Quality Improvement Study

Medicine

OPEN

Security research of blockchain technology in electronic medical records

Jia Qu, MS[a,*]

Abstract

Background: A blockchain-based Electronic Health Record(EHR) data-sharing scheme was proposed to solve the problems of data sharing difficulties and privacy disclosure.

Methods: This paper designs a blockchain-based electronic health record model based on the characteristics of blockchain antitampering, decentralization, and distributed storage. Utilize blockchain network and distributed database to store encryption-related access control policies to prevent EHR data from being tampered with and leaked. Data security sharing protocol combines Distributed Key Generation (DKG) and reencryption.

Results: The protocol used the Delegated Proof of Stake(DPOS) algorithm to select the proxy node, which reencrypted the EHR to share data between a pair of users. Simulation experiments and comparative analysis showed that DPOS efficiency was higher than Proof of Work (POW) and slightly lower than the Practical Byzantine Fault Tolerance(PBFT).

Conclusions: The scheme proposed in this paper is more decentralized and less computationally intensive.

Abbreviations: DKG = distributed key generation, DPOS = delegated proof of stack, EMR = electronic medical record, HER = electronic health record, PBFT = possible byzantine fault tolerance, PKG = private key generation, POS = proof of stack, POW = proof of work.

Keywords: Blockchain, Data sharing, Distributed key generation, DPOS, Electronic medical records, PBFT, POW

1. Introduction

With the rapid development of the medical industry and the rapid increase in medical health data, many hospitals have begun to use Electronic Health Record (EHR)[1] to record patients' medical health data. Electronic medical records have many benefits, such as providing a convenient storage method for medical data, a data source for doctors to prescribe, and research data for research institutions. Usually, a patient will generate his electronic medical record after seeking medical treatment in 1 hospital. Previous medical records or data are often needed when the patient seeks medical treatment in another hospital. At this time, electronic medical records must be shared among different medical institutions. Due to the various medical data types, it is always a research hotspot to integrate and store them reasonably and share them effectively. Simultaneously, the electronic medical record contains a lot of private information of the patient, preventing the leakage of private data when sharing, which is also a research problem.

The development of cloud computing.[2,3] Provides an exemplary method for EHR sharing. Usually, hospitals will outsource EHR to a cloud server. When other users want to obtain individual medical records on the cloud, they need to be verified by the cloud. After the verification is passed, the cloud will share the data with the user; but a cloud-based EHR sharing scheme.[4,5] It also has a drawback: data storage centralization. This also means that all medical data is stored in the cloud. Once the cloud server is maliciously hacked, the medical data stored on the cloud will be leaked, resulting in problems such as disclosing user privacy. The consequences are very serious.

The development and application of blockchain technology.[6–8]have brought new opportunities to solve this problem. In 2008, Satoshi Nakamoto published the paper "Bitcoin: A peer-to-peer electronic cash system,"[9] which mentioned the blockchain technology based on Bitcoin. This technology immediately attracted widespread attention once it was proposed. Blockchain technology has the advantages of decentralization and distributed storage, nontampering, etc., and can provide higher security. Based on the benefits of this technology, researchers gradually began to use blockchain technology to build EHR sharing systems.[10–13] Xia et al proposed a blockchain-based medical data sharing model MeDShare.[14] The system uses blockchain to store medical data packets and smart contracts to track all data operations. Once malicious behavior is detected, it can be revoked in time. Access authority to data; according to the access authority, the legitimacy of the data requester's identity is verified, and data security sharing can be realized after verification to prevent data privacy leakage. Fan et al proposed the

Funding: The author(s) received no financial support for the research, authorship, and/or publication of this article.

The authors declare that they have no conflict of interest.

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Ethical approval/patient consent: Not applicable.

[a] Hebei Petroleum University of Technology, Information center, Hebei Petroleum University of Technology, Chengde, China.

**Correspondence: Jia Qu, Information center, Hebei Petroleum University of Technology, Chengde 067000, China (e-mail:15696966@qq.com).*

How to cite this article: Qu J. Security research of blockchain technology in electronic medical records. Medicine 2022;101:35(e30507).

Received: 2 October 2020 / Received in final form: 2 August 2022 / Accepted: 5 August 2022

http://dx.doi.org/10.1097/MD.0000000000030507

MedBlock solution, which uses the blockchain's distributed ledger to achieve effective Electronic Medical Record (EMR) access and retrieval and to share electronic medical records among authorized users.[15] Encryption strategies are used in the scheme to ensure the security and privacy of information while reducing costs; as the scheme improves the consensus mechanism, it effectively enhances block consensus efficiency. Besides, Zhang et al proposed a blockchain-based personal health record sharing scheme[13]; this scheme constructs 2 different blockchains to realize the safe sharing of medical data. The scheme constructs a private chain and a consortium chain, respectively. The private chain realizes the encrypted storage of personal medical data. The alliance chain saves the security index corresponding to the personal medical data and secures data sharing by verifying the doctor's identity token, which protects medical privacy data, but uses 2 types of zones. Blockchain will not only increase costs, but its execution efficiency will also decrease.

This article proposes a blockchain-based electronic medical record security sharing solution. This article's solution is improved on the model presented in the reference "Towards blockchain-based scalable and trustworthy file sharing",[16] and a data security sharing protocol is designed. The protocol combines the Distributed Key Generation (DKG) technology.[17,18]and the reencryption scheme.[19] Compared with the traditional identity-based encryption scheme, the scheme in this paper does not use Private Key Generation (PKG) to generate the master key but uses DKG technology to allow users of each institution to negotiate to generate a private key, which not only prevents the private key of each institution when the PKG is maliciously compromised. The key leakage problem also effectively resists collusion attacks among users. The scheme adopts reencryption technology and, based on ensuring the confidentiality, integrity, and privacy of the EHR, it realizes the sharing of encrypted data between a single pair of users.[20]

2. Methods

2.1. reEncryption

reencryption is a conversion mechanism used between ciphertexts, initially proposed by blaze.[20] reencryption is used to solve the inconvenience when users share data. While reducing the burden on users, it can also enhance the reliability and security of data. In the reencryption process, each participant cannot obtain any plaintext messages. The specific work process involves 3 roles: data owner, data user, and agent. When the data owner Alice wants to share the encrypted file with the data user Bob, Alice generates a reencryption RE key for Bob and transmits the proxy key to a third-party semitrusted agent through a secure channel. The user uses the proxy key to reencrypt the encrypted file according to the proxy reencryption algorithm. After Bob obtains the reencrypted file, he can use his private key to decrypt the reencrypted file, and the plain text file can be obtained after decryption.

2.2. Blockchain-based electronic medical record sharing model

This solution's model improves on the reference "Towards blockchain-based scalable and trustworthy file sharing".[16] The original model consists of data owners, users, storage providers, agents, and miners. This model is shown in Figure 1 (Blockchain-based electronic health record sharing model), mainly composed of 4 roles: N authoritative centers, data owners, data users, and agents. N authoritative centers are our newly added roles, and the remaining roles are originally included in the original model. N authoritative centers constitute blockchain nodes composed of hospitals, banks, insurance companies, research institutes, etc., within an alliance organization, and each node can play at least 1 role. References "Towards blockchain-based scalable and trustworthy file sharing"[16] model. The storage data provider can only store the EHR data of 1 medical institution. The blockchain node is composed of a single node with high access pressure. This solution model The blockchain node is composed of N institutions, which can effectively alleviate blockchain access pressure. This model uses a distributed database and blockchain to store medical data together; the database stores encrypted EHR. The blockchain stores the corresponding access control strategy of the EHR, the storage address on the database, and the data hash of the EHR. Adopting this storage mode solves not only the problem of centralized data storage in the databases of

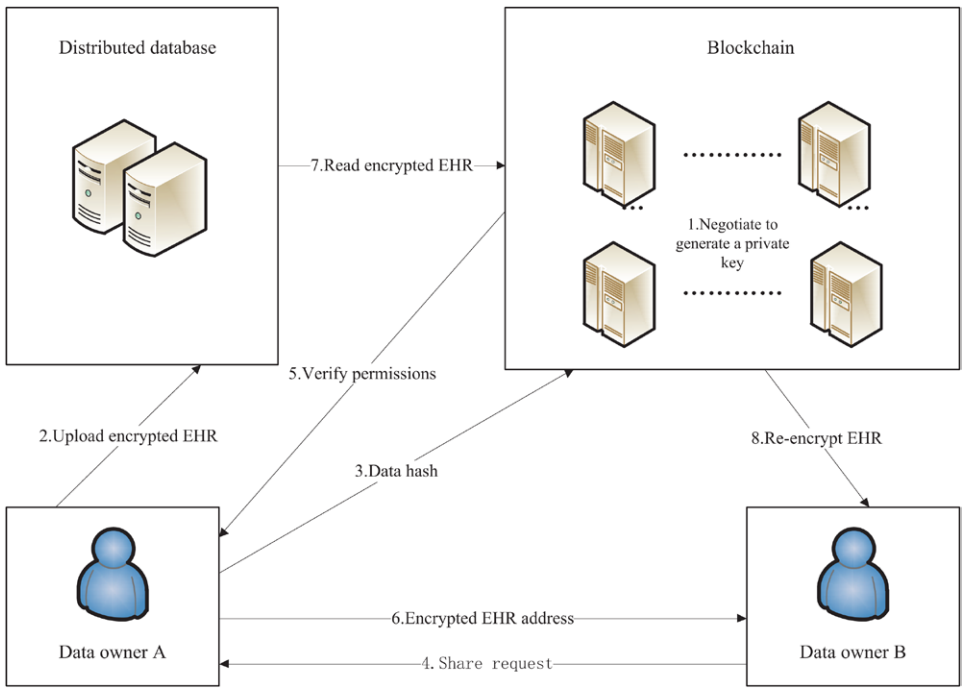

Figure 1. Blockchain-based electronic health record sharing model.

various medical institutions but also reduces the pressure of data storage and high-frequency access on the blockchain.

1) N authoritative centers: N authoritative centers represent different medical-related institutions in the alliance chain, such as hospitals, research institutes, banks, insurance companies, etc. Each authoritative center can generate a part of the secret by itself and then negotiate each organization's private key based on its identity information.
2) The data owner owns their own HER and can share EHR with other organizations. The data owner encrypts the original medical data, stores it in a distributed database, and stores the HASH value, storage address, and access control strategy of the blockchain's medical record to prevent malicious tampering with data. In data sharing, the data owner must generate a reencryption key and distribute the key to the proxy node.
3) Data users can obtain EHR from the data owner. Authorized data users can obtain the reencrypted EHR by sending a verification request or using their private key to decrypt the reencrypted EHR.
4) Agent: According to the Delegated Proof of Stake(DPOS) consensus algorithm,[21] the miner node is recommended as the agent node. The agent performs a reencryption algorithm to reencrypt the EHR. Specifically, the proxy node reencrypts the EHR according to the reencryption key from the data owner.

2.3. Electronic medical record sharing protocol based on blockchain

According to this scheme's model, this paper adopts a multi-center reencryption scheme as the data sharing protocol. The agreement is improved based on the reencryption plan proposed by Matthew Green. In Matthew Green solution, the user's private key is generated by Private Key Generation (PKG). Still, there is a problem: if the authenticity of the PKG cannot be trusted, the user's private key may be leaked. This scheme uses DKG technology to optimize the key generation part of the reencryption scheme to improve the security of user key generation. After DKG is used, each user's private key is negotiated and generated based on the remaining users; even if a user is Malicious, attacks can also ensure the key's security. The specific data sharing protocol consists of the following 5 steps: system initialization, key generation, data storage, data sharing, and data recovery.

1) Key generation: Each authority returns its private key SKId according to the input parameters and identity mark Id.
2) Data storage: After a patient is treated in the hospital, the hospital will generate its EHR. For EHR, the hospital first encrypts the HER with its own public key SKId, obtains the encrypted EHR ciphertext CId according to its identity Id and plaintext EHR, and then stores the CId distributed database. Then, as the data owner, the hospital signs the original EHR writes the signed EHR, HASH, storage location, and access control strategy into the file, and then broadcasts the transaction. The miner verifies and writes the transaction to the blockchain after the verification is passed.
3) Data sharing: When a user wants to read a certain EHR of a certain hospital, the user must first send a signature request to the hospital. The hospital first verifies whether the user's identity is legal through the request message. It then checks the file's access control policy, If the user's identity is legal and has read permission. Then the hospital will use the user's identity Idj and its private key SKId to generate the proxy reencryption key Rk. After that, the hospital will send the agent key and the storage address of the EHR to the agent node. The agent node will read the encrypted EHR file stored on the distributed database according to the storage address. Then, the proxy node uses the proxy reencryption key Rk to reencrypt the encrypted EHR to obtain the reencrypted ciphertext Cidj. Finally, the proxy node sends the reencrypted EHR cipher text Cidj to the user.
4) Data recovery: When the user receives the reencrypted EHR, he can use his private key SKIdj to decrypt the reencrypted ciphertext and obtain the EHR plaintext file after decryption.

2.4. Ethical approval

Ethical approval is not necessary because no human subjects and patient information were collected and studied.

2.5. Analysis

2.6. Correctness analysis. The scheme proposed in this article is similar to the reference "Efficient revocable ID-based signature with cloud revocation server".[22] The reference "An ID-based linearly homomorphic signature scheme and its application in blockchain".[23] First, generate the master key, and then create the user private key based on the master key. In these schemes, a trusted third-party authority (such as PKG) is required to protect the master key and generate the user's private key. However, there is no trusted third party in this scheme's model, so the DKG technology in the literature "Robust threshold DSS signatures".[17] and "Secure distributed key generation for discrete-log based cryptosystems".[18]is used to achieve the Key generation when trusting a third party. Therefore, the correctness of the user's private key age can be guaranteed by DKG technology.

2.7. Security analysis. First of all, the model proposed in the scheme uses a distributed database to store the encrypted EHR, which ensures that even if the encrypted data is leaked, the encrypted data cannot be decrypted by the attacker without the private key of the data owner. Get the plaintext content. The model also uses the blockchain's HASH, storage address, and access control strategy to store data. According to the characteristics of the blockchain itself that can be tamper-proof, data security and privacy are greatly improved. Specifically, since the blockchain itself contains many nodes, once data is written to the blockchain, each node will back up the data, so unless a 51% attack occurs, the data on the blockchain can't have Tampered; even if a 51% attack occurs in the end since the original EHR is not stored on the blockchain, this tampering will not affect the metadata of the EHR. Secondly, in terms of the protocol proposed in the scheme: the identity-based proxy reencryption protocol used in this paper has been optimized and improved, and the user private key generation part no longer relies on PKG to generate, but each institutional user chooses polynomial generation. The secret value is used to generate your private key. Compared with the centralized key generation method such as PKG, the distributed key generation method can effectively prevent the private key's leakage. Its security lies in: even a single user. In the event of a malicious attack, the attacker cannot obtain the user's secret value, let alone obtain the private key. The EHR stored in the distributed database encrypted by the user's public key cannot be decrypted by the attacker using his private key. Suppose multiple users are maliciously attacked, or multiple users conduct a collision attack. In that case, the private key cannot be obtained because the secret value sent by each user is checked in the protocol, and the private key cannot be generated if the check fails. Therefore, it can be concluded that the user's private key is safe and not easy to be leaked by malicious attacks. After the user's private key is generated, suppose a certain data user wants to obtain the EHR's plaintext

content; first, it needs to meet the access control policy, and secondly, it needs to decrypt the EHR ciphertext. We divide the remaining steps of the agreement into 2 phases. Phase 1: Data user B first sends a request with his signature to data owner A. The data owner checks the access policy corresponding to the user and regenerates it after confirming that he has read permission. It becomes the agent key, sends it to agent S, and sends the agent's encrypted data storage address. We assume that the data owner is credible at this stage, and the data user has never exposed his identity credentials to others. Attacker C cannot recover the key. We can imagine different attack scenarios of the attacker:

1) Case 1: C sends a request to A to try to obtain encrypted data. Since C does not have the user's identity credentials, after A receives C's request, the access control policy corresponding to C cannot be viewed, so the access control policy will not be executed. In the following protocol steps, the C attack was unsuccessful.
2) Case 2: Allow attacker C to intercept the request message sent by user B to A and perform a replay attack. Suppose that C can successfully deceive A, which causes A to treat C as B. Then A can query B's corresponding access control policy. If B has the read permission, A will generate a proxy key for B and then send the proxy key and the address of the requested data to the agent. The agent performs the remaining steps typically, And then sends the reencrypted ciphertext to C. However, this ciphertext is still unable to be decrypted by C because the ciphertext is encrypted and generated with the proxy key for B.

The second stage of the protocol is: After the agent receives the storage address of the reencrypted and encrypted data sent by the data owner, the agent downloads the encrypted data according to the protocol, and reencrypts the data ciphertext, and then sends the reencrypted ciphertext to the user. In the reencryption process, we still assume that the data owner is credible, and the identity credentials of the data user have never been exposed to others. The agent is semitrusted; that is, the agent is interested in the stored EHR file and Trying to obtain the content of the file to gain benefits, but will perform each step of the agreement in accordance with the agreement, and will not withdraw from the agreement halfway, and will not provide false data. Then there are 2 ways for the agent to try to obtain the EHR plaintext: Method 1, directly decrypt the first-layer ciphertext according to the private key of the data owner; Method 2, reencrypt the encrypted file and use the data user's private after reencryption The key decrypts the ciphertext. For method 1, since the data owner is credible and its identity credentials are not exposed, the private key of the data owner generated according to the distributed key cannot be obtained by the agent, so when the agent obtains the first-level ciphertext file, The private key cannot be used to decrypt the file, that is, the agent cannot obtain the EHR plaintext through this method. For the second method, suppose the agent reencrypts the ciphertext with the agent key and then obtains the reencrypted ciphertext. To obtain the EHR plaintext, the agent needs to obtain the private key of the data used to decrypt the second-layer ciphertext. In the same way as the method, since the identity certificate of the data user is not exposed, and the private key is generated according to the distributed key generation method, the agent cannot obtain the private key of the data user, and the agent cannot decrypt the second layer of ciphertext. To get the EHR plaintext. In short, the first phase of the protocol can effectively resist identity masquerading and replay attacks. The second stage of the protocol assumes that the agent is semitrusted. The 2 ways that the agent tries to obtain the EHR plaintext will not affect the scheme's security, nor will it affect the authenticity of the EHR obtained by the data user.

3. Results

As there are some problems in current medical informatization, we enumerate these problems and analyze the solutions proposed in this plan for these problems:

1) Privacy and security issues. This program uses asymmetric encryption technology to encrypt data, ensuring that private data will not be threatened. Storing the HASH of medical-related data in the blockchain ensures that the medical data cannot be tampered with and its nonrepudiation.
2) Data accessibility, operability, and integrity issues. This solution uses a distributed database to store encrypted data, stores the original data hash and access permissions in the blockchain, facilitates the detection of different permissions of various institutions, realizes data sharing among various institutions, and ensures data accessibility and operability. Because the blockchain has distributed database characteristics, the data is backed up on each node, effectively preventing data loss and ensuring its integrity.

This article also uses a comparative analysis method to evaluate the proposed electronic medical record sharing program. Since the solution in this article is based on the blockchain and is offered to solve the problem of medical data sharing, it is consistent with the document "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain",[13] the document "Towards blockchain-based scalable and trustworthy file sharing",[16] the document "MedRec: using blockchain for medical data access and permission management".[24] The proposed scheme belongs to the same type of medical blockchain scheme, so this scheme and the above 3. The comparison of these schemes, starting from the consensus mechanism adopted by each scheme, the type of blockchain, and the computing power requirements, can effectively compare the advantages and disadvantages of this scheme. The results are shown in Table 1.

Table 1

Comparison of our scheme with existing medical blockchain schemes.

Medical blockchain solution	Consensus mechanism	Single strand	Computing power demand	Maintenance cost	Network resource occupancy rate	Blockchain type
References (Zhang & Lin, 2018) scheme	PBFT	No	Small	High	High	Private Blockchain, Consortium Blockchain
References (Cui & Asghar & Russello, 2018) scheme	POW	Yes	Large	Low	High	Consortium Blockchain
References (Azaria & Ekblaw & Vieira & Lippman,2016) scheme	POW	Yes	Large	Low	Low	Consortium Blockchain
This article scheme	DPOS	Yes	Large	Low	Low	Consortium Blockchain

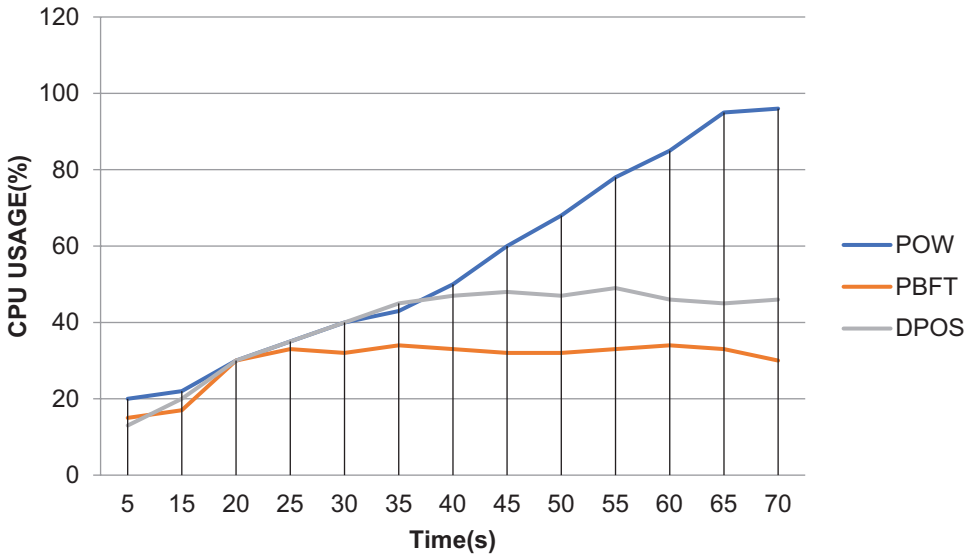

Figure 2. Comparison of the CPU occupancy rate of the 3 consensus mechanisms.

The comparison in Table 1 shows that this solution uses the DPOS consensus algorithm as the consensus mechanism. The reference "Towards blockchain-based scalable and trustworthy file sharing"[16] and the reference "MedRec: using blockchain for medical data access and permission management"[24] use the POW consensus algorithm. This scheme is compared with the above 2 schemes. The number of nodes that need to be started is relatively small, and there is no need to spend a lot of computing power to maintain the blockchain. Although the reference "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain"[13] requires relatively little computing power, the solution involves 2 blockchains: the consortium chain and the consortium blockchain. Private chains, 2 types of blockchains, must be more expensive to maintain, and the decentralization of private chains is not as good as that of consortium chains.

To compare the efficiency of the 3 consensus algorithms, we simulated the 3 consensus algorithms and obtained the CPU occupancy rate of each consensus algorithm when running through the simulation test on experimental data. The results are shown in Figure 2 (Comparison of the CPU occupancy rate of the 3 consensus mechanisms). The simulation results show that DPOS is not as fast as PBFT in response, but DPOS has significantly less CPU usage than POW.

To compare the 3 consensus algorithms' network occupancy rates, we simulated them in a network environment. We obtained the network occupancy rate of the 3 consensus algorithms through 5 experiments. The results are shown in Figure 3 (Comparison of network occupancy rate under 3 consensus mechanisms). As the PBFT consensus mechanism is a Byzantine fault-tolerant, it is necessary to tolerate invalid nodes and shield malicious nodes' influence on the consensus results. Therefore, to solve the Byzantine failure of f nodes, the consensus mechanism requires the system's total number of consensus nodes to reach at least 3f + 1. In the consensus process, all consensus nodes have to broadcast twice to the entire network before reporting the blockchain's electronic medical record. The new medical information block in the system reached an agreement. From the above analysis, it can be seen that the PBFT consensus mechanism has designed 2 network-wide broadcasts for all nodes. This process seriously affects the consensus

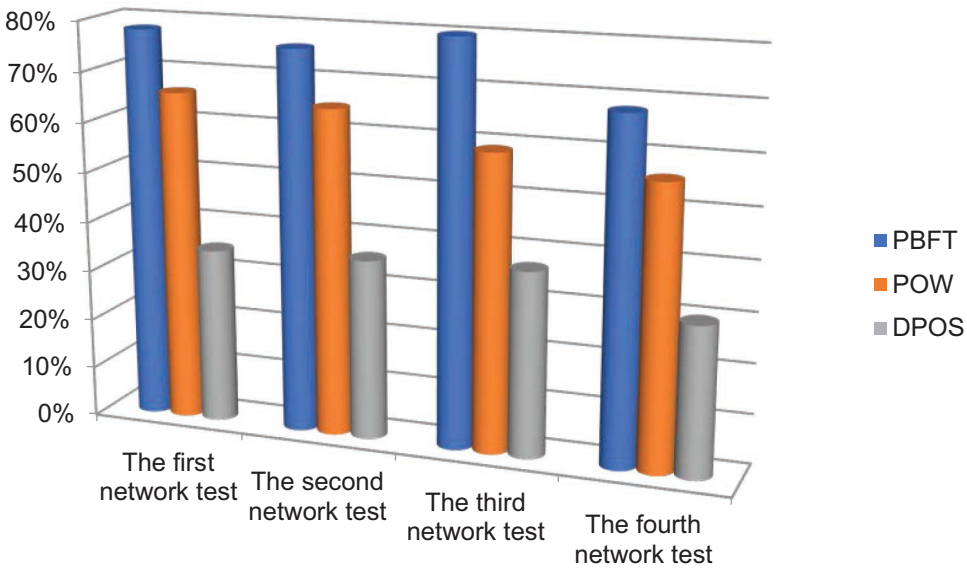

Figure 3. Comparison of network occupancy rate under 3 consensus mechanisms.

process's throughput performance and causes network resource consumption. Figure 3 shows that the average network occupancy rate of the PBFT consensus algorithm is around 80%. The POW consensus algorithm's average network occupancy rate is around 60%, and the average DPOS consensus algorithm is around 30%.

In summary, compared to the other 3 solutions, the CPU efficiency of this solution is not as good as the reference "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain".[13] Still, it is higher than the reference "MedRec: using blockchain for medical data access and permission management"[24] and "Towards blockchain-based scalable and trustworthy file sharing".[16] In terms of network resource occupancy rate, this solution is much lower than the other 3 solutions, which ensures a higher degree of decentralization without spending too much computing power and cost. This solution has certain advantages.

4. Discussion

The DPOS algorithm does not need to consume much computing resources, and the consensus speed is faster than other consensus algorithms. Still, it is only suitable for a situation with few consensus nodes. When many nodes join the blockchain system, all nodes must jointly carry out a 3-phase consensus, which leads to a large increase in communications and data transmission, likely to cause network congestion or network storms.

Because the DPOS algorithm also has apparent shortcomings in the application of medical systems, such as the efficiency of the system consensus algorithm continuing to decrease with the increase of the number of nodes and poor scalability. By studying consensus algorithms such as POW, POS, and PBFT, analyzing their advantages and disadvantages, and combining them with the Hyperledger Sawtooth framework, a new PoET (Proof of Elapsed Time) consensus algorithm will be proposed and applied in the medical system.

Since the sharing of medical data among various medical-related institutions is always a hot research issue, it is of great significance to ensure medical data privacy and realize the sharing of electronic medical records based on blockchain. This paper proposes a blockchain-based electronic medical record sharing scheme based on blockchain's decentralization and immutability characteristics. This paper's solution improves the model in the document "Towards blockchain-based scalable and trustworthy file sharing".[16] It proposes a data sharing protocol to realize the secure sharing of medical data between a single pair of authorized users. However, the solution can only realize data sharing between a single pair of users, and the efficiency of the DPOS algorithm in the solution needs to be improved. Our next research's main work is how to improve the consensus algorithm, improve the efficiency of consensus, and realize data sharing from 1 user to multiple users.

Acknowledgements

China Invention Patent Number: ZL201810024626.4
China Invention Patent Number: ZL202110369910.7

References

[1] Heart T, Ben-Assuli O, Shabtai I. A review of PHR, EMR and EHR integration: a more personalized healthcare and public health policy. Health Policy Technol. 2017;6:20–5.
[2] Dudin EB, Smetanin YG. A review of cloud computing. Sci Tech Inf Process. 2011;38:280–4.
[3] Hou JY, Shi CQ. Application of cloud computing technologies in information technology of hospitals. Electronic Design Eng. 2018;24;35–39.
[4] Zhang H, Yu J, Tian C, Zhao P, Xu G, Lin J. Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing. IEEE Access. 2018;6:40713–22.
[5] Liu Y, Zhang Y, Ling J, Liu Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Gener Comput Syst. 2018;78:1020–6.
[6] Underwood S. Blockchain beyond bitcoin. Communications of the ACM. 2016;59:15–7.
[7] Pu H, Ge Y, Yan-Feng Z, Yu-bin B. Survey on blockchain technology and its application prospect. Comp Sci. 2017;44:1–7.
[8] Vujičić D, Jagodić D, Ranđić S. Blockchain technology, bitcoin, and Ethereum: a brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh). IEEE. 1–6. March, 2018.
[9] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Manubot. 2019. Available at: https://git.dhimmel.com/bitcoin-whitepaper/. [Access date November 20, 2019].
[10] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities Soc. 2018;39:283–97.
[11] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP). IEEE. 2016;839–858.
[12] Xue TF, Fu QC, Wang C, et al. A medical data sharing model via blockchain. Acta Autom Sin. 2017;43:1555–62.
[13] Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J Med Syst. 2018;42:140.
[14] Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017;5:14757–67.
[15] Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: efficient and secure medical data sharing via blockchain. J Med Syst. 2018;42:136.
[16] Cui S, Asghar MR, Russello G. Towards blockchain-based scalable and trustworthy file sharing. In 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE. 2018:1–2.
[17] Gennaro R, Jarecki S, Krawczyk H, et al. Robust threshold DSS signatures. In International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer. 1996:354–71.
[18] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems. J Cryptol. 2007;20:51–83.
[19] Green M, Ateniese G. Identity-based proxy re-encryption. In International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer. 2007:288–306.
[20] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer. 1998:127–44.
[21] Luo Y, Chen Y, Chen Q, et al. A new election algorithm for DPos consensus mechanism in blockchain. In 2018 7th International Conference on Digital Home (ICDH). IEEE. 2018:116–20.
[22] Jia X, He D, Zeadally S, Li L. Efficient revocable ID-based signature with cloud revocation server. IEEE Access. 2017;5:2945–54.
[23] Lin Q, Yan H, Huang Z, Chen W, Shen J, Tang Y. An ID-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access. 2018;6:20632–40.
[24] Azaria A, Ekblaw A, Vieira T, et al. Medrec: using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD). IEEE. 2016:25–30.