ISSN: 2664-9640

Analysis and application of blockchain technology in medical and health field

Zekun Chen, Xiaorong Cheng *

Department of Computer, North China Electric Power University, Baoding Hebei, China

* Corresponding Author

Abstract

In contemporary society, health has become a new pursuit for people in addition to material needs, and with the development of Internet technology, the amount of health data of citizens has exploded. How to effectively manage medical data and use these data to improve the overall medical health of society has become A key question. This article builds a new medical health information management system based on blockchain technology, integrates health data collected from various sources, and forms a continuous, multi-dimensional health information database. Make effective use of health data, provide guidance for disease prevention and treatment, and improve the life and health of the whole people.

Keywords

Blockchain; Consensus Algorithm; Block Producer Election Mechanism; Medical Health; Health Data Management

1. Introduction

With the rapid economic development and the continuous improvement of living standards, people's attention is not only limited to the pursuit of material life, but physical health has become the focus of more people's attention. It is this kind of change that has caused the continuous increase in people's demand for medical resources, thereby stimulating the forward development of the entire medical and health field. The “Outline of the “Healthy China 2030” Plan” released in 2016 is a key issue in the form of national policies that promote health as a priority for development. The development of the Internet allows everyone to record their own physical health data at any time, conduct online medical consultations to obtain diagnosis results, and the diagnosis results obtained from offline hospital visits form a huge personal health data set. These data can help doctors better diagnose diseases and evaluate health conditions, and at the same time provide individuals with a personalized monitoring and management platform that fully understands their physical conditions. However, since there is no integrated system to process these huge, complex, and independent health data, it is difficult to ensure the effective use of these data. Therefore, the effective way to solve these problems is to establish a comprehensive, detailed and holistic medical and health system.

The medical and health system built with blockchain technology can apply the characteristics of blockchain technology such as decentralization, tamper resistance, loss prevention and high confidentiality to the collection and management of health data[1].Decentralization can collect health data in a distributed manner, reduce the high burden of centralized collection, and improve the information collection efficiency of the medical and health system. The anti-tamper feature can obtain correct health data at any location to ensure the accuracy of the data. Loss prevention changes the shortcomings of easy loss of locally stored data, reduces the number of data backups, and ensures data storage security. The confidentiality of the blockchain will ensure the safety of health data during storage and transmission, greatly reducing the risk of

ISSN: 2664-9640

citizens' health data leakage. This article will combine blockchain technology to build a medical and health system plan to provide a new idea for the government or medical institutions.

2. Blockchain technology

Blockchain is a database based on distributed technology[2], which has the characteristics of security and stability, and is shared by users in the network at the same time. Blockchain allows parties who do not know each other to trust the shared record of an event, because data is stored in a structure called "blocks", and these "blocks" are connected to each other by timestamps and hash values It forms a chain structure, so it is called a "blockchain".

2.1. The structure of the blockchain

As a kind of chain storage structure, each node packs all the information in the time period, and selects the appropriate node according to the rules to generate the next block on the chain. The two blocks are arranged in chronological order into a chain. Each block on the chain consists of two parts, namely the block body and the block header. The block structure is shown in Figure 1.

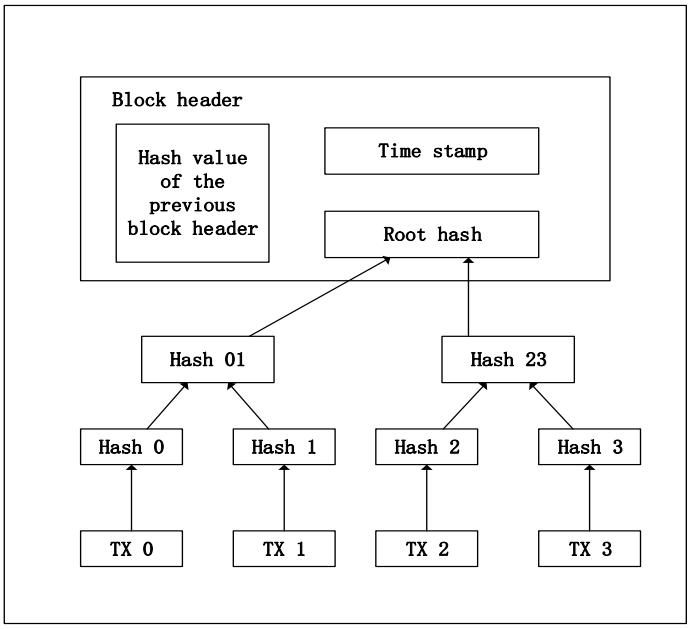

Figure 1: Block structure

The block header consists of the hash value in the previous block header, the timestamp, and the hash root of the transaction broadcast in the blockchain network. The block body stores the transactions broadcast in the blockchain network in the form of a merkle tree, and at the same time generates a hash value based on this information and stores it in the block header.

2.2. Consensus algorithm

The key algorithm in the implementation of the blockchain is the consensus algorithm[3-5], that is, the distributed system uses a decentralized method to form a unified protocol algorithm for the network state. After all nodes have packaged the information, they need to select a suitable node to generate a new block. This suitable node is called the block producer. And how to select the appropriate block producer needs to know some information about the nodes in the blockchain, and the consensus algorithm is the main mechanism for block producer selection. Consensus algorithms are mainly divided into two types: based on workload proof mechanism and based on equity proof mechanism.

Based on the proof-of-work mechanism(PoW): Before the block producer is selected, each node will use a random number, the timestamp in the block header, the hash root, and the hash value

ISSN: 2664-9640

of the previous block header to calculate the current time period. The hash of the node. Then according to whether the calculated hash meets a certain condition (such as less than the given target value), if it meets, the node is selected as the block producer, and the block is connected as the next block at the same time On the blockchain.

2) Based on the proof-of-stake mechanism(PoS): the selection of the block producer will be executed according to the current amount of digital currency. In the Bitcoin transaction system, the proof of equity is to allocate interest income based on the amount of currency owned by the user and the time of ownership.

The consensus algorithm of the proof-of-work mechanism has shortcomings such as a large amount of calculation and a 50% computing power attack (if a node has 50% of the computing power of the entire network, it has the ability to tamper with the information of the entire link), so in the blockchain In the development of, the consensus algorithm of the equity proof mechanism has become the first choice of people. The consensus algorithm based on the proof-of-stake mechanism does not generate huge computing overhead, and in this mode, the user's income and the user's currency age maintain a certain relationship, and it has nothing to do with the performance of the computer itself.

3. Problems in the current healthcare system

At present, citizens' physical health data basically comes from hospital diagnosis and treatment information, but the medical systems of different hospitals and different CDCs are different, and the types of databases storing and managing health data in different medical systems are also different. This has led to the dispersion of citizens' health information. Since it is possible for a patient to be treated in multiple hospitals, his health information will be repeated in the medical system of these hospitals, and the data repeatability is high. It is difficult to integrate health data to form its exclusive and continuous multi-dimensional database for the same target, and it is impossible to perform the tasks of the citizen's medical and health system such as evaluating its health status, disease diagnosis and long-term observation[6].

With the development of the Internet and mobile networks, more and more health-related software and apps have entered the public's field of vision. The development of the Internet of Things technology and the production and use of various sensors and smart devices have made it easier to collect and store citizens' health data, and the amount of data has increased geometrically. However, there is still no overall system to effectively record, track and manage these isolated, fragmented, and traceless health data, which cannot effectively prevent the occurrence of diseases and help treat diseases. Therefore, it is very necessary to establish a systematic and safe medical and health system for citizens' health information management. By establishing a medical and health system, individuals, governments, and medical institutions can obtain citizens' health data more conveniently and quickly, and provide comprehensive and complete health data for each individual, including physical conditions, historical diseases and other information; more timely diagnosis Diseases, prevent diseases more effectively, and realize integrated medical and health management.

By combining blockchain technology to build a health data management system, citizen health information from medical institutions, health software and other sources will be effectively used to solve the problem of decentralization and islanding of health data; duplicate data will be judged and sorted in the system, Remove redundant data and solve the problem of data duplication; store the integrated data in the blockchain to improve the confidentiality of data transmission, avoid data loss, and ensure the safety of citizens' health data[7].

ISSN: 2664-9640

4. Medical and health management system design plan

The system model proposed in this paper is shown in Figure 2.Users in the medical and health system (such as medical institutions, CDCs, etc., and the health App server database as a user) generates an information list from the collected personal health information of citizens, and the list uses identity information to identify the health information of different citizens , And then broadcast this list to all users in the entire system. All users select the block node according to the agreed consensus algorithm, which is responsible for verifying health information, and then enters the health information into the blockchain according to the identity.After the entry is over, other users synchronize the information in the blockchain, and perform repetitive detection based on the health information stored in the blockchain. After the detection is completed, duplicate items will be removed from their own health information list and paid to the block producer.

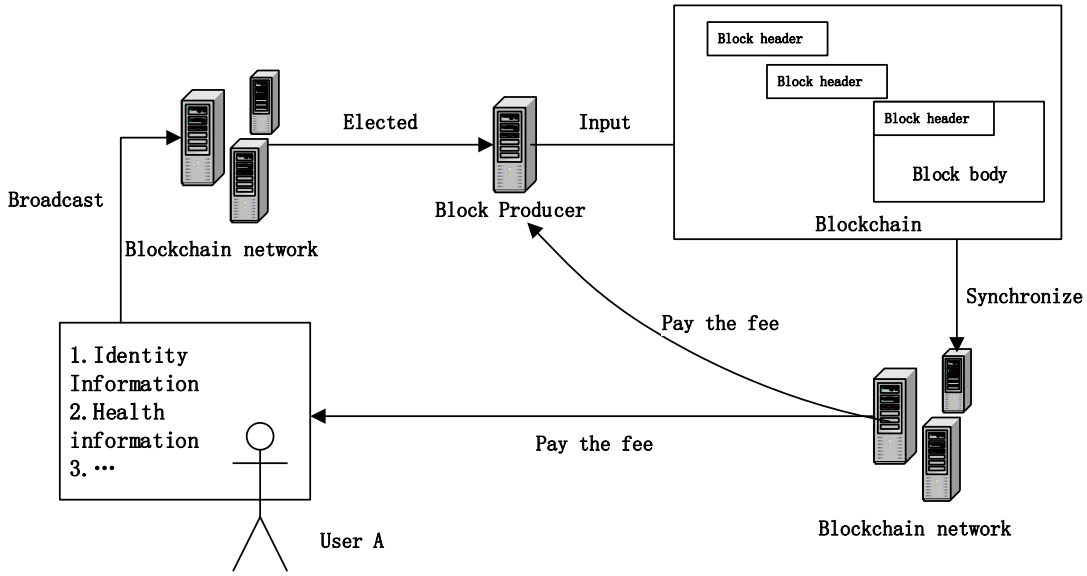

Figure 2: System model

4.1. Information collection

After a user A in the system collects health information, it will be based on the citizen's health information type (divided into physical condition information, disease information, etc.), attributes of the collected information (including addition, modification, deletion, etc.), and treatment plan, etc. The information is packaged according to different identification information to generate a list of health information, and then the list is broadcast in the entire system.

The health data collected by user A is confidential information to other users. Only when it is selected as a block producer or audited by the block producer, and verified, can it be uploaded to the blockchain and synchronized to other users. In response to this confidentiality requirement, the system can use a security key for protection. At the same time, in order to ensure the authenticity of user A's identity, the digital signature of user A can be added to the health information list to ensure the reliability of the data.

4.2. Election of block producer

The system uses a consensus algorithm based on proof of rights to elect block nodes to ensure the consistency of the blockchain and reduce computational overhead. The selected block nodes are responsible for generating the next block on the chain. The first block was established by the National Centers for Disease Control and Prevention, and the next block was the user

ISSN: 2664-9640

agent who collected and uploaded the most effective citizen health information in the previous stage. After the block producer is selected, the block producer will conduct a unified review of all health information lists in the current system. In the review process, in order to avoid a large number of lists in a short time and affect the efficiency of the system, the principle of sorting according to the number of citizens in the list is adopted, and the review is carried out with a large number of users first, so that users of medical institutions with a large amount of data can be guaranteed Priority is given to review, and individual App users will be reviewed later. However, because there may be a small number of medical information, but in very urgent cases, emergency signs can be added to ensure the review and upload of emergency information data, and upload and broadcast at the fastest speed in some major medical problems. The identification of each stage selects the number of health information as the limit. For example, choose c as the identification value. When the number of uploaded health information exceeds c but is less than 2c, switch to the next stage. The user who uploads the most information at this time is elected as the block producer. One stage of review work, and so on. After the review, the current block producer will complete the block entry work.

4.3. Entering new blocks and paying fees

After user A submits the health information list to the block node, the block producer obtains the complete list through the security key. After the review is passed, the health information list is stored in the block body in the form of a merkle tree, and the root hash, the hash value in the previous block header, the timestamp, and the block producer address information are added to the block header. Entry of new blocks. After the new block is generated, link it to the current block chain and broadcast it in the whole system.

After the new block is broadcast, all users perform synchronization work, scan the new health information list locally, synchronize their own health information, eliminate duplicate health information in the list, complete the optimization processing of health information, and avoid uploading duplicate health information The waste of system resources caused by information. At the same time, according to the block producer address information in the block, a certain detection fee is paid to the block producer to encourage users to upload more health data and strive to become a new block producer. In this way, in real life, medical institutions can carefully examine and treat citizens and improve public health.

5. Feasibility Analysis

The solution in this paper uses the blockchain to record citizenship information and health information. However, the blockchain is an open distributed database, and each node has a data backup, which means that there are nodes facing the risk of privacy leakage.

Because the blockchain is a distributed database, every user in the system stores a data backup, which can avoid data loss and damage. At the same time, the blockchain has the characteristics of decentralization, which can collect health data in a distributed manner, reduce the high burden of centralized collection, and improve the information collection efficiency of the medical and health system. At the same time, the data can be prevented from being illegally tampered with. Only after passing the review of the block producer, can the data in the blockchain be uploaded or modified. After the block is updated, the entire system will be synchronized to ensure the consistency of the data in the system, and avoid the occurrence of different versions of data from interfering with the operation of the medical and health system, thereby causing public health threats. In the process of information transmission, the encryption system is used to protect citizens' private information, which ensures the safe and stable operation of the entire system. Obtaining a certain service fee by the block producer can encourage users to submit correct and effective health information, carefully review the

ISSN: 2664-9640

information and ensure information security, and improve the security level of the entire system.

6. Performance evaluation

Assuming that each sub-unit in the system reports the health information of 500 citizens at the same time, the audit efficiency of the certification center or block producer is 50 per day. According to the scheme of this article, when the number of health information exceeds k1, a new health information reviewer needs to be added. It is assumed that k1=50 and a total of 3 system members including the block producing node participated in the information review. Through simulation calculation, the time cost comparison between the distributed health information processing scheme based on blockchain and the traditional centralized processing scheme is shown in Figure 3.

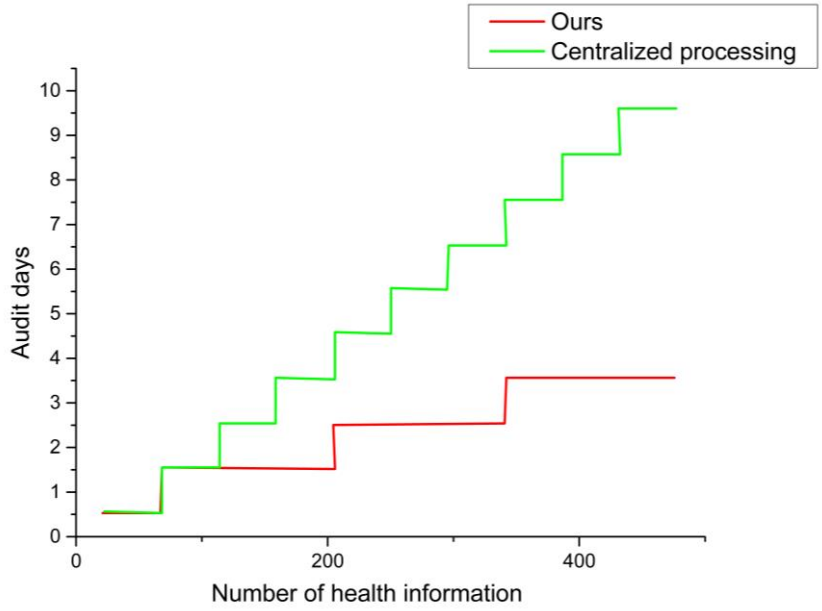

Figure 3: Time cost comparison

It can be seen from Figure 3 that under the premise of an audit efficiency of 50/day, when the amount of information is less than 100, the time cost of the two schemes is basically the same. With the increase in the amount of audit information, the time overhead of distributed processing based on blockchain is significantly lower than that of centralized processing. Therefore, in terms of audit efficiency, this solution has more advantages.

7. Conclusion

This article builds a new type of medical and health system through blockchain technology. Compared with the traditional medical information management system, the system uses blockchain technology to improve the collection efficiency of medical information and improve the accuracy and security of information. , To provide ideas and solutions for building an overall medical and health system, thereby improving the public health level. By establishing a medical and health system, collecting citizens' health information, such as patient's physical signs, daily routines and acquired diseases, provides a complete and comprehensive data information for the hospital's diagnosis and treatment, which is to maximize the use of health data.

At present, artificial intelligence technology is developing rapidly, and smart medical care has become a nationally valued project. The health information database obtained by the system can provide a wide range of data sources for artificial intelligence technology. Participating in

ISSN: 2664-9640

training with national health data can help people train as soon as possible. A powerful artificial intelligence medical program supplements the current medical system to promote the development of smart medical care and enhance the progress of the entire medical field. Complete data information can provide reference for individual citizens, so that people can pay attention to their physical condition at any time to prevent the occurrence of diseases. The government can also assess the physical fitness of citizens based on the data of the system, provide assistance for the country to formulate some guidelines and policies, and provide scientific and technological support for the "Healthy China" strategy.

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[Online], Information on: https://bitcoin.org/bitcoin.pdf, October5, 2018

[2] Zhu Yan, Wang Qiaoshi, Qin Bohan, Wang Zhonghao. Blockchain technology and its research progress[J]. Journal of Engineering Science, 2019, 41(11): 1361-1373.

[3] Ding Yue. Research on consensus mechanism based on blockchain [D]. Nanjing University of Posts and Telecommunications, 2019.

[4] Ken Jia. Discussion on the development status and prospects of blockchain consensus algorithm [J]. Computer Knowledge and Technology, 2019, 15(32): 34-35.

[5] Li Futao. Consensus mechanism in blockchain [J]. China New Communications, 2019, 21(21):12.

[6] Wang Xu. Research and implementation of privacy protection of medical data sharing based on blockchain [D]. Xidian University, 2019.

[7] Dai Linlin, Jia Chengqiang, Miao Fan, Yang Haifeng. Research on the application of blockchain related technologies in railway passenger ticket system[J]. Railway Computer Applications, 2019, 28(11): 23-26+37.