Research and design of medical data sharing and insurance automatic claim system based on blockchain technology

Yuan Chen, Heng He* and Jiacheng Zheng

Wuhan University of Science and Technology, Wuhan, China

*Corresponding author: Chen_Yuan0101@163.com

heheng@wust.edu.cn

1064072620@qq.com

Abstract. In recent years, blockchain technology has been applied to various business scenarios with its characteristics of decentralization, openness, self-consistency and information immutable. In the medical insurance industry, disputes often occur between insurance institutions and policyholders due to inaccurate personal information and different confirmation of contract terms. With the digitalization of medical information and the rapid development of science and technology, insurance claim settlement schemes based on blockchain and homomorphic encryption can enable the hospital, the insurance institution and policyholders to establish a trusted mechanism, which can ensure the authenticity and security of the policyholder's personal information and the validity of the contract. The scheme combines Paillier homomorphic encryption and blockchain smart contract while designing access control list to control patients' data. In the scenario of insurance claim settlement, it can not only protect the privacy of patients' medical data, but also ensure the correct settlement result of insurance claim.

Keywords: blockchain, hyperledger fabric, homomorphic encryption, case sharing.

1. Introduction

In the past medical system, patients' personal health data is mainly stored centrally, and the medical data between most hospitals is relatively closed. Patients' personal health records are generally stored in the database of a single hospital or even in the paper medical account book, which is difficult to distinguish due to various factors. At present, only a few hospitals in China can share medical data, especially when medical information needs to be verified, saved and synchronized. The patient during the whole treatment might involve many cases, check, hospitals and even the final insurance claims, and in an environment where complete and trusted access to medical data is not established, it's very difficult for the hospital or the insurance agency to access the patient right related medical data and update the medical data. For the hospital, if the new hospital cannot obtain the latest medical data of the patient in time when the patient is transferred to another hospital for treatment, it may lead to the unknown condition of the patient or the treatment time delay or other serious problems; For the insurance institution, in order to avoid the insured person deliberately concealing the past disease history and other situations, the insurance institution should check and verify the insured person's past medical history before signing the insurance contract with the insured person. If the latest medical data of the patient cannot be obtained in time, it is easy to cheat the insurance or occur other illegal phenomena.

In addition, patients do not have control over their medical records in the current medical system. On the one hand, patients' medical data are often filled and controlled in by the hospital, which inevitably leads to information leakage, malicious modification and other bad situations. On the other hand, the phenomenon that the insurance institution can directly query the medical information of the policyholder through the hospital staff violates the privacy of the insured.

In view of various problems existing in medical data sharing and insurance claim settlement scenarios, this paper proposes a medical record security sharing and insurance claim automatic settlement scheme based on blockchain and homomorphic encryption. By designing smart contracts and combining blockchain technology with homomorphic encryption technology, a trusted

mechanism is established among hospitals, insurance institutions and patients through blockchain to ensure the security of user medical record data. The patient has the right to control the medical record data, and other users need to apply for the permission to access the medical record data from the patient. Only after obtaining the permission can they access the medical record data of the patient. When a user goes to a hospital to see a doctor, the doctor applies for access to the patient and fills in the medical record. The medical record information is broadcast in the blockchain network. After being verified by other users in the blockchain network, the medical record information will be written into the blockchain; When users make insurance claims, they interact with the blockchain network. Using the smart contract, the blockchain will return the claim results based on the patient's insurance information, and the insurance institution cannot learn any privacy of the patient during this process.

2. Blockchain and related technologies

2.1 Blockchain

Blockchain, as its name suggests, is a chain of blocks. In a blockchain network, data is stored in blocks, which are hashed to generate a hash value for each block, and eventually all the blocks are linked back and forth by the hash value to form a blockchain. Blockchain uses a consensus mechanism to determine the authenticity and originality of data, and data is stored after encryption, so medical records are hard to tamper with. In terms of rights management of medical data, blockchain can control access rights through digital signature to ensure that information is not peeped; With the private key, personal data can be securely shared with doctors or insurance agencies, improving the efficiency of information sharing. We choose to use blockchain technology precisely because of its two core characteristics of data that is hard to tamper with and decentralization, which can create a trusted environment and thus provide another technical solution for the reliability of the database. Blockchain itself can not rely on any third party to complete the data transmission of distributed nodes, storage, and verify the relevant data communication network, which means it can be seen as a completely transparent distributed large network books, everyone can add data information anytime and anywhere, and it can also provide services to any user demand.

By dividing administrative authority, blockchain can be divided into public chain, private chain and federation chain. Public chain, such as Bitcoin or Ethereum, can be freely joined by anyone to compete for billing rights through "mining". Without access control measures to restrict data information, the privacy of data can not be protected; Private chain is established by enterprises or organizations themselves, with strong data access control measures. And the data on the blockchain is usually not open to the public. In order to achieve a balance between the public chain and the private chain, there is the alliance chain. The alliance chain is usually jointly established by several organizations and the alliance. The data in the alliance chain network is only accessible to the members of the alliance and it needs to be read according to the access control rules customized by the alliance. If a node wants to join the alliance chain network, it needs the permission of the alliance member. Comparatively speaking, alliance chain has better flexibility and elasticity.

2.2 Hyperledger fabric

Hyperledger Fabric is a blockchain platform currently widely used in enterprises, and its code is fully open source. Unlike public chains such as Bitcoin and Ethereum, Hyperledger Fabric members need to register with a trusted Membership Service Provider (MSP) for authorization before joining the network, thus avoiding the overhead of Proof of Work(PoW) resource and greatly improving transaction processing efficiency. Compared with other blockchain projects, its main features are:

(1) Highly modular, the core architecture in Hyperledger Fabric is highly modular and has a high degree of configuration freedom to provide innovative capabilities for the financial, insurance, healthcare, supply chain and other industries;

(2) With support for general-purpose programming languages, Hyperledger Fabric supports the use of high-level programming languages such as Java, Go, Python and Node.js, allowing developers to get started quickly without having to learn domain-specific languages from scratch;

(3) Pluggable options, ledger data can be stored in multiple formats , consensus mechanisms can be swapped, and support for different MSPS;

(4) Provides the ability to create channels that allow a group of participants to create their own trading ledgers. This is a particularly important choice for some networks. In these networks, some participants may be competitors and do not want every transaction they make to be known to all participants. In this case, the two participants can form a channel that has a copy of the ledger of the channel, while the other competitors do not.

2.2.1 Distributed ledger

Hyperledger Fabric has a ledger subsystem, which mainly consists of two components: world state and transaction log. Each node in the blockchain keeps a copy of the ledger. The distributed ledger system is shown in Figure 1. The world state component acts as a database of books, describing the state of the books at a given point in time. The transaction logging component records all transactions that produce the current value in the world state.

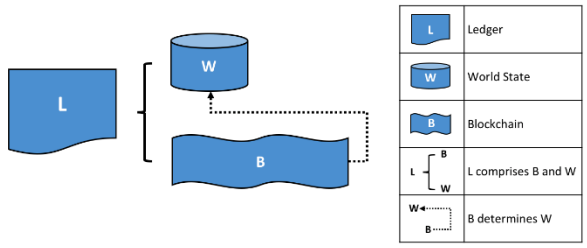

Fig. 1 Ledger diagram

2.2.2 Smart contract

The smart contract is a piece of code deployed on a blockchain that is automatically executed once an event triggers the terms of the contract. It is typically written by a developer using the Go language to provide the state-handling logic of a distributed ledger. The smart contract can be deployed by their peers in the blockchain and docker containers can invoke smart contracts in a secure environment and then interact with data through communication protocols. In different development scenarios, developers can develop smart contracts according to specific conditions, as shown in Figure 2.

Fig. 2 Smart Contract Schematic

Smart contract is a core technology of blockchain, which is characterized by automation, decentralization and enforceability. By writing smart contract into blockchain with computer code, a network contract can be completed and successfully executed on time. Thanks to the characteristics of smart contracts, the application of these emerging technologies to medical data sharing and automatic insurance claims can simplify transaction processes and improve work efficiency while ensuring data security.

2.2.3 Consensus mechanism

Blockchain is a peer-to-peer transaction, in which transaction proposals submitted by peers in the network are written into the blockchain ledger in chronological order, resulting in high latency. In a distributed environment, we don't have a central institution like a bank to ensure that all the bookkeeping content on the chain is consistent, or that the transaction proposal isn't tampered with, so we need a mechanism to agree on the order of transactions that happen at the same time. This algorithm for reaching a consensus on the order of transactions within a time window is called the consensus mechanism. The consensus mechanism mainly includes Proof of Work, Proof of Stake, Delegated Proof-of-Stake, Directed acyclic graph, Practical Byzantine Fault Tolerance and Proof-of-Authority. The schematic diagram of consensus mechanism is shown in Figure 3:

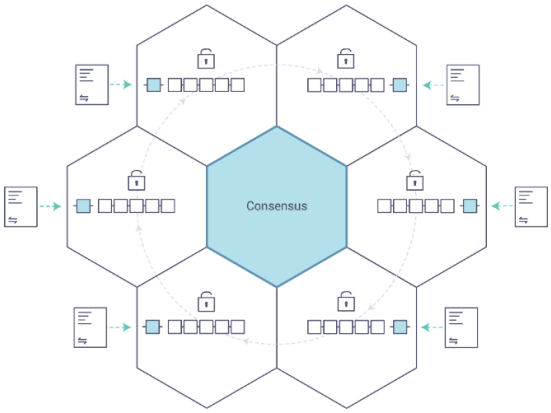

Fig. 3 Schematic diagram of consensus mechanism

2.2.4 Paillier's homomorphic encryption

Homomorphic encryption refers to the homomorphic encryption of the original data, and specific operations such as addition or multiplication are performed on the ciphertext. The calculation results are the same as those obtained by direct calculation of plaintext. The main feature of Paillier's homomorphic encryption is that it pays attention to the security of data processing. It will not leak any information of the original text during the whole calculation process, and the result after calculation is still in the encrypted state. Paillier encryption system is a probabilistic public key encryption system invented by Paillier in 1999. Based on the difficult problem of compound residual class, it supports addition homomorphism and number multiplication homomorphism and has the characteristics of high computational efficiency and complete security proof. Paillier algorithm mainly includes three parts: key generation, encryption process and decryption process.

The key generation process is as follows:

(1) Randomly selected two large prime Numbers p, q, and satisfy the gcd(p*q, (p-1) * (q-1)) = 1, here the gcd(p * q, (p - 1) * (q 1) calculate the number of two greatest common factor;

(2) Calculation n=p*q and lambda = lcm(p-1,q-1), here the lcm(p-1,q-1) means calculating minimum common multiple of two Numbers;

(3) Pick the integer $g \in Z_n^*$ at random;

(4) Define function $L(x) = \frac{x-1}{n}$ and calculate $u = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, the generated public key is (n,g) and the private key is (λ,u).

The encryption process is as follows:

(1) Enter the plaintext message m, and 0≤m<n;

(2) Select random number $r \in Z_n^*$, and satisfy 0≤r<n;

(3) Calculate ciphertext $c = g^{\mathrm{m}} r^{\mathrm{n}} \bmod n^2$.

The decryption process is as follows:

(1) Enter the cipher c, and $c \in Z_{n^2}^*$;

(2) Compute the plaintext message $m = L\left(c^{\lambda} \bmod n^2\right) * u \bmod n$.

Correctness analysis：

Assuming that the disease insured by the patient is $M_n, E(M_n)$ represents the ciphertext after homomorphic encryption, and the disease recorded in the patient's electronic health record is M, the following calculation will verify whether the patient is qualified for claim settlement:

$$\begin{gathered} E(M_n) \times E(M)^{-1} = \\ (g^{m_n} \times r^{n_2}) \times (g^{m} \times r^{n_1})^{-1} mod\ n^2 = \\ (g^{m_n - m} \times r^{n_2 - n_1}) mod\ n^2 = \\ E(M_n - M) \end{gathered} \tag{1}$$

If

$$M = M_n,\ D(E(M_n) \times E(M)^{-1}) = D(M_n - M) = 0. \tag{2}$$

2.2.5 Django

Django is a free, open source framework for Python that provides a number of common modules for web backend development, allowing developers to focus on the business side. It is fast to develop, simple to use, and full of features. Its web applications section can be used to quickly build high performance and elegant web sites. By using the Django framework, you can build and maintain high quality web applications with minimal cost.

The Django framework uses the MTV design pattern, which is derived from the MVC pattern. In MVC mode, the Model layer, View layer and Controller layer are closely connected but independent from each other. Each layer provides its own independent interface for other layers to call. This design reduces the coupling between codes and increases the reusability of code modules. MTV design pattern is actually a refinement of MVC pattern, which separates the View layer in MVC pattern at a deeper level, making the View layer more focused on the implementation of business logic, while the parsing and rendering of View is completed by the Template layer. The schematic diagram of MTV design is shown in Figure 4, which contains the following three levels:

(1) Model: Data storage layer, which handles all data-related business and interacts with the database;

(2) Template: the Template layer, which handles page display;

(3) View: Business logic layer that handles the concrete business logic and calls Model and Template when appropriate.

In addition, the Django framework has a URL dispenser that distributes browser-side page requests to different views, which then call the corresponding Model and Template.

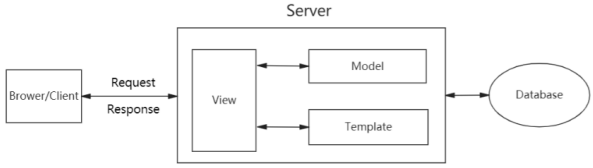

Fig. 4 Django MTV Design Pattern schematic

3. The realization of safe case sharing and automatic insurance claim system

3.1 System structure design

The system structure is shown in Figure 5. The system includes three roles: patient, doctor and insurance institution. In addition, the role of administrator is set up for registration and management of system users. Take patients as an example, in this system, patients can view personal medical records, apply for insurance claims, purchase insurance products and some other operations. At the same time, the system realizes the safe sharing of medical record data by designing access control list. When other users want to access medical record data, they need to send access request, and

patients can obtain access permission only after approving the request in the authorization management module.

Fig. 5 System structure diagram

3.2 Medical treatment process design

As shown in Figure 6, in the initial state, ordinary users see a doctor in the hospital. At this time, the doctor does not have access to the user's medical record data and needs to send an access request in the system. After obtaining permission, doctors fill out medical records based on the patient's past medical records and visits. After the process is complete, users can revoke access rights as required.

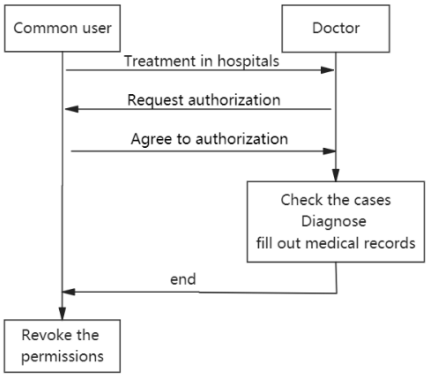

Fig. 6 Flow chart of normal treatment

3.3 Insurance claim process based on blockchain

As shown in Figure 7, the user interacts with the blockchain to apply for insurance claim, and the blockchain invokes the smart contract to return the claim result, so that the user can be informed of the claim result. In this process, the insurance institution cannot be informed of the patient's medical record data, and the privacy of the patient's medical record data is ensured while the user successfully obtains the claim.

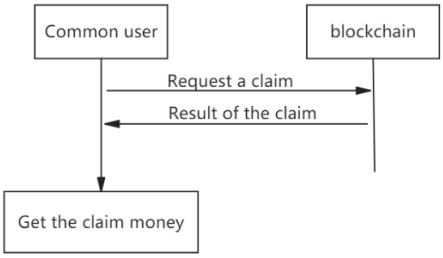

Fig. 7 User claim process

4. Conclusion

In this paper, blockchain is introduced in the process of medical data sharing to build a trust mechanism, and smart contracts are written to realize automatic insurance claims. In this system, users' medical data and health information are permanently recorded in the blockchain, and the decentralized characteristics of blockchain are utilized to ensure the authenticity and reliability of data, which protects users' rights and interests to a certain extent. Due to the natural self-consistency between smart contract and medical insurance contract, it can not only save the tedious verification process of traditional medical insurance, but also help insurance institutions and users to develop reliable insurance contract. The execution of the contract is transformed into the effective execution of the function of smart contract, which effectively improves the efficiency of insurance claims.

References

[1] J.Li Lin, Medical data security protection based on blockchain technology, Electronic Design Engineering, 2022, 10.013,62-70.

[2] J. Wang Tianyu,Wu Min, Zhou Ying, A medical health data transfer and security sharing scheme of medical union based on block chain, information system engineering, 2022,(05),68-71.

[3] J. Elghaish Faris; Pour Rahimian Farzad; Hosseini M. Reza; Edwards David and Shelbourn Mark, Financial management of construction projects: Hyperledger fabric and chaincode solutions, Automation in ConstructionVolume 137, 2022, 10.1016/J.AUTCON.2022.104185.

[4] J. Tang Huanhuan, Research on smart contract technology and application based on block chain, Computer Programming Skills & Maintenance. 2022,(03), 128-131.

[5] Zhang Xiang，Design and Implementation of Medical Insurance System Based on Blockchain Smart Contract Technololgy，master，Huazhong University of Science and Technology，HuBei China，2019.5.21.

[6] J. Yu Jia,Hu Guangyu,Wan Yanshaopeng, Research on smart medical reimbursement platform based on block chain, Information and Communication Technology.2020,14(03),51-56.

[7] J. Liu Yanwen,Wu Tao,Shen Bin,Yang Jindong,Pang Da. Design and Implementation of construction data Sharing Platform based on Django, Modern Computer, 2022,28(02),117-120.

[8] J. Qian Zhenghao,Wang Jun,Luo Jinxi. Design and implementation of Hyperledger based health insurance and electronic medical affairs linkage system. Computer Era. 2021,(12),55-59.