A Design of Medical Information Sharing Model Based on Blockchain Technology

Hao Jiang, Hao Peng and Songyi Dian*

College of Electrical Engineering and Information Technology, Sichuan University, Chengdu, China
*scudiansy@mail.scu.edu.cn

Abstract. Through the studying of the status quo of medical industry, we find some problems with the sharing of medical data. The medical data in traditional medical institution is stored on severs and its backup database, resulting in lack of communication among medical institutions and ineffective use of medical resources. In order to solve this problem, we propose a medical information sharing model based on blockchain technology. In this model, we build a p2p network to connect different medical institutions and other nodes. Meanwhile, we establish two associated blockchain to store medical data digests and requests. Each node in the p2p network can search the medical information in the distributed medical institutions. In this way, we have integrated medical data between medical institutions and improved the transparency and sharing of medical data. Also, we improve the traditional POW (power of work) algorithm, by using the double-chain structure, we reduce the confirmation time of a block.

1. Introduction
The blockchain was proposed by Nakamoto in 2009, it was first used in bitcoin. It is a decentralized distributed public ledge, which mainly applied to the financial field [1] [2] [3]. In the bitcoin system, transactions can be found in all nodes, and the records are completed by all nodes. With the increase of nodes and blocks, all the transactions in blockchain are hard to be changed. In a broad sense, we can treat the blockchain as a natural distributed system, the data is stored on distributed nodes. Compared with traditional database, the data in blockchain is safer and is widely backed up on distributed nodes. However, there are inherent deficiencies in data search speed and data formatted storage.

We generally think the data in blockchain is very safe as blockchain is composed of interconnected blocks. Figure 1 shows the general structure of a block [3][4].

In Figure 1, A block mainly contains two parts. In block head, it contains some information of the current block and the related information of the previous block. In the block body, it contains many transactions. Each block body records every transaction and encrypts it with a hash algorithm, finally, this information was recorded in block as a merkle root. Every ten minutes, a block may be created, then it will be added to the chain. Due to each block is related to the previous block, all the blocks will be connected in series to form a chain. Each block is created by all nodes, and all nodes reach to a consensus status by POW algorithm. In the process of consensus, each single node searches a proof by a hash calculation, and the node finds the proof first which can generate a block and get profits [5]. Since the blockchain was appeared in 2009, many blockchain applications has emerged. Practical tests found that blockchain has strong security.
The traditional database is a warehouse which was built on a computer storage device, and usually organized by data structure. Due to the complex structure of the data, we can easily store complex data and search for data in the database. The security of database depends on many factors, including the reliability of the system, the security of the network, the stability of the database itself, etc. Therefore, an actual database faces many uncertainties. At present, the security of the database is achieved by many aspects, including identity verification, data verification, access control, etc.

In traditional medical institution, the medical data was stored in servers and its backup database. The data may be tampered maliciously, and the sharing between different institution is difficult [5]. With the development of medical technology, the sharing of medical data is also facing new requirements. We use the knowledge of blockchain, database, cryptography, and using their advantages to establish a medical information sharing system. This system is similar to a widely distributed resource search engine. We put different medical institution onto a p2p network, then we use a public ledger to store the medical data digests base on blockchain technology. Any node in the p2p network can search medical information on public ledge [6] [7]. The method increases the searching speed of medical information. Meanwhile, in order to increase the transparency of medical data query, we build a secondary chain to store requests.

In this paper, we use the POW as the consensus algorithm. As we know, the POW needs many time to confirmation a transaction. We propose a double-chain structure to store medical data digests and requests. By using the double-chain structure, we can greatly reduce the confirmation time.

2. The model of the medical information sharing system
In this medical information sharing model, in order to realize the distributed storage of medical data digests, we build a p2p network between each node. Figure 2 shows the structure of the p2p network.

The p2p network has 4 characters, the characters include doctor, patient, medical institution and searching database. These four types of characters have different functions in the network.

For medical institution nodes in p2p network, it usually contains some databases [6] [7]. Whenever we want to store a medical data, the medical institution node will extract the key information of the medical data at the same time, and then the key information will be transformed as a transaction. The institution node will submit the transaction to the p2p network and stores it in the corresponding database. By using our algorithm, the transaction will be recorded on the main blockchain, so any node can view the medical data digest. In this way, medical data becomes more opening and shareability.

In this model, some non-medical institution nodes also have databases which are called searching database. These nodes convert the medical data digest in the main chain into a corresponding database operation, and then operate on database. These nodes have an API (application programming
interface), and we can access the searching database and search the medical data in the p2p network by using the API.

For doctor nodes, this type of node doesn’t contain a database, which is mainly used to submit the requests by doctors. When the doctor wants to query some data in database, he will send a request to the p2p network. When the requests reach a consensus by each node, medical institution nodes will check its own database according to the doctor’s request. If there is corresponding medical data, it will be send to the doctor node. In addition, we build a secondary chain to store request information to distinguish the information in the main chain.

The last type of node is patient nodes. This type of nodes also doesn’t contain a specific database, it is mainly used to submit some authorized information. For some private data, the patient will encrypt and store it into the medical institution’s database. In order to access this data for doctor, the patient can submit the doctor’s proxy re-encryption key to the p2p network. The corresponding medical institution will use the proxy re-encryption key to handle the encrypted information, then send the re-encrypted data to the corresponding doctor [8]. Similarly, we store these proxy re-encryption keys in the secondary chain.

3. Medical data storage Model
We divide medical data into two types: medical institution’s data and patient private data. Figure 3 shows the storage method of medical data.

![Figure 3. The storage method of medical data]

The medical institution’s data belongs to medical institution. we store this type of data in the database and submit the data digests to the p2p network.
For private data, its ownership belongs to the patient. We use the owner’s public key to encrypt it, then store ciphertext in the database. Also, we submit the private data digests to the p2p network.

4. An improved pow algorithm

Bitcoin system uses the POW (power of work) as the consensus algorithm [1] [2] [8] [9]. The algorithm generates a block about 10 minutes, people usually think a transaction can be confirmed after 6 blocks, so a transaction needs 1 hour to be confirmed, which greatly reduces efficiency. In the medical information sharing model, we have adopted a double-chain structure to reduce the confirmed time of a transaction. Figure 4 shows the double-chain structure.

![Double-chain structure](image)

**Figure 4.** The double-chain structure

We design a double-chain structure for the medical information sharing model. For the data in the p2p network, there are mainly three types: data digest, request, proxy re-encryption key. We store the data digests in a main chain, which uses the traditional POW algorithm, and a block is generated about 10 minutes. For the remaining request data and the proxy re-encryption key, we build a secondary chain to store them. The secondary chain is generated basing on the main chain. When the main chain is generated, the difficulty level will reduce, and all nodes will continue to calculate proof on the basis of the proof in the main chain. When the next proof is found, the secondary block will be generated, and the information in the main block will be added in the secondary block. In this way, the two blockchains will form a strong coupling relationship and the data in the two blockchains is hard to be changed.

Due to the difficulty is different in the two blocks, so that the generate time will be diverse, and the main chain will use more times than the secondary chain. Considering the requests is less than transactions, we control generated time to 2 minutes of the secondary block. It is worth noting that when the main block is generated, the secondary block will start to be generated immediately. Therefore, in some time, the main block and secondary block are generated synchronously.

Through the design of the improved POW algorithm, there are several advantages:

- Reduce the confirmation time of a transaction. Through the connection between the main chain and the secondary chain, we reduce the confirmation time from 1 hour to 36 minutes.
- We store different data in different chain, which will be more convenient for data processing.
- The double-chain structure makes the data more secure.

5. Medical data encryption and sharing

For medical data, we divide it into two types: medical institution’s data and private data. For medical institution’s data, we mainly store it on the database and submit its digest to the main blockchain, and people can freely access these data through the request to the p2p network.
For private data, it is encrypted by the owner’s public key and then stored in the medical institution’s database, we use the proxy re-encryption to achieve the data sharing [8].

When the patient authorizes the doctor to query his information, the proxy re-encryption key will be sent to the p2p network [10]. After it is verified by the consensus algorithm, and the medical institution will complete the re-encryption operation according to the ciphertext and the proxy re-encryption key, and the ciphertext will be sent to the doctor, by using his private key, so that the doctor can see the specific data. The model uses the LWE (learning with errors) [9] to finish the proxy re-encryption.

1) Generate a random matrix $A \in Z_q^{n \times n}$, select safe integer $q, n$

2) Generate the public key and the private key: public key $pk = P, P = R - A, S \in Z_q^{m \times 1}$, where $R, S$ are gaussian parameters, then the private key is $sk = S$

3) Encryption algorithm:

$$c = (c_1, c_2) = (e_1A + e_2, e_3P + e_3 + m \cdot \begin{bmatrix} q \\ 2 \end{bmatrix})$$

Where $e_1, e_2, e_3$ are error parameter.

4) Decryption algorithm:

$$m = c_1S + c_2$$

Judging from the distance from 0 to select 0 or 1

5) Re-encryption key generation algorithm:

$$rk_{a \rightarrow b} = (P_b, Q)$$

$$Q = \begin{bmatrix} X & -XS_B + E + S_A \\ 0 & I \end{bmatrix}$$

Where $X$ is random matrix and the $I$ is noise.

6) Re-encryption algorithm:

$$(c_1', c_2') = h_1(A, P_b) + (h_2, h_3) + (c_1, c_2) \cdot Q$$

Where $h_1, h_2, h_3$ are from the error distribution.

6. Conclusion

In the medical information sharing system, we combine the knowledge of blockchain, database and cryptography to build a medical information sharing system. By using the system, we can enhance the utilization of medical data and promote the sharing of medical data. It will be greatly beneficial for the development of medicine.

The model also has some disadvantages. Due to the use of the POW, we will waste some computing ability, when the system become bigger, it will waste a lot of resources. In addition, the encode of the medical date digest need the help of the medical professionals.

Acknowledgments

This work is supported by Fundamental Research Special Funds for Central Universities (20826041A4133).

Reference

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [OL]. (2008-10-31) [2016-11-02]. https://bitcoin.org/bitcoin.pdf

[2] D. Vujčić, D. Jagodić and S. Randić, “Blockchain technology, bitcoin, and Ethereum: A brief overview,” 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East
[3] E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalkılıç, “Towards secure e-voting using ethereum blockchain,” 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-7.

[4] L. Mertz, “(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution,” in IEEE Pulse, vol. 9, no. 3, pp. 4-7, May-June 2018.

[5] Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481-494

[6] Merkle R C. A digital signature based on a conventional encryption function. In: proceedings of the 1987 conference on the Theory and Applications of Cryptographic Techniques. Berlin Heidelberg, Germany: Springer. 1987. 369-378

[7] L. Mertz, “Hospital CIO Explains Blockchain Potential: An Interview with Beth Israel Deaconess Medical Center's John Halamka,” in IEEE Pulse, vol. 9, no. 3, pp. 8-9, May-June 2018.

[8] Xue Teng-Fei, Fu Qun-Chao, Wang Cong, Wang Xin-Yan. Medical data sharing model via blockchain. Acta Automatica Sinica, 2017, (9):1555-1562

[9] Aono Y, Boyen X, Phong L T, Wang L. Key-private proxy re-encryption under LWE. In: proceedings of the 2013 International Conference on Cryptology in India. Charm, Germany: Springer International Publishing, 2013. 1-18

[10] R. A. Sarıtekin, E. Karabacak, Z. Durgay and E. Karaarslan, “Blockchain based secure communication application proposal: Cryptouch,” 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-4.