the existing medical information systems, the complex authority management of multiple private keys of the medical information systems constructed based on the blockchain should be realized from the following steps:

A. Assign different private keys: For different user roles (such as patient, doctor, and researcher), the systems assign different private keys. Each private key corresponds to a specific user role that distinguishes the user's identity and permission level.

B. permission level definition: determine the permission level and operation scope corresponding to each private

key. For example, a patient's private key may have permission to upload and manage an individual medical record, a physician's private key may have permission to view a patient medical record, and a researcher's private key may have permission to query public medical record information.

C. multi-factor authentication: in the process of private key management, a multi-factor authentication mechanism is adopted to ensure the security of the private key. For example, the combination of password, fingerprint recognition or hardware security modules, and other technologies enhances user authentication security.

D. access control list (ACL): establishes an access control list that associates a private key with a specific access right. ACL can define which private keys have access to which medical record and which operations can be performed.

E. permission approval process: design the permission approval process to ensure that the allocation of private keys and permission changes are subject to the authorization process. Any private key assignment, permission modification, or revocation requires the approval of authorized personnel.

F. logging and auditing: realize the logging and auditing functions of private key usage, and monitor the usage and operation records of private key. Timely find abnormal operations and take corresponding measures to ensure the safety of medical records.

D. Encryption technology guarantee: in combination with encryption technology, the private key is stored and transmitted in an encrypted manner to prevent the private key from being disclosed and used illegally. Ensure the security and privacy of the private key.

3. Related research status at home and abroad

3.1 The related research status of China

Domestic research institutions and scholars have carried out a lot of empirical research and theoretical discussions on the application of blockchain in medical information systems. They proposed different application models and technical solutions and discussed the potential role of blockchain in medical information sharing, privacy protection, data security, etc. These research results provide important theoretical support and practical guidance for promoting the innovation and development of medical information systems.

Chen Baifan, a scholar, pointed out that the traditional electronic medical record systems used in domestic hospitals currently difficult to achieve information interaction, resulting in the "information island effect". At the same time, centralized traditional medical information systems are prone to failure or hacker attacks, data security can not be guaranteed. In addition, it is difficult for hospitals to monitor patients' medical data which can easily lead to serious privacy breaches. However, the blockchain-based medical information sharing scheme can use blockchain technology to achieve the encrypted and secure storage and efficient sharing of medical information, and protect the privacy of patients and the ownership of personal medical data [2].

In order to solve the problem of medical systems architecture, scholars Sun Xuebo and Jiang Jinxi designed a medical systems architecture based on blockchain. The systems use blockchain technology to store and manage data, discuss the intelligent contract design method of medical systems based on blockchain in detail, and provides the specific implementation scheme. They built a blockchain platform with intelligent contract function to store medical data and realize doctor-patient interaction. At the same time, a medical information system is developed by using front-end calling various interfaces and graphical clients [8].

Different from previous scholars, Chen Zengjujiao designed the blockchain architecture of the medical data information systems, including the initialization systems, data acquisition and upload query and analysis, and other core modules. The architecture adopts a dual-channel deployment mode and medical chain code to realize the management and access control of medical data. At the same time, the server and Android data terminal are also developed, which completes the construction and function realization of medical data information systems and solves the problems of poor data security and difficult data sharing in traditional medical systems [3].

3.2 The relevant research abroad

In the United States, Europe, and other places, many research institutions and medical institutions are actively exploring the application of blockchain technology in medical information systems. They continue to explore the potential applications of blockchain technology in the medical field and strive to promote its implementation and application in actual medical practice through empirical research and case analysis.

EL Azzaoui, ABIR, Chen, and other scholars proposed the implementation of blockchain and intelligent contract

and information-hiding technology to enhance the security and privacy of data communication in key systems, such as intelligent medical supply chain communication networks. They demonstrated the feasibility of using the framework of the Hyperledger intelligent contract and the level of security required. It is proposed to apply blockchain and intelligent contracts to information hiding technology to enhance the security and privacy of data communication in key systems, such as intelligent health care [4].

Some electronic medical information systems and technologies have been adopted in developed countries in recent years, but such technologies have serious privacy risks and security concerns, particularly with regard to data transmission and data transaction records. Moreover, the high cost and complexity of these technologies make their application very difficult for less developed countries. Scholar Anass Rghioui et al. are committed to solving these problems and propose a solution based on distributed blockchain architecture to enhance the security of medical information systems. Such solutions are particularly suitable for developing countries, which lack high-tech infrastructure and lack interoperability between systems [5].

3.3 Summary of research status

In summary, relevant scholars in China and abroad have conducted in-depth research on the application of blockchain technology in medical information systems in different directions and achieved fruitful results, which is also a powerful proof of the huge application potential of blockchain technology in medical information systems. However, the research of domestic and foreign scholars mainly focuses on data security, sharing, and management. At present, there are still some challenges and deficiencies in the performance and scalability, laws and regulations, and practical application of blockchain technology in medical information systems. Further research is needed to solve these problems and promote its application in the medical field.

4. Related problems and solutions

4.1 Scalability issues

Because blockchains require each node to have a complete, identical set of book storage, the growing chain size places a heavy storage burden on nodes that have joined the blockchain systems. At the same time, the hardware resource threshold of the nodes that join the blockchain network is becoming higher and higher, which has a great impact on the security and scalability of the blockchain systems [6].

Solution

To solve this problem, it is very important to design a general scheme to optimize blockchain storage. In particular, this can be achieved by node grouping and historical data fragment clipping.

A. Aiming at the difficult problem of storage pressure in the scene, the rules of data fragmentation can be designed aiming at the data quantity and the bottom layer structure of the blockchain, and the nodes are used for data storage. Compared with the traditional distributed storage scheme based on DHT, no large-scale storage data movement is required after the nodes are added or reconstructed, and a single node only needs to save a group state table with a very small storage amount to obtain the data storage position of the whole chain, thereby ensuring efficient data exchange between the nodes.

B. Facing the problems that the large number of nodes leads to increasingly inconvenient block data management and the interaction cost is gradually increased, the scheme of node grouping can be used pertinently. The key point of this scheme lies in proposing multiple indexes according to the node hardware energy and combining the Ping delay data between nodes, to achieve the goal of dynamically dividing node groups. In the process of index selection and measurement, the requirements of different scenarios are fully considered to ensure the overall performance of the group is balanced and reduce the communication cost within the group.

C. After the data cutting, the node needs to be reconstructed and an outage process needs to be added, and a method for acquiring the cut data needs to be added. In order to meet the needs of the downtime process, and increase the node access to cut data, should also design the corresponding node interaction mechanism. In this way, the clipped data can be efficiently and reliably transmitted between nodes, and the integrity, security and robustness of the blockchain systems are ensured.

On the premise of maintaining the node functional integrity and not affecting the system performance, the storage scheme of optimizing the blockchain can effectively solve the problems of high redundant storage and waste of node storage resources [6].

4.2 The retrieval efficiency problem

Due to the block structure specific to blockchains, it is not possible to retrieve specific details of transaction data directly from the chain. Therefore, how to efficiently retrieve data in blockchain is a problem worth studying [7].

Solution

A double-level index framework based on blockchain can be designed to solve these problems. The framework integrates two existing index methods into an inner layer index structure and an outer layer index structure, wherein the outer layer index is stored through a MySQL database so that users can realize rich and diverse query functions and blocks where target data is located can be quickly positioned. At the same time, the B-tree structure is used to store transaction data in the block and to create an internal index, which is mainly used to improve the speed of data retrieval within the blockchain.

A. External index structure based on MySQL database: This index structure can store the field information of common query conditions in electronic medical records. The user can use a single-value query and a combined query. You can speed up data queries by creating highly differentiated field indexes. The query result includes the location of the block where all the target data satisfying the query conditions are located [7].

B. An internal index structure based on the b-tree structure: the transaction data in the block is redefined through a transaction index tree based on the b-tree structure. A transaction index tree is constructed by using the b-tree structure, and each node is used for storing the main keyword of a transaction and a corresponding transaction address. The transaction record is pointed directly to the complete electronic medical record [7].

5. Problems to be overcome in 6-blockchain in medical information systems

Although great achievements have been made in the research on the application of blockchain medical information systems, there are still many important problems in the practical application that need to be solved.

A. Compatibility issues: There are a variety of data formats and standards in medical information systems, including medical records, diagnostic results, drug information, and so on. These data may come from different medical institutions, devices, and systems, resulting in inconsistent formats and different data structures. When these data are stored on the blockchain, they need to be standardized into a unified format and structure to ensure the effectiveness of data exchange and sharing between different systems. Therefore, there is also a need to develop uniform data standards and formats so that the blockchain system can properly parse and process these data. At the same time, it is necessary to ensure that the blockchain system has good interoperability and can seamlessly exchange and share data with other medical information systems. This needs to consider data format conversion, data transmission protocol, security authentication, and other issues to ensure that the data interaction between different systems is safe, efficient, and reliable.

B. Performance and transaction speed issues: Transactions in medical information systems usually need to be processed quickly, such as patient visits, doctor prescriptions, and data exchange within the hospital. Therefore, the blockchain systems need to have a high transaction speed, be able to quickly verify and record transactions, and ensure the real-time and reliability of transactions. However, the traditional blockchain systems may have the problem of slower transaction speed, for example, the block confirmation time of bitcoin is longer. Therefore, we need to consider how to optimize the blockchain systems to meet the needs of the medical information systems, such as fragmentation, side chain, consensus algorithm optimization, and so on, to ensure that the systems can efficiently handle large-scale data.

C. Compliance issues: Medical information systems address legal and regulatory requirements such as the strict privacy and security requirements imposed on medical data by regulations such as HIPAA. When storing and sharing medical information within a blockchain, there is a need to ensure compliance with relevant legal and regulatory requirements, which may require some technical and legal adjustments. Medical information involves sensitive data, so relevant laws, regulations and compliance requirements, including data privacy regulations, medical confidentiality laws, etc. need to be observed when using blockchain technology. There is a need to ensure that medical information systems are designed and implemented in compliance with legal and regulatory requirements.

D. Cost and return on investment issues: the introduction of blockchain technology may require significant investment, including systems development, deployment, operation and maintenance, security, and other costs. At the same time, investors need to evaluate the actual benefits and values of blockchain technology in medical information systems. Investors need to comprehensively evaluate the actual value and potential benefits of blockchain technology

according to the actual demand and development stage of medical information systems, so as to make a reasonable investment decision. At the same time, it is necessary to consider the uncertainty and risk of blockchain technology and reasonably assess the possibility and feasibility of return on investment.

To overcome these obstacles, technical, legal, privacy, security and other factors should be comprehensively considered to ensure the effective application and smooth implementation of blockchain in medical information systems. At the same time, continuous exploration and innovation are needed to find solutions to overcome these obstacles and promote the application of blockchain technology in medical information systems.

6. Conclusion

Blockchain technology provides a feasible solution to health care information management. Although some obstacles remain, enhancing the integrity, security, and traceability of data makes the use of blockchains in health care a worthwhile project. The medical systems based on blockchain technology not only ensure that patients understand their own information in time but also ensure the reliability and safety of information, which is conducive to the use and management of medical information for patients and improves the efficiency of medical security. With the emerging potential of blockchain technology, the future prospects of healthcare information systems become even broader.

References

[1] Mehta Shaun, Grant Kiran, Ackery Alun. Future of blockchain in healthcare: potential to improve the accessibility, security and interoperability of electronic health records [J]. BMJ Health & Care Informatics, 2020, 27 (3).

[2] Chen Baifan. Research on the security of medical information sharing based on blockchain [D]. Tutor: Yu Xiulan. Chongqing University of Posts and Telecommunications, 2020.

[3] Chen Zeng. Research on medical data information system based on Internet of Things and blockchain [D]. Tutor: Yu Hua. Chongqing University, 2021.

[4] EL Azzaoui, Abir, Chen, Haotian, Kim, So Hyeon, et al. Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems [J]. SENSORS, 2022, 22(4).

[5] Anass Rghioui, Said Bouchkaren, Anas Khannous. Blockchain-based Electronic Healthcare Information System Optimized for Developing Countries [J]. IAENG International Journal of Computer Science, 2022, 49.0 (3.0).

[6] Zhang Li-wan. Research on optimization scheme of blockchain storage [D]. Southeast University.

[7] LI Jing-wen. Blockchain-oriented electronic medical record retrieval method [D]. Tutor: Wang Jian. Nanjing University of Aeronautics and Astronautics, 2021.

[8] Sun Xue-Bo, Jiang Jin-xi. Design of medical information systems and intelligent contract based on blockchain [J]. Journal of Liaoning University of Science and Technology, 2020, 43 (02): 135-145.