

Design of a Smart Contract for Medical Records Based on Blockchain

Junran Zhang*

Department of Electronic & Information Engineering, Beijing University Of Technology, Beijing, China

*Corresponding author: junran.zhang@ucdconnect.ie

Abstract. In today's medical field, an ever-increasing number of different medical institutions begin to share patients' cases. Although this provides convenience for patients to seek medical advice, it will also lead to the problem of data abuse, and the patient's medical records are also at risk of being leaked or tampered with. The decentralization, non-tampering, openness, transparency, and traceability of blockchain technology can effectively solve these problems. This paper mainly studies a kind of medical records electronic contract which can guarantee the authenticity, security, and security of medical data. Firstly, patients own their medical records, and their medical data can be stored on the blockchain. The certificates of doctors and patients will also be stored on the blockchain. Secondly, the identities of doctors and patients need to be double verified in the storage process to ensure the authenticity and reliability of the data on the chain. Finally, the performance of a smart contract is evaluated by experiments. The smart contract studied in this paper can assure that large-scale medical data can be effectively stored and ensure the security of electronic medical records. And it can realize the sharing and reading of medical information between different hospitals.

Keywords: Blockchain technology; medical data protection; smart contract.

1. Introduction

In recent years, with the continuous growth of China's population and the durative optimization of the medical security system, the number of medical records has also increased significantly [1]. Due to the rapid development of information technology and network technology in the medical field, large quantities of medical institutions have used electronic equipment to record medical data. The number of electronic medical records is increasing year by year, and the modern management of hospital medical records has become an inevitable trend. The physical address of electronic medical record files is mostly stored in the server controlled by HIS (hospital information management system), and the data between various medical institutions are not interconnected, which brings inconvenience to patients when they visit different medical institutions [2]. To further facilitate the medical treatment of patients, hospitals in many places across China have implemented the sharing and reading of electronic medical records. However, in today's society, the security, authenticity, and validity of online information cannot be guaranteed to a certain extent. The networking of medical information has the following two problems. First, the traditional electronic medical records sharing platform stores the user's account, password, and password verification program on the central node server. If the server is attacked and the password is tampered with, the user's medical records and other personal information will be exposed [3]. Second, due to the lack of supervision, false medical advertisements are prevalent on the Internet. Some people use forged patient identities and fake medical records to advertise medical products or medical institutions for illegal profits, which makes it difficult to guarantee the authenticity and effectiveness of medical information on the network. Therefore, it is necessary to build a medical record system with information security and real data. In today's information technology, blockchain is tamper-proof and has related functions that can guarantee the authenticity and security of data. Therefore, the application of blockchain technology in the medical field can more effectively help hospitals and patients store medical records and electronic medical records.

Blockchain technology is a multi-person shared transaction recording platform that uses a blockchain data structure to verify and store data and reach a consensus of multi-party trust [4]. Distributed node consensus algorithms are used to generate and update data on the blockchain, and cryptography is applied in the blockchain to protect users' data security. Transactions based on blockchain will be recorded. The non-tampering and non-deletion of blockchain information enable the realization of information sharing and consistent decision-making among multiple subjects, to ensure the openness and transparency of the identity of each subject and the transaction information between subjects.

The smart contract is a computer protocol that can be propagated and used to verify or execute contracts [5]. It is equivalent to an automatically executed contract, which is executed through code without human participation [6]. Smart contracts are written into specific blocks of the blockchain in code through node consensus. Contract code encapsulates contract rules and scenarios that trigger contract execution. After submitting the smart contract and obtaining the returned contract address and other information, the user can initiate a transaction to call the contract. The operation principle of a smart contract is shown in Figure 1.

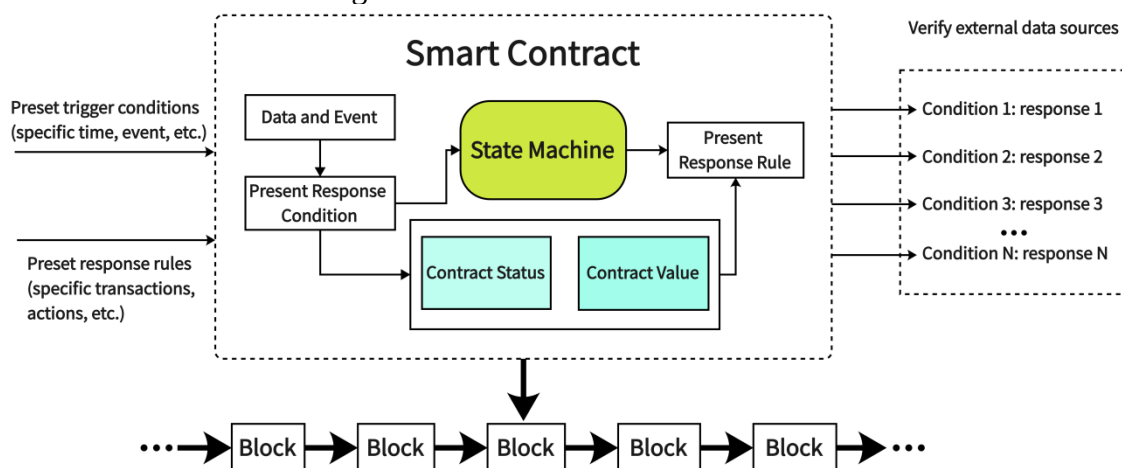


Fig. 1 Smart contract operation principle

To ensure the authenticity of medical data, improve the security of medical data, and solve the problem that medical data cannot be interconnected, this paper designs an electronic medical record smart contract based on the Hyperledger Fabric platform through blockchain technology. The smart contract is mainly composed of two parts, the first part is registration and certificate storage, and the second part is data generation and verification. After simulating the case information and testing the smart contract, it is found that the smart contract has high storage efficiency and meets the user requirements.

The second section of this paper introduces the framework of the medical record model and describes the design process of the smart contract in detail. The third section introduces the consensus mechanism selected in this paper, analyzes the choice of consensus algorithm, simulates the smart contract, and evaluates its performance. The fourth section summarizes the full text, analyzes the current shortcomings of the project, and puts forward future improvements to the project.

2. The architecture of Blockchain Based Medical System

2.1. Overall Framework of the Medical Records Model

The medical record model proposed in this paper is an alliance chain composed of multiple hospitals. The model is mainly composed of six entities: regulators, medical institutions, patients, doctors, alliance chains, and other users. All alliance chain members work together to maintain the entire alliance chain. The medical record model is shown in Figure 2.

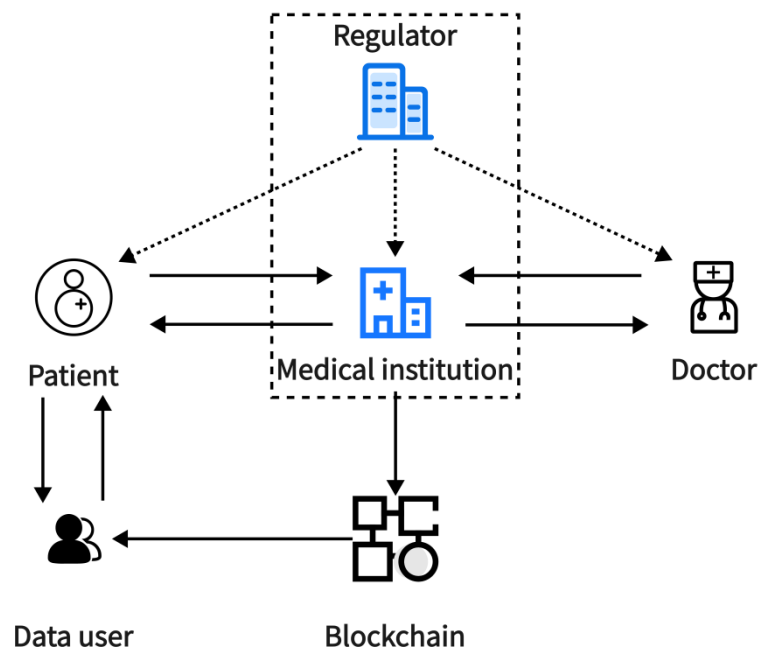


Fig. 2 Framework of the model of the medical record

(1) Regulator: Issue registration certificates to doctors, patients, and medical institutions who join the alliance chain and register for the first time, and serve as the supervision department of the medical data sharing process to supervise and manage the relevant data of patients, doctors, medical institutions and other users. By default, the regulator can be fully trusted.

(2) Medical institutions: Medical institutions refer to all hospitals that join the alliance chain. Medical institutions generate medical data, encrypt the data after being authorized by patients, and store the medical data in the alliance chain.

(3) Patients: Owner of medical data. Patients can selectively share medical data with other data users, and only patients who join the alliance chain network have access to the network.

(4) Doctors: Doctors can generate medical data after diagnosing patients and upload the generated medical data to medical institutions for further verification.

(5) Alliance chain: The nodes of the alliance chain are composed of multiple medical institutions and insurance companies and are jointly maintained. The alliance chain network is responsible for storing the uploaded medical data to ensure the authenticity of the medical data and prevent the medical data from being tampered with maliciously.

(6) Other users: If other users want to obtain the medical data of a patient, they need to obtain the authorization of the patient to access the data. Patients can also set their medical data to be visible to specific user groups.

There are six steps for medical records from generation to uploading and storage, and then to subsequent access.

Step 1. Doctor registration. Doctors provide their identity information and submit registration applications to their medical institutions. After the regulatory department and the medical institution check the identity and qualification of the doctor, the medical institution returns the relevant private key of the doctor and stores the corresponding certificate on the chain.

Step 2. Patient registration. The patient submits the registration application when seeing a doctor. After the medical institution verifies that the identity is correct, the medical institution returns the relevant private key of the patient and stores the corresponding certificate on the chain.

Step 3. Medical record generation. The patient visits the doctor first. After the doctor completes the diagnosis, the doctor edits the medical record of the diagnosis and generates the patient's case information. For the medical record to be effective, the medical record must also include the signature of the patient and the signature of the doctor.

Step 4. Authentication. Doctors send medical data to medical institutions for verification. First, the medical institution invokes the smart contract to verify the doctor's identity. If the verification fails, an error will be reported and the error result will be returned. If the verification succeeds, the patient's identity will continue to be verified. When verifying the identity of the patient, if the verification passes, the medical data will be regarded as valid data, stored and waiting for uploading. If the verification fails, an error will be reported and the error result will be returned.

Step 5. Data storage and upload. The medical institution will verify the effective medical data storage and upload it to the blockchain.

Step 6. Patient access to medical records. Patients can log in and query their medical records, and after being authorized by other patients, they can view the case information of relevant patients according to the specific ICD code.

2.2. Smart Contract Overview and Workflow Design

This paper designs the corresponding smart contract based on the above medical record model. To simplify the design, the smart contract combines the regulator and hospitals into medical institutions. The flow chart of the smart contract is shown in Figure 3.

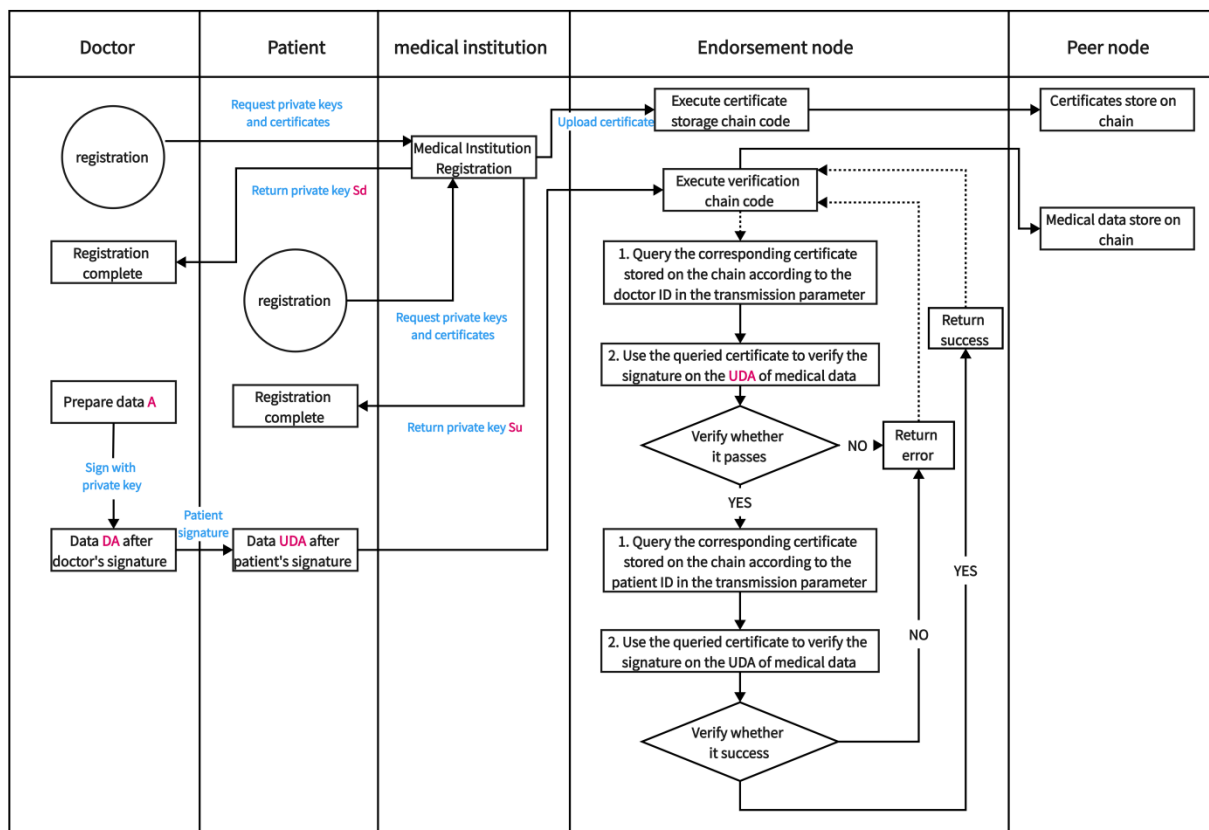


Fig. 3 Flow chart of smart contract

2.2.1 Registration and deposit certification

Doctors and patients first need to register in medical institutions. When registering, it will involve certificate storage. The relevant ID and certificate of the doctor or patient are required in the process of certificate storage. The certificate will first be converted into JSON format during the certificate deposit process. Then it will judge whether the ID of the registrant already exists. If the ID already exists, the registered ID will be returned. If the registrant is a new user, the user will be registered and its ID and certificate will be stored on the blockchain. The registration data includes the identity ID and the contents of the certificate.

2.2.2 Medical data

In the smart contract, medical data is divided into medical signature metadata, namely attribute data and signature data, and ID data of doctors and patients. Medical signature metadata includes hospital name, doctor name, patient gender, patient age, patient ICD, patient symptoms, treatment plan, medication, and timestamp. All medical data will be stored online. Medical data can only take effect with the signatures of both patients and doctors.

2.2.3 Authentication

In the authentication process, the received json string is first parsed to get the ID and the structure of the certificate of the patient and doctor. Then, use the ID in the medical data to find the certificate of the corresponding doctor and patient on the blockchain. Next, decompile the certificate and pass X.509 cryptographic algorithm parses the certificate content and obtains the certificate content of doctors and patients. Finally, SHA 256 algorithm is used to calculate the hash value of the signature. Pass in the public key, the signature in the medical record, and the hash value of the signature, and verify the signatures of doctors and patients through the ECDSA algorithm. The verification will pass only when the signatures of doctors and patients are correct. If the signature verification of the doctor or patient fails, an error will be returned. After the verification, the medical data will be stored on the blockchain. The certificates of doctors and patients are stored on the blockchain at the time of registration, which is easy to find as a searchable certificate.

3. Program Evaluation

3.1. Choice of Consensus Mechanism

The core of a blockchain network is a distributed ledger, which records all transactions on the network. The process of keeping the ledger synchronized throughout the network is called consensus [7]. That is, multiple nodes reach a consensus on a certain date, and multiple nodes reach a consensus on the order of multiple data. The nodes here can be any computer equipment, such as a PC, laptop, mobile phone, router, etc. the data here can be transaction data, status data, etc. The consensus algorithm can make the computer group work together and can tolerate the failure of some member hosts. Generally speaking, the failure of the host will be treated in two ways: Byzantine failure and non-Byzantine failure [8]. The Raft consensus algorithm selected in this paper is a consensus algorithm that supports non-Byzantine faults. The raft can guarantee that in the case of non-Byzantine failure of some nodes in the system, the system can still process the requests of clients. Raft is a consensus algorithm for managing replicated logs [9].

3.1.1 Raft node status and leader election

In the Raft algorithm, each node can only be in one of three states: follower, candidate, and leader.

Follower: Initially, all nodes are followers. The followers receive the replication logs from the leader and perform corresponding actions as required by the leader. When the followers do not receive the heartbeat message from the leader within a certain period, they will change their status as candidates and run for leadership.

Candidate: candidates will be elected, and the candidate node with the most votes will become the leader.

Leader: as the node with the highest status, the leader is responsible for receiving calls from clients, organizing log replication to other nodes, and coordinating and managing the whole computer cluster.

The candidate will return to the follower if the leader node has been selected. Similarly, if the leader finds that the term value of another leader node is higher, it will also return to the follower.

Raft divides the system time into logical segments. Each logical segment is called a term. The term can be any length. Each term begins with the election and ends before the next term.

Raft uses the heartbeat mechanism to select the leader. In the beginning, all nodes are followers. Followers will maintain the follower state only if they can receive valid RPC heartbeat messages from

the leader or candidate [10]. The leader will send heartbeat messages periodically. If there is no leader, the node with the smallest waiting timeout will increase its term number and recommend itself as a candidate. First, the candidate votes for itself, and then send an RPC message requesting voting to other nodes, asking them to select it as the leader. The candidate node will remain until a node wins the election or no node wins the election. Each node can only cast one vote. If a candidate wins most of the votes during the election time, it will become the new leader in this term. If at the same time, the other node announces that it is the new leader and has higher tenure values, then the nodes with higher tenure values become the new leader. If the votes of multiple candidates are the same, no node will win. The leader will be re-elected every once in a while. The leader node election process of the Raft algorithm is shown in Figure 4.

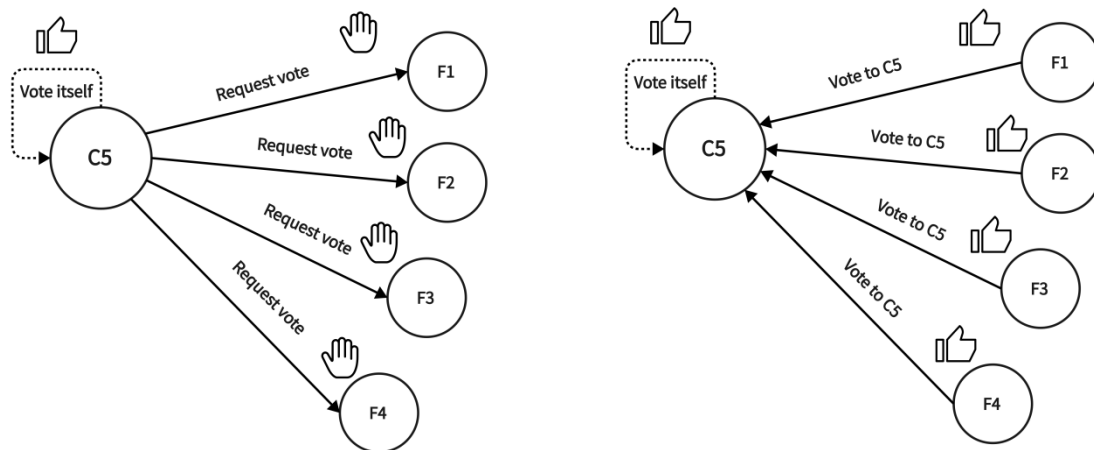


Fig. 4 Leader election process of Raft algorithm

3.1.2 Analysis of algorithm selection

This paper uses the Raft consensus algorithm which can not tolerate Byzantine failures. The reason lies in the compromise between the complexity and security of the system. Assuming that there may be Byzantine faults on n nodes in a system at the same time, Byzantine fault tolerance requires the existence of more than $3n+1$ nodes in the system [11]. For example, to deal with 100 potential malicious nodes, at least 301 nodes need to be deployed. This will make the system more complex and consume more resources. When dealing with n non Byzantine fault nodes, the Raft algorithm only needs $2n+1$ nodes [12]. Considering that the model is in the alliance chain environment. To improve safety, the digital certificates will be used to protect users' data, so malicious nodes are unlikely to occur. Therefore, the Raft algorithm with relatively lower complexity and the cost is selected.

3.2. Performance Evaluation of the Smart Contract

For the Raft algorithm, if the total number of nodes is n , for the logging stage, the number of the communication will be $n-1$, for the data submission stage, the number of the communication will also be $n-1$, and the number of the total communication is $2n-2$, so the Raft algorithm's complexity is $O(n)$ [13]. Although the number of consensus communication of the Raft algorithm is small, the Raft algorithm can not identify Byzantine nodes, so there is still a certain risk [14].

To better evaluate the medical record model designed in this paper, the relevant experimental simulation is carried out on the designed smart contract. The hardware environment of the experiment is as follows: the CPU is Intel (R) core (TM) i7-9750h CPU @ 2.60GHz, RAM 16 GB. The experimental environment is constructed as follows: install ubuntu-22.04 on VMware® Workstation 16 Pro 16.2.3, take hyperledger fabric as the simulation platform, and all the codes are implemented in Go programming language. In the process of generating medical data, medical data needs the signatures of patients and doctors to take effect. Therefore, in the verification process, the signatures of doctors and patients need to be verified. Zhou et al. [15] recorded the encryption time and

decryption time of medical data and analyzed the efficiency of smart contracts according to the required time. This paper simulates the change of verification time with the increase of medical data when verifying the signatures of doctors and patients in smart contracts. The number of medical data increased from 9 to 45, and the increment of each test was 9. The test results are shown in Figure 5.

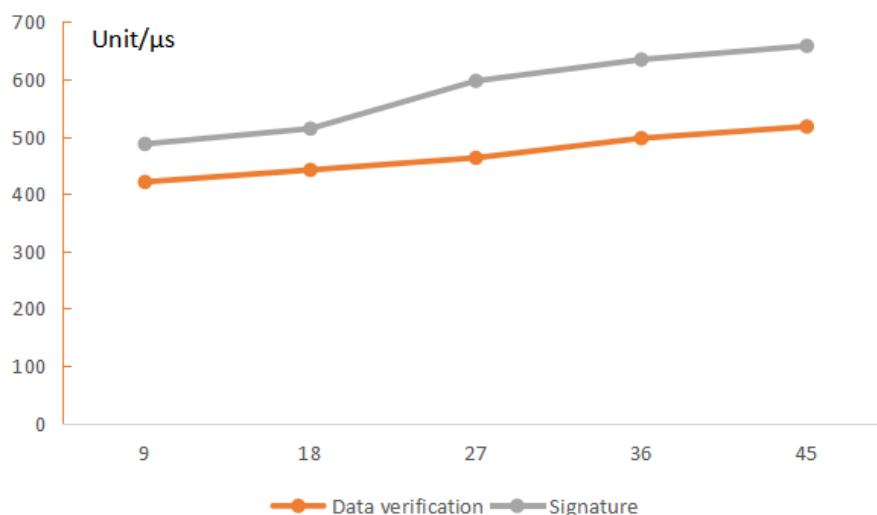


Fig. 5 Signature and data verification time consuming

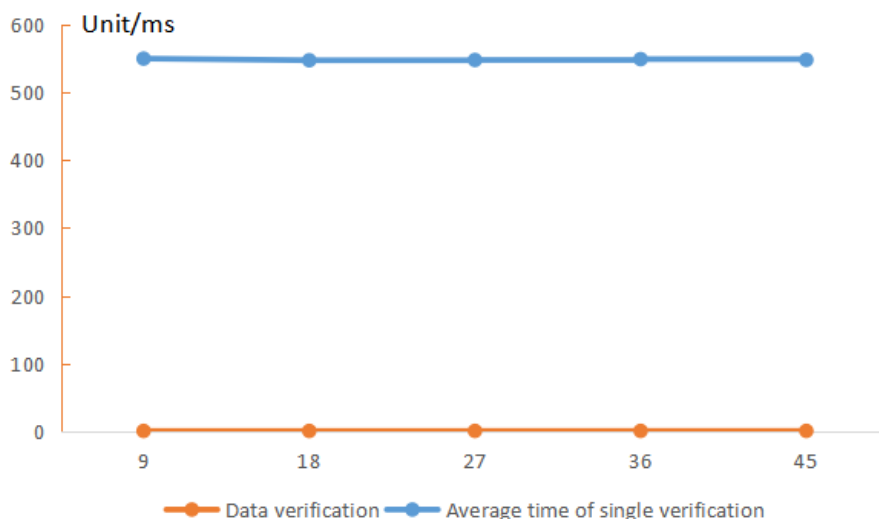


Fig. 6 Average time of single verification

Chen et al. [16] recorded the total time spent to complete a data writing and the time spent to query a single data in the cross-domain authentication of the medical alliance chain and compared the time spent on these two functions. Figure 6 shows the change in the average time-consuming of a single recorded case with the increase in medical data. The change of the time required for verification is also added to the line chart as a comparison. To better fit the practical application, doctor authentication and patient authentication are combined into one step in the smart contract code, which improves the efficiency of authentication. When recording the verification time, it does not include the time to resolve the certificate. It can be seen from Figure 5 and Figure 6 that the time-consuming of each item is in microseconds and milliseconds. With the increase in the number of medical records, the time to verify the identity of doctors and patients also increases, and the average time-consuming of a single recorded case is basically the same. The smart contract can ensure that the uploading time of medical data of a single patient is within 0.6s, which shows that it can guarantee the authenticity of medical data and quickly save or obtain medical records.

4. Summary

Based on blockchain technology, this paper proposes a smart contract for electronic medical records, which effectively ensures the authenticity and effectiveness of medical records through the dual identity authentication of doctors and patients, realizes the safe storage of medical data and reduces the storage pressure of local data. Then, by creating medical records and recording the time spent on verification and signature and the average time spent on recording a single case, the smart contract in this paper was tested to verify its applicability to the smart contract.

However, the research of this paper still has some limitations. First, the RAFT consensus algorithm can not tolerate Byzantine fault, so there are still deficiencies in the security of the model. Secondly, at present, users can only select the electronic medical record to be visible to specific groups when uploading medical data, and convenient data access and user communication have not been achieved. In future research work, how to improve the consensus algorithm so that it can minimize the computational complexity when identifying Byzantine nodes, and how to better realize the authorization and data access between patients will be considered.

References

- [1] Wang, R. J. , et al. "Medical Blockchain of Privacy Data Sharing Model Based on Ring Signature." *Journal of University of Electronic Science and Technology of China* (2019).
- [2] Durneva, Polina , K. Cousins , and M. Chen . "The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review." *Journal of Medical Internet Research* 22.7(2020):e18619.
- [3] Liu, Z. H. , et al. "Research on Secure Storage of Medical Data Based on Blockchain." *Chinese Medical Equipment Journal* 40.3(2019):4.
- [4] Swan, M. . *Blockchain: Blueprint for a New Economy*. O'Reilly, 2015.
- [5] Szabo N. Smart contracts: building blocks for digital markets. Accessed: Jun. 5, 2022. [Online]. Available:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
- [6] Clack, C. D. , V. A. Bakshi , and L. Braine . "Smart Contract Templates: foundations, design landscape and research directions." (2016).
- [7] Cachin, C. , and M. Vukoli . "Blockchain Consensus Protocols in the Wild (Keynote Talk)." (2017).
- [8] Lamport, L. , R. Shostak , and M. Pease . "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems* 4.3(1982).
- [9] Yang, W. , Garg, S. , Huang, Z. , and Kang, B. "A Hybrid Consensus Algorithm for Master-slave Blockchain in a Multidomain Conversation System." *Expert Systems with Applications* (2022).
- [10] He, C., Xiao, B., Chen, X. et al. *Federated Learning Intellectual Capital Platform*. *Pers Ubiquit Comput* (2021).
- [11] Gramoli, and Vincent. "From blockchain consensus back to Byzantine consensus." *Future Generation Computer Systems* (2017):S0167739X17320095.
- [12] Ongaro, D. , and J. Ousterhout . "In search of an understandable consensus algorithm." *USENIX Association* (2014).
- [13] Liu, C. , Guo, S. , Guo, S. , Yan, Y. , Qiu X. , and Zhang, S. "LTSM: Lightweight and Trusted Sharing Mechanism of IoT Data in Smart City." *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5080-5093, 2022.
- [14] Buttar, H. M. , et al. "Countering Active Attacks on RAFT-based IoT Blockchain Networks." (2022).
- [15] Zhou, Z. Q. , et al. "Medical Data Security Sharing Scheme Based on Alliance Chain" *Journal of Applied Sciences* (2021).
- [16] Chen, Y. B. , et al. "Design of Cross-domain Authentication Scheme Based on Medical Consortium Chain." *Computer Science* (2022).