WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 3, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v3n1.06
Journal homepage: https://wepub.org/index.php/IJCSIT/index

A Review of Blockchain-Based Research on E-Health Data Sharing

Mingzhi Qin, Qingtao Wu

School of Information Engineering, Henan University of Science and Technology, Luoyang 471023, China

ABSTRACT

With the development of medical data informatization, the data security, data privacy, and data controllability of electronic medical data with patient's personal privacy have gained social attention. Blockchain technology has decentralized characteristics, and the development of blockchain technology provides an effective solution for the secure sharing of e-medical data. Many scholars have proposed e-medical data security sharing solutions based on blockchain technology, and these solutions have attempted to solve the security problems encountered in sharing traditional e-medical data. By summarizing and analyzing the schemes in this field, this study analyzes the advantages, disadvantages, and challenges that the current mainstream schemes have, mainly in terms of blockchain data security storage, access control security sharing, and so on, in order to promote the further development of the e-medical data security sharing scheme based on blockchain technology. This study analyzes the blockchain-based e-medical data security sharing scheme proposed by scholars by analyzing the blockchain technology, cryptography technology, smart contract technology, P2P network technology and other related topics. Through systematic analysis and comparison, it explores the challenges of the current research and provides references for the future proposals of blockchain technology-based schemes.

KEYWORDS

Blockchain; Security sharing; Electronic medical data

1. INTRODUCTION

Along with the rapid development of information technology, medical services are moving towards digitalization and informationization. The wide application of Electronic Health Records (EHR) systems marks the entry of medical information into the digitalization mode. Traditional paper-based medical data has shortcomings such as not easy to be saved and not easy to be disseminated, however, converting paper-based medical data into electronic information data and saving it in EHR system solves the problems of traditional medical record data. Internet medical data informatization not only successfully solves the problem of difficult to save patient medical record data, but also greatly improves the efficiency of hospitals and saves valuable medical time for patients. For electronic medical data, if EHR data can be shared, it can be used to conduct multi-faceted, multi-angle, multi-expert research and judgment for difficult cases, which in turn improves the level of public medical health and treatment efficiency [1]. At the same time, the sharing of EHR data avoids the cumbersome process when patients are treated across hospitals, enables timely consultation and timely analysis, reduces patients' medical expenses, and saves patients' valuable time.

However, e-medical data contains patients' private information.E-medical data is characterized by high sensitivity, privacy, and large quantity, and hospitals treat e-medical data as extremely valuable

information among themselves, and these characteristics make the storage and sharing of e-medical data challenging everywhere.e-medical data is commonly stored in each hospital server independently of each other, which results in the phenomenon of data silos. In addition, patients often have no control over the generated e-medical data and cannot generate specific access control conditions for a particular environment, which can be used to control access by hospital staff such as doctors [2-3]. Moreover, hospitals, as the central organization for storing electronic medical data, are prone to single-point attacks, and once attacked by a single point of attack, a large number of patients' electronic medical data will be leaked, losing the rights and interests of both the hospitals and the patients, and the servers within the hospitals also have the possibility of being tampered with by malicious users, which does not guarantee the authenticity of the electronic medical data. In conclusion, there are some challenges in e-medical data storage and sharing that need to be attempted to be solved.

Blockchain as a decentralized technology provides a new solution to the above problems. 2008 scholar Nakamoto published the paper "Bitcoin: A peer-to-peer electronic cash system" in the first proposed blockchain technology, the technology has decentralized and distributed storage characteristics, can do the data difficult to tamper with, openness and transparency, security depository and other advantages, these advantages are exactly the shortcomings in the safe storage and sharing of electronic medical data [4-5]. With the continuous development of blockchain technology, when the blockchain enters the 2.0 era, smart contract technology is introduced, and the data of the blockchain is operated through smart contracts, which increases the transparency of data operation. The development of blockchain has become a powerful tool for solving the security sharing of e-medical data [6]. Due to the decentralized characteristics of blockchain, blockchain has been used in scenarios such as drug traceability and intelligent medical care, and the existence of reliability, robustness and fault tolerance of blockchain features ensures the application of real-world scenarios.

However, there are still some challenges in the application of blockchain technology in e-medical data sharing [7-9]. First, the distributed characteristics of blockchain technology require a large amount of storage space, which can easily bring the storage performance of distributed nodes to a threshold and increase the system load of nodes. Second, the open and transparent characteristics of blockchain cannot guarantee the confidentiality of the data, and it is necessary to combine the encryption characteristics of cryptography technology to jointly guarantee the confidentiality of the data, and to use the access control that cryptography can provide to control the sharing of the data, in addition to the problems of the data storage format, the differences in laws and regulations, and so on [10].

In summary, this paper will summarize all aspects of blockchain-based e-medical data security sharing scheme, and discuss in depth the problems of e-medical data sharing, data storage, and data access control based on blockchain technology. It mainly includes the introduction of relevant technical background, secure storage of e-medical data, secure sharing and access control, analyzing the advantages and shortcomings of the existing solutions, and finally making a summary, which will serve as a reference for the future proposal of e-medical data security sharing solutions based on e-medical data, so as to promote the development of e-medical data sharing based on the blockchain as well as its application.

2. BACKGROUND

This section of the review provides background information on blockchain, smart contracts, P2P networks, and consensus mechanisms to guide the generalization of the scenarios in the review section.

2.1. Blockchain

Blockchain as the emergence of decentralized technology, widely used in various fields, with decentralized characteristics, replacing the centralized existence of disadvantages in the traditional industry, and promoting the development of the traditional industry. Among them, the development of blockchain can be roughly divided into three stages: the birth of bitcoin, so that blockchain technology is known to people, the first period of blockchain technology, represented by bitcoin, the application of digital currencies, the widespread use of blockchain technology as decentralized transactions, of which, ethereum, bitcoin constitutes the mainstream blockchain technology. The second period, then the introduction of smart contracts, the introduction of smart contracts, not only the blockchain as a decentralized currency platform, the birth of many derivatives, including DAPP and other specific applications, people at this time the blockchain as a decentralized storage, the use of the blockchain platform to deposit evidence. The third period, on the other hand, is the period of alliance chain development, the rapid development of the alliance chain, on behalf of the blockchain technology is widely used in all walks of life, among them, the first blockchain technology is Fabric, the alliance chain is more in line with the reality of the application, so the development of the more rapid.

2.2. Peer To Peer(P2P) Network

Essentially, blockchain is a peer-to-peer network. P2P networks have a variety of topologies, communication patterns between nodes, and types of nodes that participate. Predominantly, there are three main categories of network topologies, which are centralized, decentralized structured, and decentralized unstructured.

This property of peer-to-peer is inherited by blockchain. Additionally, the governance model is being used to classify blockchains. As a result, blockchain systems can be broadly classified into two classes based on the presence of permission and network governance followed. As per the presence of permission, there are two types, which are permissioned and permissionless. According to governance, there are also two kinds, which are public and private.

2.3. Smart Contracts

A smart contract can be thought of as an automatically invoked procedure that is initiated when a transaction is executed. All blockchain systems support smart contracts; however, they differ in terms of the language in which smart contracts can be written and the environment in which they are executed. Solidity, Golang, Serpent, Java, Python, and LLL are the most often used smart contract languages. There are numerous execution environments available, including the Ethereum Virtual Machine (EVM), Java Virtual Machine (JVM), Docker Image, and Haskell execution environment.

2.4. Consensus Mechanisms

Consensus mechanism as one of the core technologies of blockchain, the technology aims to achieve node message consistency through consensus, so as to complete the synchronization of messages between nodes, different consensus mechanisms determine the blockchain to reach a consensus in different ways, such as proof of workload, through the calculation of the difficult hash value will be the data uploaded to the chain, with the difficulty of the difficulty of the hash value to improve, will continue to consume arithmetic power. There are two other consensus mechanisms, POS and DPOS, which complete the uplinking action through the share rights and interests. Although the consumption of arithmetic power is canceled, it reduces the decentralized characteristics and violates the characteristics of blockchain with decentralized characteristics. In addition, there is PBFT consensus mechanism, which has the characteristic of preventing Byzantine fault tolerance, through the nodes

communicate with each other in order to reach an agreement, and since PBFT eliminates the token transaction, it is more suitable for the field of electronic medical data.

3. BLOCKCHAIN-BASED EHEALTH DATA SHARING SOLUTION

3.1. Secure Storage of Ehealth Data

E-medical data is saved into the blockchain, and the data is uploaded to the blockchain through the consensus algorithm.In the model about the storage of e-medical data, many scholars have improved the storage efficiency by improving the consensus algorithm, as well as combining with the encryption algorithm to ensure the safe storage of e-medical data.

Literature [11] used cloud storage to build a medical blockchain system to protect the storage security of medical data, and carried out on-chain operations through the POW consensus mechanism, but the POW consensus mechanism required a lot of computing power. However, POW has the stability of decentralization, so there are still scholars to study the POW consensus mechanism, among which, Literature [12] proposed the MedRec medical blockchain system, which uses the POW consensus mechanism to achieve consensus, controls data access through the management of medical data access permission, and realizes the storage of patients' medical data. Literature [13] proposed a blockchain-based electronic medical record management system to manage electronic medical records, and realized the prototype of the management system through the blockchain "Hyperledger" platform, and adopted the POW consensus algorithm to achieve block consistency. In the above schemes, POW and DPOS are used for consensus operation. For a large number of electronic medical data, POW needs to consume a large amount of computing power to complete consensus, while DPOS has certain shortcomings due to its high throughput but insufficient degree of decentralization. PBFT consensus mechanism has Byzantine fault tolerance and does not require computing power consumption.The PBFT workflow is shown in the figure1.Therefore, for the medical field, PBFT can be used for consensus, which will improve the performance of the system. For this reason, many researchers have conducted studies to construct medical data storage models for PBFT.

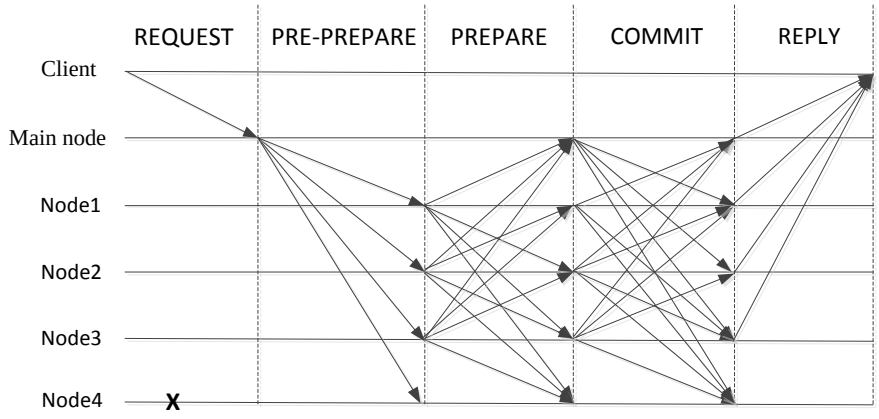

Figure 1. PBFT consensus process

Literature [14] proposed to use zero-knowledge proof and proxy re-encryption technology to protect the privacy of medical data, in which PBFT is used for consensus on-chain operation of blockchain. Although PBFT has certain advantages compared with other traditional consensus algorithms, when the number of nodes increases, the communication between nodes greatly increases and the efficiency is reduced. Literature [8] proposed a blockchain-based electronic medical record management system, MedBlock, which improved the PBFT algorithm through the idea of DPOS algorithm and improved the efficiency of the system. However, the voting method of this scheme is simple, which is easy to lead to the emergence of Byzantine nodes and has low reliability. Literature [15] proposed the sc-PBFT consensus algorithm for the sharing of electronic health records among medical institutions,

which has the feature that node status can be checked. In the process of consensus, the credibility of nodes needs to be checked to achieve the purpose of secure consensus.

To sum up, in view of the block chain security storage problem, many scholars improve the system availability by improving the consensus mechanism in the block chain, combined with cryptographic primitives to complete the data security storage work, however, these encryption technologies rely on complex principles, resulting in increased computing overhead, therefore, in the block chain-based electronic medical data storage work, There are still some difficult problems to solve.

3.2. Secure Sharing of Electronic Healthcare Data

Many scholars have conducted research on the safe sharing of electronic medical data, and protected the data with access control brought by cryptography. The combination of cryptography and blockchain has promoted the development of safe sharing of electronic medical data. In the field of electronic medical data, cryptography algorithms have special requirements. For example, the encryption and decryption speed is fast, and the access control is set freely to meet the practical needs. The overall sharing process is shown in Figure 2. Therefore, many scholars have invested in the research.

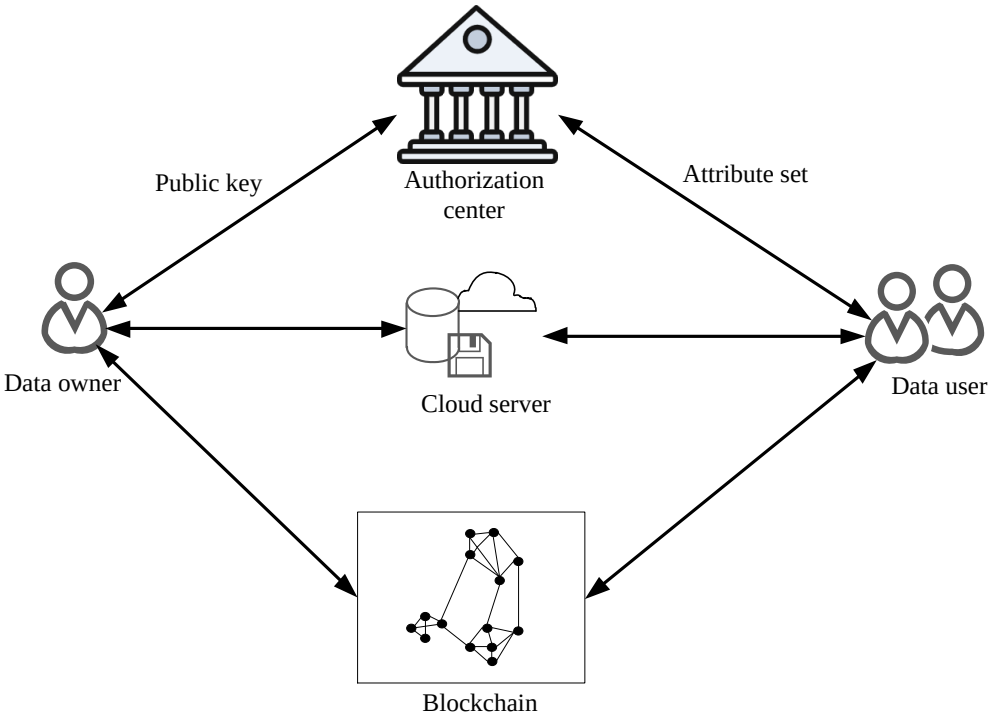

Figure 2. Electronic medical data sharing diagram

Literature [16] constructed an electronic medical record privacy protection scheme based on blockchain and attribute encryption. In the scheme, medical record data can be securely shared through attribute encryption. Based on CP-ABE and optimized, this scheme has higher encryption and decryption efficiency and can be better applied to medical blockchain. Literature [17] proposed a decentralized secure EHR sharing framework, using smart contracts and attribute encryption, and designed a constant-size attribute scheme based on attribute encryption to effectively improve the performance of the encryption algorithm.Literature [18] proposed a medical data sharing scheme combining permission-block chain, IPFS and improved CP-ABSE to provide better privacy protection, key management and high efficiency. Literature [19] propose to introduce a hierarchical access control readable blockchain model for data sharing through attribute-based encryption and chameleon hashing, under which data owners can specify who can modify their data by setting access policies and authenticating modifiers using digital signatures.

In summary, the use of attribute-based encryption technology can flexibly implement access control according to attributes to adapt to the complex scenarios and dynamic access needs of medical systems. With this technique, only users who meet a specific set of attributes can have decryption and access rights, thus ensuring the privacy of the data. Most importantly, in the healthcare context, collaboration and information sharing can be achieved across organizations and roles. However, due to the high computational complexity, the running time will become very long when processing a large number of data, which will consume a lot of resources. In addition, due to the need to manage multiple keys for attribute-based encryption, there are additional costs associated with key management.

In the electronic medical data sharing model based on blockchain, not only attribute encryption is shared, but also proxy re-encryption technology can impose access control on electronic medical data. Proxy reencryption is implemented through proxy key conversion to convert a ciphertext into one that can be decrypted, so that multiple shareers can obtain data, ensuring data security to a certain extent.

Literature [21] combined proxy re-encryption technology with sequential multi-signature.An assisted electronic medical record scheme based on blockchain is constructed. The program is mainly aimed at one.For multiple consultations or referrals, make sure that the patient is treated by one or more doctors data security in the case of diagnosis. Literature [22] propose a blockchain-based approach to complete medical information sharing the model, the scheme uses Internet of Things technology (IOT) for data collection to the cloud server and the agent are based on the re-encryption algorithm to achieve anonymous sharing.

If proxy reencryption is used for sharing, there will be an untrusted third party, and the third party will be relied on to complete the proxy conversion service. Then, if the agent is not honest, there is a risk of key leakage.

4. CONCLUDING REMARKS

With the continuous development of blockchain technology, blockchain-based e-medical data system will have more new possibilities to promote the development of smart healthcare, protect the privacy of patients' e-medical data and improve convenience at the same time. In this paper, from the perspective of blockchain-based e-medical data sharing, data storage and sharing, we collate the literature on blockchain-based e-medical data sharing in recent years, and analyze the advantages as well as disadvantages of the existing solutions.

At present, there are still challenges to be overcome in the existing schemes, and new technologies need to be constantly found to integrate with blockchain technology for better application in the field of e-medical data, and secondly, the continuous development of cryptography technology will also promote the development of blockchain technology as a background scheme for e-medical data scenarios, and it is believed that in the future, there will be a more efficient cryptographic algorithms are more suitable for encrypting e-medical data with large data volume. medical data. Finally, blockchain technology as decentralized attempts to solve the problems in the traditional centralized e-medical data scenarios, it is believed that blockchain can effectively solve some of the problems and land to bring convenience.

ACKNOWLEDGEMENTS

This work was supported in part by the Key Technologies R & D Program of Henan Province under Grant No. 232102210028, 232102211008 and 232102210048.

REFERENCES

[1] Hoerbst A, Ammenwerth E. Electronic health records [J]. Methods of Information in Medicine, 2010, 49(04): 320-336.

[2] Jensen P B, Jensen L J, Brunak S. Mining electronic health records: Towards better research applications and clinical care [J]. Nature Reviews Genetics, 2012, 13(6): 395-405.

[3] Zou R, Lv X, Zhao J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system [J]. Information Processing & Management, 2021, 58(4): 102604.

[4] Xia Q I, Sifah E B, Asamoah K O, et al. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain [J]. IEEE Access, 2017, 5: 14757-14767.

[5] Berdik D, Otoum S, Schmidt N, et al. A survey on blockchain for information systems management and security [J]. Information Processing & Management, 2021, 58(1): 102397.

[6] Akarca D, Xiu P Y, Ebbitt D, et al. Blockchain secured electronic health records: Patient rights, privacy and cybersecurity [C]. 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2019: 108-111.

[7] Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management [C]. 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016: 25-30.

[8] Fan K, Wang S, Ren Y, et al. Medblock: Efficient and secure medical data sharing via blockchain [J]. Journal of Medical Systems, 2018, 42: 1-11.

[9] Huang H, Zhu P, Xiao F, et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data [J]. Computers & Security, 2020, 99: 102010.

[10] Wang M, Guo Y, Zhang C, et al. MedShare: A privacy-preserving medical data sharing system by using blockchain [J]. IEEE Transactions on Services Computing, 2021, 16(1): 438-451.

[11] Esposito C, De Santis A, Tortora G, et al. Blockchain: A panacea for healthcare cloud-based data security and privacy? [J]. IEEE Cloud Computing, 2018, 5(1): 31-37.

[12] Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management [C]. 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016: 25-30.

[13] Usman M, Qamar U. Secure electronic medical records storage and sharing using blockchain technology [J]. Procedia Computer Science, 2020, 174: 321-327.

[14] Huang H, Zhu P, Xiao F, et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data [J]. Computers & Security, 2020, 99: 102010.

[15] Pang Z, Yao Y, Li Q, et al. Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm [J]. IEEE Access, 2022, 10: 87803-87815.

[16] Jiang Y, Xu X, Xiao F. Attribute-based encryption with blockchain protection scheme for electronic health records [J]. IEEE Transactions on Network and Service Management, 2022, 19(4): 3884-3895.

[17] Wang M, Guo Y, Zhang C, et al. MedShare: A privacy-preserving medical data sharing system by using blockchain [J]. IEEE Transactions on Services Computing, 2021, 16(1): 438-451.

[18] Liu J, Wu M, Sun R, et al. BMDS: A blockchain-based medical data sharing scheme with attribute-based searchable encryption [C]. ICC 2021-IEEE International Conference on Communications. IEEE, 2021: 1-6.

[19] Zhang T, Zhang L, Wu Q, et al. Redactable blockchain-enabled hierarchical access control framework for data sharing in electronic medical records [J]. IEEE Systems Journal, 2022, 17(2): 1962-1973.

[20] EFANOV D, ROSCHIN P. The all-pervasiveness of the blockchain technology [J]. Procedia Computer Science, 2018, 123: 116-121.

[21] Chen Z, Xu W, Wang B, et al. A blockchain-based preserving and sharing system for medical data privacy [J]. Future Generation Computer Systems, 2021, 124: 338-350.

[22] Liu X, Yan J, Shan S, et al. A blockchain-assisted electronic medical records by using proxy reencryption and multisignature [J]. Security and Communication Networks, 2022, 2022.