**Abstract**-At present, all medical information systems are managed and operated by medical institutions. In order to protect the privacy of patients, in principle, it is not allowed to transfer and share information outside of medical institutions, except for the patients themselves requesting to retrieve and view their personal information. This medical institution-oriented patient medical information management system will inevitably cause medical Data is scattered in different hospitals, and fragmented medical data reduces the quality of medical services. On the other hand, the demand for medical information in the fields of medical research and artificial intelligence is increasing. There are few data available for medical research, and the reliability of the data is difficult to guarantee. Although a large amount of medical data is generated every day, because the data is scattered in different medical institutions, only a small part of the data is actually available.

Keywords--blockchain; privacy; bitcoin;

1. INTRODUCTION

The rapid development of society, the geometric increase of new medical diagnosis information every day, but at the same time, due to the independence of various medical systems, doctors in different hospitals and even different departments cannot share this medical information, resulting in a waste of resources and increasing the cost of patients. burden. The development and application of blockchain technology provides a new direction for solving the problem of medical data storage and sharing.

Medical BLockchain is an open information service platform developed based on blockchain technology, which can safely integrate and manage medical information generated by various devices including smart phones and scattered in different medical institutions. Medical consumers can set different reading permissions for each personal information according to their needs, so that they have full ownership and control of their own medical information. Medical service providers can record the medical records of medical subjects with the consent of consumers. Enter Medical BLockchain. Individuals, research institutions, or companies who wish to obtain medical information from others can obtain the medical information resources they need after obtaining the consent of the information owner. At the same time, software developers can use the API and SDK provided by the Medical BLockchain platform to create various medical information-based services.

Medical Blockchain is based on a central server and node server architecture. The central server is responsible for accessing the node server, ensuring the data consistency of each node server, and providing support services for synchronizing the blockchain data of the node server. Each node server connects to the central server, sends a block chain increase message to the central server, and then the central server broadcasts to each node server to achieve the purpose of synchronization. Due to the limitations of the broadcasting mechanism of traditional servers, all servers need to broadcast messages to every other server, which requires these servers to be exposed on the World Wide Web. In Medical Blockchain, due to this central server coordinating feature, node servers can achieve information independence from each other and do not know each other's existence, ensuring the independence and privacy of the medical diagnosis process. Each node server independently maintains the doctor and patient information of each medical system. At the same time, it also reduces the difficulty of networking. The node server can selectively sleep according to its own situation, and when it comes online again, it can synchronize data from the central server. The node server provides users with a web access interface, which can be adapted to multiple access devices such as mobile phones and computers.

**Related work.** This system uses python language, based on flask framework, and uses central server and node server architecture to update and maintain the entire medical blockchain. Each node server independently accesses the central server, and the node server provides users with access to web services. Doctors use the platform to view, modify and submit medical information to users. Patients can view their own medical information, and can access the entire blockchain information through different node servers. Medical information uses AES symmetric encryption technology, using the patient's name as the secret key, so that both doctors and patients can view their own medical diagnosis information.

**Our contribution.** Based on the blockchain system, the central server and node server models are used to manage the entire medical blockchain model; traditional blockchains use hash and proof of work to verify the availability of the block, but in this system, no proof of work is required. Only the hash is used to verify the blockchain to avoid unnecessary overhead; due to the uniqueness of the blockchain, the medical diagnosis bill is used to record the doctor's diagnosis of a specific patient, and finally the patient's medical information is summarized in the form of bill; The node server saves doctor information and patient information, and the node servers are isolated from each other to ensure the confidentiality of information between multiple node servers; medical information uses the AES encryption algorithm, and the password uses patient information by default. In the traditional decentralized blockchain system, all nodes responsible for user access need to broadcast their own changes. The central server-node server model adopted in this solution greatly reduces the difficulty of networking and ensures Independence.

**organization.** The second part discusses our privacy issues to resolve this article; the third section outlines the platform, while the fourth section details the technical implementation; the fifth section discusses future expansions. The sixth section finds the blockchain and its conclusions.

1. **THE PRIVACY PROBLEM**

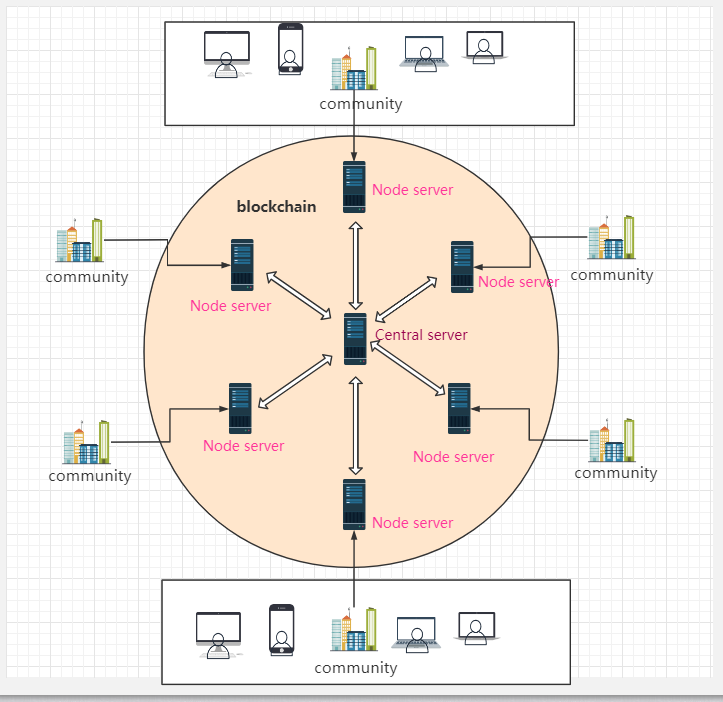
For some intractable diseases, experts in many departments are required to conduct group consultations, or even doctors from different hospitals to conduct simultaneous consultations. However, since each medical system is relatively independent, it is difficult to share medical diagnosis information. In addition, experts need to share various materials during consultation. If a patient goes to a different hospital, he needs to bring his own medical diagnosis information. From the perspective of medical diagnosis, the patient cannot or should not see some medical diagnosis information that is too specific. This requires the new doctor to reconsider Making a diagnosis under the current situation not only increases the probability of misdiagnosis, but also causes a waste of medical resources, and at the same time increases the patient's time and energy input. For some patients who need long-term treatment, doctors often need to prescribe targeted diagnosis and treatment plans through the patient’s past treatment process and medication habits. However, due to the isolation of various medical systems, doctors can only use the medical record card or Patient description, to understand the patient's diagnosis and treatment process locally, and cannot have a relatively complete control of the patient's entire treatment process. For patients, the cost of changing doctors during treatment is relatively high. Blockchain technology can solve the above problems that medical information cannot be shared well due to the independence of medical structures. As a blockchain service center, each medical system records all medical diagnosis information under this system, and records each medication and the current diagnosis and treatment at the same time; the blockchain service center will submit the data update status to the central server, The central server broadcasts the data update message to all node servers registered with the central server. This not only ensures the uniqueness of the blockchain of the entire system, but also synchronizes all blockchain node servers to ensure the data consistency of each node server.

1. **PROPOSED SOLUTION**

We start with a system overview. As shown in Figure 1, the three entities that make up our system are hospitals and community users who are interested in downloading and using; node servers that provide user access services; and provide various node server access systems and synchronization node server functions Central server.

Although users in the system usually retain (pseudo) anonymity, we can store the service configuration on the database of the blockchain node server and verify their identity. The design of the system itself is as follows. Blockchain nodes accept two new transaction types: Taccess, used for access control management; and Tdata, used for data storage and retrieval. It is easy for users to use these network operations to complete the access and modification of the blockchain. At the same time, it provides a resultAPI interface to support dedicated timing services for individual customers.

To illustrate, consider the following example: a user uses an application on our platform to protect her privacy. When a user registers for the first time, a new share (user, generate a service identity and send it along with the associated permissions to the blockchain in the Taccess transaction. The data collected on the server (such as sensor data such as location) uses shared encryption The key is encrypted and sent to the blockchain in the Tdata transaction, which is then routed to a key-value store outside the blockchain, while only keeping a pointer to the data on the public ledger (the pointer is the SHA-256 of the data) Hope value). Both services and users can now use the following methods to query the data associated with pointers (keys) of the Tdata transaction. The blockchain then verifies that the digital signature belongs to the user or service. For services, their permission access data will also be checked. Finally, users can change the permissions granted to the service at any time to issue a Taccess transaction with a new set of permissions, including revoking access to previously stored data. Develop a web-based (or mobile) dashboard that can summarize data and The ability to change permissions is quite trivial, similar to the development of centralized wallets, such as Bitcoin's Coinbase1. Blockchain foreign key value storage is an implementation of Kademilia [16], a distributed hash table (or DHT​​), added Use LevelDB2 and the interface with the blockchain to achieve persistence. DHT is maintained by the node network (may be disconnected from the blockchain network). Read/write transactions. The data is on the node and replicated to ensure high availability. It is an illuminating alternative to Blockchain solutions can be considered for storage. For example, a centralized cloud may be used to store data. Although this requires some level of trust in third parties, it has advantages in scalability and ease of deployment.





IV. THE NETWORK PROTOCOL

Now we describe in detail the underlying protocol used in the system. Use the AES encryption algorithm to encrypt the description items of the block, and hash all the information of the previous block to ensure the uniqueness of the blockchain.

1. *Building Blocks*

Now, we briefly introduce the relevant building blocks throughout the rest of this article. We assume familiarity with Bitcoin [17] and blockchain.

1) Identity: The central server has no user database, only cached blockchain data, and does not perform authority management. The node server has three types of identities, namely doctor, patient, and admin. Patients can only view their own medical data, and have no authority to modify their own medical data and view and modify other medical information. Doctor can view all medical data and make additional changes to medical information. At the same time, the doctor identity also has the authority to increase the patent and doctor. As a super administrator, Admin has the highest level of authority, can access and append all user information.

2) Blockchain storage: Initially, there is only a central server, so the head blockchain node of the blockchain is created by the central server. The hash index field does not include all other data strings in its own field hash value. When a node server is started, the node server automatically registers its information with the central server. Then the central server will automatically send all the block information cached by itself. The node server responds to the central server's add node command, and completes the addition and update of all blockchain information in sequence. At this point, the node server is successfully registered, and normal operations of adding medical information blocks can be performed. Blockchain information is distributed and stored on each node server, independent of each other, and mutual supervision to ensure the uniqueness of the blockchain. In theory, the entire blockchain information does not include the blockchain information stored by the central server. The blockchain information of the central server is only used as a distribution cache, but the central server is also essential. Decentralization, as the name suggests, is to remove the central server, but because each node server may be in different network segments, it is difficult to achieve information intercommunication, and it is also to form the island effect of a single node server.

3) Strategy: A set of permissions granted to the service by user u, represented by POLICYu, s. For example, if you have a mobile phone

Need to access the user's location and contact application, then policy u, s = {location, contact}. Please note that any type of data can be safely stored in this way, assuming that the service will not break the protocol and the tag data is incorrect. A safeguard measure that can partially prevent this from happening is introduced into the mobile SDK, but in any case, the user can easily detect the deceptive service because all changes are visible to her.

4) Auxiliary function: Parse (x) deserializes the message sent to the transaction, which contains parameters; the CheckPolicy (pksig k, xp) shown in protocol 2 verifies that the initiator has the appropriate authority.

B. Blockchain protocol

The patient’s PHR information contains information about the patient’s identity, gender, age, clinical diagnosis, medication use, etc. In order to achieve effective sharing of medical data while protecting patient privacy, we classify the sensitivity of the patient’s PHR information in the form of key-value pairs. Information of different sensitivity levels is stored, and different access rights are given to different keys to ensure that only the data owner (patient) or the applicant authorized by the data owner can obtain complete PHR information. In order to achieve efficient medical data sharing, different access rights are controlled through hierarchical encryption and key management. Authoritative nodes on the alliance chain can access part of the patient's medical information without sending data requests to the patient. In order to protect the patient's Privacy, which does not contain patient identification information.

C. Privacy and security analysis

First, the characteristics of the blockchain enable data to be transmitted in ciphertext, and during the data transmission process, the data owner sends and receives data packets through its address in the blockchain. Due to the anonymity of blockchain accounts, users cannot obtain the true identity of the other party during data sharing. Second, this article uses Algorithm 3 to encrypt the keyword index, and no electronic medical record information about the data owner will be displayed during the keyword search. Third, this article uses proxy re-encryption technology to ensure the privacy of user data during data sharing. A legitimate user wants to obtain the electronic medical record stored in the blockchain by the data owner. First, after obtaining consent, encrypt himself, and generate a new composite identifier for each user service pair to ensure that only a small part of the data The adversary obtains two signature and encryption keys at the same time. If the opponent only gets one key, the data is still safe. Note that in practice we can further separate the identity to limit the identity of a single compromised compound. For example, we can generate a new key for every one hundred records stored. In this section, we briefly introduced possible ways to expand the blockchain in the future. These can play an important role in shaping a more mature distributed trusted computing platform, rather than the current most advanced system. More specifically, they will greatly improve the platform proposed earlier.

A. From storage to processing

One of the main contributions of this article is to demonstrate how to overcome the publicity of the blockchain. So so far, our analysis has focused on storing pointers to encrypted data. Although this method is suitable for storage and random queries, it is not very effective for processing data. More importantly, once the service queries some raw data, it can be stored for future analysis.

A better way may be to never let the service observe the original data, but allow it to run calculations to obtain the final result directly on the network. If we split data sharing (for example, using Shamir's secret sharing [23]), instead of encrypting them, then we can use secure multi-party computing (MPC) to safely evaluate any function.

In Figure 2, we illustrate how MPC relates to blockchain, especially in our framework. Consider a simple example in which a city holds elections and wishes to allow online secret voting. It has developed a mobile application to use our system to vote, and now it has enhanced the MPC function with suggestions. After the online election took place, the city then submitted its back-end code summary results. The network selects a subset of nodes randomly, and the interpreter converts the code into a secure MPC protocol. In the end, the result is publicly stored in the ledger, which can be safely prevented from tampering. As a result, no one can understand what a personal vote is, but everyone can view the results of the election.

An example of a secure calculation process in a blockchain network. The upper left block (EVote process) is an insecure code, the parameters (\*) in which are marked as private, and are stored as shared in the DHT. The network randomly selects a subset of nodes to calculate the secure version of EVote, then broadcasts the result back to the entire network, and then stores it in the ledger.

B. Trust and decision-making in the blockchain

The POW consensus algorithm is extremely safe. If you want to destroy the system, you need to master 51% of the system's computing power to ensure system security. However, the node server needs to consume a lot of resources to store data, and the data takes a long time to enter the chain, which is important for medical data storage and sharing. For the platform, this will cause unnecessary waste of resources. The POS consensus mechanism reduces the dependence on computing power, but the medical data platform itself does not generate and use tokens, and the POS mechanism is easy to cause centralization and increase security risks. DPOS further reduces resource waste, and the mechanism of agents taking turns on duty reduces centralization risks and strengthens system security.

**VI。CONCLUSION**

The decentralization and anti-tampering characteristics of blockchain technology make it very suitable for sharing medical data. The author proposes a blockchain-based electronic medical record sharing model, which is suitable for users in different medical institutions to share their own electronic medical records conveniently, anonymously and safely. First of all, two types of blockchains are introduced and designed. In addition, the distributed key generation technology is combined with the type and identity-based proxy re-encryption scheme to realize the secure sharing of data between users, using the DPoS consensus algorithm Maintain the blockchain. In this solution, the data owner implements fine-grained access control strategies by classifying the types of electronic health records. Finally, it analyzes the anti-tampering, data protection and response to security protocol attacks, and evaluates the performance of this scheme in terms of communication overhead and computing overhead. The results show that this scheme can well meet various requirements such as privacy and sharing, and the computing power demand and communication cost are lower than existing schemes. However, the model in this paper only analyzes and improves on security and performance, and does not consider reducing storage overhead and improving consensus efficiency. In future work, more comprehensive and in-depth research can be conducted on this.

REFERENCES

1. Craig Gentry. Fully homomorphic encryption using ideal lattices. In STOC, volume 9, pages 169–178, 2009.
2. Scaling the facebook data warehouse to 300 pb, 2014.
3. Rt.com. Obama announces legislation protecting personal data, student digital privacy, 2015.
4. M. Rosenfeld, “Analysis of hashrate-based double spending,” CoRR, vol. abs/1402.2009, 2014.
5. J. Barcelo. (2014). User Privacy in the Public BitCoin BlockChain.Accessed: Dec. 12, 2018. [Online]. Available: <https://goo.gl/mN2y6V>
6. Dajie Ltd. Website. Accessed: Dec. 12, 2018. [Online]. Available:www.dajie.eu
7. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013.
8. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission anagement,” in Proc. Int. Conf. Open Big Data (OBD), 2016, pp. 25–30.
9. Y. Lewenberg, Y. Sompolinsky, and A. Zohar, “Inclusive block chain protocols,” in Proc. Int. Conf. Financial Cryptography Data Security, 2015, pp. 528–547.
10. Internet of Things Companies: The Biggest IoT Directory. Accessed: Dec. 12, 2018.
11. A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, “Is bitcoin a decentralized currency?,” IEEE Security Privacy, vol. 12, pp. 54–60, May 2014.
12. M. Rosenfeld, “Analysis of hashrate-based double spending,” CoRR, vol. abs/1402.2009, 2014.