Original Research Article

Design of a blockchain based medical data sharing platform

Zhang Hui, Xu Haohao

School of Information Engineering, Yulin University, Yulin, Shaanxi, 719000, China

Abstract: With the increasing importance of medical data sharing and collaboration, people urgently need a powerful and secure medical data platform. How to securely and completely share medical data has become the problem we need to solve. This article proposes the design of a healthcare data sharing platform that provides secure and reliable data sharing services. The platform utilizes blockchain technology and big data technology, and adopts a microservice architecture that allows for flexible and scalable operations. The data sharing platform adopts anonymization and permission control strategies to ensure that only authorized personnel can access sensitive information, ensuring the confidentiality and integrity of shared data. By utilizing cloud+blockchain storage solutions, medical data can be saved and transmitted in the cloud, while also improving the operational speed of block-chain networks.

Keywords: Block-chain; Data sharing; Medical data

1. Introduction

With the increasing importance of medical data sharing and collaboration, there is an urgent need for a powerful and secure medical data platform. Despite the vast amount of medical data, most of it is still stored in the databases of medical institutions, which results in medical data being isolated into "information islands" that cannot be shared or fully utilized for their intended value. In addition, data storage solutions are susceptible to factors such as node loss, leading to an increased risk of information loss. In addition, due to the data being stored in third-party structures, the individual using the data is unable to understand and freely use their own medical data, which is also a problem. Therefore, how to securely and completely share medical data has become the problem we need to solve.

2. System requirements analysis

With the continuous advancement of digitization and informatization, the quantity and complexity of medical data are also increasing. These data include medical records and examinations. In the medical industry, encryption and decryption technology is very important because it can protect patients' privacy and sensitive information. Blockchain technology is gradually being applied in the healthcare industry to improve data security and reliability. The encryption and decryption of medical data based on blockchain needs to be popularized to meet the needs of the medical industry.

(1) Medical institutions need to protect patients' privacy and sensitive information. Due to the specific permission restrictions on the use of medical data, encryption and decryption techniques are necessary. Blockchain can provide highly secure data protection, and encryption technology is the key to achieving this security.

(2) Medical institutions need to ensure the integrity and consistency of data. Using blockchain to store and maintain medical records ensures the security and reliability of data. In this case, encryption and decryption

techniques can protect the integrity of data to prevent unauthorized modifications.

(3) Medical institutions need to ensure data traceability. Blockchain technology can provide this traceability, while encryption and decryption technology can ensure that only authorized personnel can access data.

In short, there is a universal demand for blockchain based medical data encryption and decryption. The use of this technology can protect patient privacy, ensure data integrity and consistency, and provide data traceability. Encryption and decryption techniques are the foundation for implementing all these features.

In this field, user trust and anonymity are very important requirements. Firstly, user trust and anonymity can protect personal privacy.Secondly, user trust and anonymity can enhance the credibility of medical data. In traditional medical data storage and sharing, the authenticity and credibility of the data are often difficult to guarantee. Finally, user trust and anonymity can promote the sharing and communication of medical data.

Based on the above requirements, we can design a complete blockchain system that can support large-scale data transactions, application development, and operation. This system is based on advanced blockchain technology, using efficient consensus algorithms and smart contracts to ensure data security and reliability while meeting different application needs, providing users with stable, efficient, and secure blockchain services. At the same time, the system also supports cloud operations and encryption/decryption modules to meet different application scenarios and security requirements.

3. Design of a blockchain based shared healthcare platform

3.1. Overall technical architecture of the system

Users can upload personal medical data through the front-end interface of the application layer. The system uses dynamic hybrid encryption algorithm and ring signature algorithm to process user data, establishes smart contracts for the processed data, and then deploys smart contracts to store the data on the blockchain. During the data storage process, the consensus mechanism of the system consensus layer can generate blocks by deploying block packaging rights to store the data on the blockchain. The block time collection scheme returns the data upload time. New system users can synchronously access medical and health data uploaded by other nodes on the blockchain through nodes, and view medical and health information shared by other users on the platform.

3.2. User design

The data provider needs to input personal medical information into the webpage and synchronize and upload the personal medical data they can provide. Then, the user data will be pre priced based on the trained medical data price, and the medical data will be encrypted and uploaded to the designated cloud storage space. Smart contracts will automatically display the type of medical data and send relevant information to the blockchain network to reach consensus and go live. Information such as data prices and medical data types will be annotated and displayed on the platform, but cannot be traded. Auditors will inspect the medical personal information data uploaded by users and grant them the authority to conduct legal transactions on personal medical data after confirming its legality. Users' personal medical data can be purchased through data sharing platforms.

Data buyers include research institutions, hospitals, universities, and certain enterprises that have a demand for medical data. After comparing their identity information with the written chain, the data buyer will send a request to the blockchain network. Upon receiving the legitimate and valid medical data key information that has been verified by the data auditor, the data buyer can view the verified medical data records on the platform and

make purchases based on the predicted price and medical data type category provided by the value prediction model. After selecting the required records and paying the corresponding fees, the platform will automatically call the smart contract, download the corresponding medical data records from the cloud, and use the encryption and decryption module in the public service module for processing. Provide decryption services for the data downloaded by the data purchaser.

3.3. Design based on blockchain consensus algorithm

Consensus algorithm is an algorithm used in distributed systems to achieve consistency. In distributed systems, the uncertainty of communication and operations between nodes may lead to differences in understanding of the system state among different nodes, resulting in conflicts. The goal of consensus algorithms is to achieve consistent decisions between different nodes, thereby ensuring the consistency and reliability of the system.

In order to meet the efficient data storage requirements and convenient access to block time on the system platform, a node synchronization scheme based on PoA consensus mechanism will be proposed. The use of PoA consensus mechanism can improve the speed of block generation, which in turn helps users meet the demand for medical data storage. The idea of the node synchronization mechanism based on PoA is shown in Figure 1.
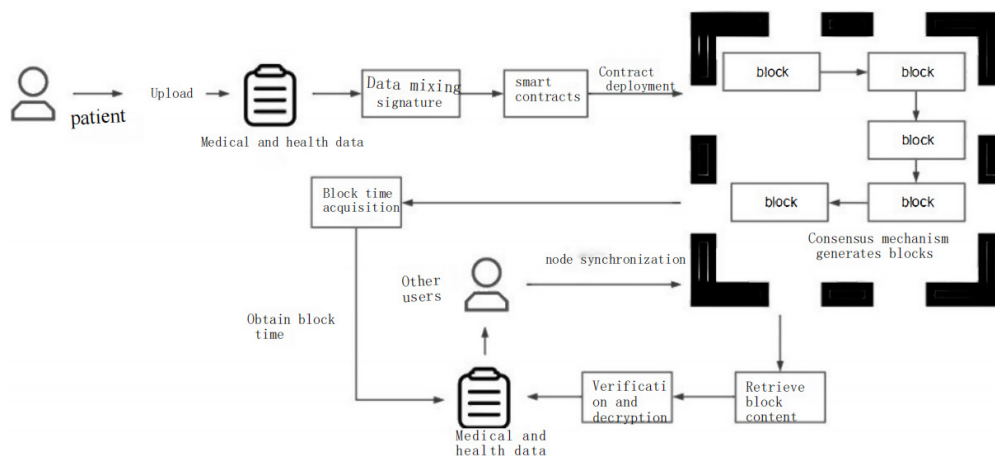

Figure 1. Overall idea of node synchronization mechanism and block time acquisition scheme based on PoA consensus.

Patients upload their own medical data, which is then processed through a consensus mechanism to generate blocks. As a result, other nodes receive the same content. When medical patients receive shared data, other patients can use the block time method to obtain the time in the block and return it.

3.4. Design of smart contracts

After the system calls the chain code to add medical data, it collects the medical data information filled in by the WEB backend user. The medical data value prediction model of the public service module predicts the medical data value of the data and adds value to the data information after receiving the predicted value. The user's complete medical data is encrypted within the public service module, and then uploaded to the cloud to obtain the cloud's data storage address and authorized access link. Finally, all key medical data information is sent to the blockchain network to achieve consensus on chain and other functions.

In the medical and health data sharing platform built on blockchain, data storage is a crucial technology. The platform utilizes smart contracts to implement the function of storing user health data on the chain, ensuring

the security and reliability of the data. The present invention provides an innovative user medical and health data storage solution, which includes text data and image data. Text data includes patient medical records, while image data includes patient laboratory test results or imaging images. During the contract transaction process, the generated transaction hash value is saved in alphanumeric format, using the same saving scheme as text data. This data storage solution not only effectively protects user privacy, but also improves the traceability and credibility of data, providing a solid technical guarantee for the sharing and utilization of medical and health data. Write smart contracts using Solidity language and complete the system using web3.js.

3.5. Cloud operation module design

There are currently two methods for storing blockchain data. Storing on chain means that all personal user data within the blockchain system is stored in blocks on the blockchain network. This method has obvious advantages and disadvantages, and its advantage is that even in the event of a hacker attack, data can be restored and resynchronized through other nodes on the blockchain network. But this will bring very high security costs to the overall system, which will also cause significant drawbacks to the storage on the chain. In fact, in order to ensure complete nodes, each node must store all the data from the system during operation. Obviously, this storage method belongs to an expensive multi storage solution. On chain storage solutions are only suitable for situations with very small amounts of data or can be applied to situations with very small amounts of data. Due to the limited scalability of current blockchain, it is impossible to store the most complete user profiles. If all running nodes can save all user data, and each node needs to continuously synchronize with each other, each user only needs to upload a few megabytes of data to achieve extreme congestion and overload of the blockchain network, which causes a very bad user experience. In addition, it requires a lot of maintenance costs to ensure the normal operation of the entire system.

The medical data purchasing system will automatically authorize access links through smart contracts, so that data buyers can download and decrypt medical data. Smart contracts are intelligent programs written by system developers that can automatically execute, ensuring that data buyers can access and decrypt data smoothly. The system will verify the identity of the data purchaser to ensure that only authorized users can access and use the data, and record the usage and access records of the data for auditing and tracking when needed. This intelligent data purchasing method facilitates data buyers to obtain medical data while ensuring the security and integrity of the data. Based on it, store and call the front-end and back-end.

4. Summary

This article discusses the situation of medical data sharing platforms, and the common problems that exist in most industries are data loss, data leakage, and unreliable third-party platforms. To solve this problem, we need to integrate blockchain technology and machine learning cryptographic algorithms together. The decentralized, tamper proof, and traceable characteristics of blockchain technology ensure the security and integrity of medical data, while machine learning algorithms provide more data support for medical research. This fusion solution effectively solves the problems in the field of medical data sharing and provides new ideas and technical support for the healthcare industry. The article proposes a medical data sharing platform based on blockchain technology. This platform has the feature of not requiring third-party institutions to recognize it, and can realize the buying and selling of medical data between data service providers and data customers, and then have data auditors verify

the reasonableness and legality of medical data. At the same time, data service providers can authorize the use of personal medical data. It is worth mentioning that the platform has the characteristics of traceable buying and selling and tamper proof.

Fund project

Author Introduction: Zhang Hui (1984-), female, born in Yulin, Shaanxi, is a professor and master's student who mainly researches big data, data mining, and computer networks.

References

[1]   Niu Guanbo Research and Implementation of a Blockchain based Medical Data Sharing Platform [D] Harbin Institute of Technology, 2020.DOI: 10.27061/d.cnki.ghgdu.2020.000661.

[2]   Tang Weiwei Design and Implementation of a Cloud Computing based Regional Medical Information Data Sharing Platform [D] PLA Hospital, 2015.

[3]   Niu Bo Design and Implementation of a Blockchain based Healthcare Data Sharing Platform [D] Guangdong University of Technology, 2020.

[4]   Xu Gang, Zhao Jingyue, Cai Lianzhong Design and Implementation of Medical Information Sharing Scheme Based on Data Exchange Platform [J] Digital Technology and Applications, 2012 (08).

[5]   Xiong Chuanmei Design and Implementation of a Regional Medical Information Data Sharing Platform Based on Cloud Computing [J] Digital Technology and Applications, 2016 (10).

[6]   Helin Research on the Theory and Practice of Constructing a Regional Medical Information Sharing Platform [D] Tianjin Medical University, 2010.