Medical Record Storage Model Based on Credibility Assessment H-Algorand Consensus Mechanism

Jiatai Sun, Zengnan Zhao, Minghui Zhang, Ning Wang and Lihua Wang*

College of Electronic and Information Engineering, Shandong University of Science and Technology, Qingdao, Shandong, China, 266590.

*Corresponding author’s e-mail: skd992990@sdust.edu.cn

Abstract. In order to solve the problems of poor security and low throughput of the current electronic medical records, this paper proposes an electronic medical record storage model based on H-Algorand consensus mechanism of credibility assessment combined with blockchain technology. To ensure the normal operation of blockchain system effectively, the model used a credibility assessment algorithm to obtain the trust value and replace the account balance in the H-Algorand consensus mechanism with the trust value as the node weight. The results show that the storage model adopted here has higher security and throughput efficiency.

1. Introduction

Electronic medical record (EMR) is a digital version of traditional personal paper medical record. A complete EMR storage system is important to the development of the whole medical industry chain, such as health management, auxiliary diagnosis and medical research. The storage and sharing of medical records is the basis of promoting the development of medical industry chain. However, EMR contains a large number of patients' privacy records. In the process of storage and sharing, data leakage will cause serious harm to the reputation, property, safety and work of patients. The emergence of blockchain technology provides a new way to realize the secure storage and sharing of EMR[1].

Blockchain technology has the advantages of decentralization, traceability, tamper resistance, anonymity[2]. At present, the application of blockchain technology in EMR storage is relatively less. Reference [3] established a patient-centered medical architecture model using blockchain and open electronic medical records. However, the model only integrates the medical records distributed in different medical institutions into one view, and still stores the records in the blockchain, which leads to great pressure on the main chain and low throughput. Reference [4] constructed a medical data sharing model based on blockchain, in which the POW (Proof of Work) consensus mechanism is used, which requires more power consumption and slower block output speed. Reference [5] proposed a dual blockchain structure of medical records security storage and sharing scheme EMRSBC, which uses the PBFT (Practical Byzantine Fault Tolerance) consensus mechanism, to a certain extent, improves the throughput of the block chain, but it can not guarantee the credibility of the participating consensus nodes, and the system is easy to be attacked by malicious nodes. For solving the above questions, a new EMR storage and sharing model is proposed. In this model, the trust value is used to replace the account balance in the H-Algorand consensus mechanism as the weight, which improves the credibility of the system nodes and the overall block efficiency.
2. System mode
The EMR storage model includes six main parts: patients, medical institutions, EMR storage blockchain, cloud server, smart contract, access record storage blockchain. The overall model of the system is shown in Figure 1.

The specific functions of each part are as follows:
1) Patient: The provider and owner of EMR, encrypt the EMR and send it to the medical institution node;
2) Medical institutions: The maintainer of the blockchain, responsible for the composition of the new block, which is uploaded to the blockchain after consensus;
3) Cloud Server: It has a large amount of storage space to store the EMR of patients;
4) EMR storage blockchain: Blockchain storing EMR. The main storage content in the blockchain includes the ID of medical institutions and patients, the hash digest of the corresponding ciphertext in the cloud server, and the storage address of the cloud server corresponding to EMR;
5) Access record storage blockchain: A blockchain that records the behavior of accessing the EMR storage blockchain;
6) Smart contract: The autonomously running program carried on the blockchain is mainly responsible for the realization of the EMR query process and the writing of access records to the blockchain.

The patient's EMR is generated by the medical institution and finally uploaded to the EMR storage blockchain. Medical institutions can query the patient's EMR with the assistance of the patient according to the needs of the patient's condition, and assist in the diagnosis of the condition. The EMR sharing process and the access process of the EMR access process are assisted by smart contracts.

Consensus mechanism is the key to achieve the consistency of distributed ledger in blockchain. The consensus mechanisms of public chain mainly include POW, Delegated Proof of Stack (DPOS), Proof of Stake (POS), and PBFT. But these consensus mechanisms are not suitable for EMR storage model. In order to ensure the security and consensus efficiency of EMR storage model, this paper selects H-Algorand consensus mechanism based on credibility assessment.

3. Credibility assessment
The trust degree of EMR storage blockchain nodes is mainly evaluated from the contribution rate and work regularity of nodes. The contribution rate is mainly based on the number of effective medical records uploaded by the node on the EMR blockchain, and the regularity of work is mainly based on the proportion of effective blocks generated when the node is the leader. Trust values are updated when a new key block is created.
To calculate the trust value of a node of a medical institution, firstly, according to (1) and (2), the contribution rate and regularity of the current node in the system are reflected.

$$G_m = \frac{1}{t} \sum_{i=1}^{t} \frac{m_i}{m}$$  \hspace{1cm} (1)

$$G_k = \frac{1}{L} \sum_{j=1}^{L} \frac{n_j}{n}$$  \hspace{1cm} (2)

Where, $L$ is the current length of the blockchain, $t$ is the number of times the current node is selected as the leader node. $m$ is the number of new blocks when the current node is selected as the leader node. $m_i$ represents the number of new blocks actually generated by consensus when the current node acts as the leader node for the $i$-th time. $n_j$ represents the number of medical records published by the current node in the $j$-th block. $n$ is the number of medical records contained in a single block. $G_m$ represents the average value of the effective block proportion produced by the current node as the leader, which is the direct embodiment of the working regularity of the nodes in medical institutions. $G_k$ represents the average number of effective medical records recorded by the current node in each medical block, which is a direct reflection of the contribution rate of medical institutions.

Then, the standard deviation $S_m$ and $S_k$ of the mean value expressed by $G_m$ and $G_k$ are calculated by (3) and (4).

$$S_k = \sqrt{\frac{1}{L} \sum_{j=1}^{L} \left( \frac{n_j}{n} - \frac{1}{L} \sum_{j=1}^{L} \frac{n_j}{n} \right)^2}$$  \hspace{1cm} (3)

$$S_m = \sqrt{\frac{1}{t} \sum_{i=1}^{t} \left( \frac{m_i}{m} - \frac{1}{t} \sum_{i=1}^{t} \frac{m_i}{m} \right)^2}$$  \hspace{1cm} (4)

In the blockchain network, the trust degree of nodes is directly proportional to $G_m$ and $G_k$, and inversely proportional to $S_m$ and $S_k$. Therefore, intermediate parameters $y_1$ and $y_2$ are introduced. Where $y_1$ is calculated by (5). Since $G_m$ is always 0 before being selected as the leader node for the first time, $y_2$ is obtained by (6) when $t$ is 0 and $y_2$ is obtained by (7) when $t \geq 1$.

$$y_1 = G_k / (1 + S_k)$$  \hspace{1cm} (5)

$$y_2 = 1$$  \hspace{1cm} (6)

$$y_2 = G_m / (1 + S_m)$$  \hspace{1cm} (7)

In order to ensure the slow growth of trust value when the medical institution node just joined the blockchain network, the trust value gradually increased after continuously submitting effective and legal EMR to the blockchain. When the trust value reaches the turning point, the growth rate of the trust value of the node is accelerated, and the permission to enter the consensus group is obtained. A logistic function $f(x)$ is introduced. $f(x)$ is shown in (8).

$$f(x) = \frac{1}{2} \left( 1 + \frac{x-a}{\lambda + |x-a|} \right)$$  \hspace{1cm} (8)

$$R = \min \{1, f(x)\}$$  \hspace{1cm} (9)

Introduce the evaluation factor $x$, $x = y_1y_2T$. $x$ is proportional to the trust value $R$. $T$ is the time for the node to join the blockchain (unit: days). $a$ and $\lambda$ are the adjustment parameters of the trust value function to adjust the change speed of the trust value. The slope of $f(x)$ is related to the value of $\lambda$. The trust value $R$ of the node is finally obtained by (9).
4. Consensus mechanism

Algorand mechanism was proposed by Micali [6], mainly to solve the problems of POW and other consensus mechanism, such as computational waste, weak scalability, easy bifurcation, and long confirmation time. On this basis, literature [7] proposed H-Algorand consensus mechanism which combines the advantages of Algorand consensus mechanism and MB-Algorand consensus mechanism. The H-Algorand consensus mechanism takes into account the block efficiency and security issues, and makes a significant improvement of the consensus efficiency at the expense of a small amount of security.

All nodes in H-Algorand mechanism have weights, and the weight of nodes is directly proportional to account balance. However, consensus mechanism relying on account balance as weight tends to concentrate bookkeeping right in the hands of a few "rich" and is vulnerable to attack. For the EMR storage model, there is no concept of tokens, so the EMR storage model mentioned in this paper replaces the account balance in H-Algorand consensus mechanism with the obtained trust value \( R \). The weight of each medical institution node is only determined by its trust value. Compared with account balance, the trust value of node can ensure the honesty of consensus group.

Suppose that each consensus group executes a cycle with \( N \) blocks. The trust value of each node in the EMR storage blockchain is obtained by credibility evaluation, and the blockchain network selects a consensus group according to the trust value of each node. According to the random number mechanism, the members of the consensus group select the leader node responsible for generating the new block. The leading node packs the information it receives and assembles it into a block to be published, and signs it. When the number of blocks to be published is enough \( N \), it is broadcast to other nodes in the consensus group. Other nodes make consensus on the received blocks in turn by H-Algorand consensus mechanism, and the new blocks are written into the blockchain after passing the consensus, and this consensus ends. Recalculate the trust value of each node and select a new consensus group.

In order to prevent the node from forging its own trust value and ensure the authenticity of the trust value, it is necessary to include the trust value information of the current consensus group members in the block. In the process of H-Algorand consensus mechanism, all nodes need to verify the trust value of the nodes in the consensus group.

5. System analysis and evaluation

5.1. Trust value analysis

The trust value \( R \) of EMR storage blockchain node is calculated by (8) and (1). In order to make the change curve of trust value meet the requirements of the system, the specific values of \( a \) and \( \lambda \) need to be determined. Take \( a = 5 \) and \( \lambda = 50 \), \( a = 10 \) and \( \lambda = 100 \), \( a = 30 \) and \( \lambda = 300 \), \( a = 50 \) and \( \lambda = 500 \), \( a = 100 \) and \( \lambda = 1000 \), and draw the change curve of trust value \( R \), as shown in Figure 2. It can be seen that with the increase of \( a \) and \( \lambda \), the trust value changes slowly. In order to ensure that the node can enter the consensus group only after the regular contribution of medical records, take and carry out the experiment. It can be seen from the curve in the Figure 2 that when the evaluation coefficient \( x \) is below 400, the trust value of the node is in the range of \([0,0.2]\). When \( x \) reaches 400, the trust value increases rapidly. When \( x \) is 600, the trust value of the node is above 0.8.

When nodes join the blockchain network, they will enter a process of slow growth of trust, unable to launch attacks on the blockchain. In the initial stage of system establishment, the trust value of all nodes is low, and the threshold value of entering the consensus group is low, which is the fragile stage of the system. However, when the system reaches a stable state and joins the system, it takes a long time to establish its own trust value, which makes it more difficult to attack the system.

5.2. Throughput analysis

Throughput is a measure of the system's ability to process transactions per unit time, and it is directly related to the system's block generation efficiency and consensus mechanism. In this paper, the
throughput is expressed by $TPS$ (transactions per second), and the calculation equation of throughput is (10).

$$TPS = \frac{\text{SumTransaction}}{\text{Time}}$$  \hspace{1cm} (10)

Where $\text{SumTransaction}$ is the amount of EMR information contained in a single block, and $\text{Time}$ is the block out time of a single block. Taking Bitcoin as an example, the block size of Bitcoin is 1MB, the number of transactions contained in each block is 2000–3000, the block time of Bitcoin is 10 minutes, and the throughput of Bitcoin is about 5. Ethereum uses an improved POW consensus algorithm on the basis of Bitcoin to increase the block generation speed, and the throughput is significantly improved, with a throughput of about 75 per second.

In this paper, we take the blockchain with the size of 1MB, 2MB and 4MB respectively to test. The number of nodes is 6, and the number of blocks produced in each consensus group is $N$. The output speed of the system changes with $N$ as shown in Figure 3. It can be seen that with the value of $N$ increasing, the system's block output speed becomes faster. According to (10), when the block size is 4MB and $N$ is 8, the throughput per second of the EMR blockchain is about 860.

The current consensus mechanisms such as POW and POS depend on the computing power or token of the system, and in order to prevent the system from being attacked by bifurcation, waiting blocks are set, so the throughput per unit time is low. This system optimizes the H-Algorand consensus mechanism based on the credibility assessment. In the execution process, it does not depend on tokens and does not need to wait for blocks. The throughput is significantly better than the consensus mechanisms such as POW, POS and PBFT, which improves the transaction throughput performance of the EMR storage model.

### 5.3. Contrastive analysis

| Consensus mechanism | Rely on tokens | Rely on computing power | Judge the credibility of the node | Prevent fork attacks | Generate blocks continuously |
|---------------------|----------------|-------------------------|-----------------------------------|---------------------|-----------------------------|
| This paper          | \(x\)          | \(x\)                   | \(\checkmark\)                   | \(\checkmark\)     | \(\checkmark\)             |
| POW (BTC) [8]       | \(\checkmark\) | \(\checkmark\)      | \(x\)                             | \(x\)               | \(x\)                       |
| POW (ETH) [9]       | \(\checkmark\) | \(\checkmark\)      | \(x\)                             | \(x\)               | \(x\)                       |
| POS [10]            | \(\checkmark\) | \(\checkmark\)      | \(x\)                             | \(\sqrt{\checkmark}\) | \(x\)                       |
| PBFT [5]            | \(x\)          | \(x\)                   | \(\sqrt{\checkmark}\)            | \(x\)               | \(x\)                       |

Table 1 shows the performance evaluation of the consensus mechanism used in this paper and the
consensus mechanisms such as POW, POS and PBFT. It can be seen that the H-Algorand consensus mechanism based on credibility assessment proposed in this paper is obviously more suitable for EMR storage systems than the current consensus mechanism.

6. Conclusion
This paper proposes an EMR storage model based on blockchain technology and applies the H-Algorand mechanism based on credibility assessment as the consensus mechanism of the system. Through the credibility assessment of each medical institution node, the trust value is used to replace the account balance in the H-Algorand mechanism as the weight, which effectively ensures the credibility of each node. Compared with the current scheme, the results show that the model in this paper has some advantages in throughput efficiency and node credibility, which can effectively guarantee the storage of EMR.

Acknowledgments
This work was supported by the Natural Science Foundation of Shandong Province, China (no. ZR2018MF005).

References
[1] Xue, T.F., Fu, Q.C., Wang, C., et al. (2017) A medical data sharing model via blockchain. Acta Automatics Sinica, 43: 1555–1562.
[2] Xia, Q., Sifah, E.B., Asamoah, K.O., et al. (2017) MeDShare: Trust-less medical data sharing among cloud service providers via block-chain. J. IEEE Access, 5: 14757–14761.
[3] Roehrs, A., Costa, C.A.D., Rosa Righi, R.D., et al. (2017) Analyzing the performance of a blockchain-based personal health record implementation. Journal of Biomedical Informatics, 92: 103–140.
[4] Yang, Y. (2017) Research on blockchain method for secure storage of medical records. Journal of Jiangxi Normal University (Natural Science), 41: 484–490.
[5] Zhang, L.H., Lan, F., Jiang, P.P., et al. (2019) Secure storage and sharing scheme of medical records based on dual blockchain. In Computer Engineering & Science, 41: 1581–1587.
[6] Gilad, Y., Hemo, R., Micali, S., et al. (2017) Algorand. New York. 51-68.
[7] Wang, B., Ren, Y.Q., Huang, D.Y. (2020) H-Algorand: public chain consensus mechanism based on multi block output. Journal of Computer Applications, 40: 2150-2154.
[8] Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. [Online] Available: http://www.bitcoin.org/bitcoin.pdf
[9] LGG, L., CHU, D.H., OLICKL, H., et al. (2016) Making smart contracts smarter. In: 2016 ACM SIGSAC Conference on Computer and Communications Security. New York. 254-269.
[10] King, S., Nadal, S. (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Online] Available: https://www.chainnode.com/doc/641.