IJIRR

International Journal of Information Research and Review
Vol. 05, Issue, 12, pp.5971-5975, December, 2018

RESEARCH ARTICLE

STUDY ON THE APPLICATION OF BLOCK CHAIN TECHNOLOGY IN SMART MEDICAL INFORMATION STORAGE

***Wei Wang, Qiming Wang and Gaomin Zhang**

College of Information Engineering, Pingdingshan University, Pingdingshan 467002, China

ARTICLE INFO

Article History:

Received 19th September, 2018
Received in revised form
26th October, 2018
Accepted 12th November, 2018
Published online 20th December, 2018

Keywords:

Block chain technology,
Smart healthcare,
Health privacy,
Information sharing.

ABSTRACT

The informatization of personal medical data is one of the key tasks of smart healthcare construction and how to securely store and share information, and make effective use of personal medical information has become a key direction for researches on smart healthcare. Based on the introduction of the development history of block chain technology in Bitcoin application field and the demand characteristic of safe storage of smart medical information, this study first analyzes the applicability of block chain for storage of personal health data, then proposes a solution scheme to realize the safe storage and sharing of smart medical information by using block chain technology, targeting individuals, doctors, and medical institutions, in which the interfaces of the network layer and application layer through algorithms are elaborated, and the personal medical information data is encrypted and stored in the block chain network to ensure that individuals have absolute read access to their own medical information.

INTRODUCTION

In August 2014, 8 ministries, including the National Development and Reform Commission and the Ministry of Industry and Information Technology of China jointly issued the "*Guidelines on Promoting the Healthy Development of Smart Cities*" (Guiding opinions on promoting the healthy development of smart city, 2014) to ensure the healthy development of smart city construction in an orderly manner. Smart healthcare is an essential component in the construction of smart cities, and its core lies in the safe storage of medical information (Yuan and Wang, 2016; He *et al.,* 2017; Mei, 2017; Zyskind *et al.,* 2015; Karame *et al.,* 2012). In the "Thirteenth Five-Year Plan" of the State Health and Family Planning Commission, it is explicitly stated that the construction of personal electronic health files is one of the key tasks in the national health informatization construction of China, and that efforts shall be made to gradually realize the national unified residents' electronic health files and implement standardized management. In order to ensure the safety of medical information and reduce the occurrence of information leaks, relevant regulations and documents concerning the protection of information security are issued in laws and policies. Domestic scholars have also conducted a lot of researches on the safe storage of smart medical information. Gao Wei and Fu Chunyu proposed an architecture design based on FCSAN+IPSAN+NAS and analyzed the corresponding data backup scheme, but its complex structure was not conducive to practical application. Shu Xiaowen made a brief analysis of the concept of cloud storage in an article themed the application of cloud storage in hospital informatization, with focus only on advantages and disadvantages of cloud storage. Therefore, in order to ensure the safe storage of smart medical information, it is necessary to conduct researches centering on security, architecture, and systems in the construction of the system platform, which will be of high research value and application value (Christidis and Devetsikiotis, 2016; Lewenberg *et al.,* 2015). This article helps to solve centralized storage of information, excessive reliance on third party for the reliability of data, and other practical issues in smart healthcare based on the block chain technology and the requirements of medical information storage, achieving de-centralized, safe and reliable sharing of intelligent medical information data.

Corresponding author: **Wei Wang,**
College of Information Engineering, Pingdingshan University, Pingdingshan 467002, China.

Applicability of block chain for storage of personal private health data

Block chain technology: Blockchain is the underlying core technology of Bitcoin applications, which uses a distributed data structure, and can record all metadata and transaction information during the transaction process of Bitcoin system (Godsiff, 2015; Godsiff *et al.,* 2015; Kraft, 2016; Kraft, 2016). The blockchain hasn't attracted the attention of researchers until the article *The Promise of the Block chain: The Trust Machine* was published in *Economist* in 2015, which

concluded that it would have a profound impact on the current information storage security and human social life, based on the analysis of the various technical aspects of the blockchain. Decentralization is the core strength of this technology, which achieves a point-to-point transaction based on centralized credit in a distributed system where the nodes do not need to trust each other, using time stamps, data encryption, distributed consensus, and economic incentives, so that the parties to the transaction no longer need to ensure the reliability of the transaction through the third-party notary agency, thus the solutions to high transaction costs, low work efficiency, data storage security and other problems commonly seen under the centralized architecture model can be found. In recent two years, more and more disciplines have been applied to study block chain, and its rapid development has attracted wide attention of financial institutions and governments (Wilson and Ateniese, 2015). The People's Bank of China stated in early 2016 that it would actively promote the official issuance of a digital currency, and then the British government has also issued a special report, "*Distributed Ledger Technology: Beyond Block chain*" (He *et al.,* 2017). The McKinsey study (Mei, 2017) clearly pointed out that block chain technology would be the core technology that has the most potential to spark the next wave of disruptive technological discoveries after steam engines, electricity, information, and Internet technologies.

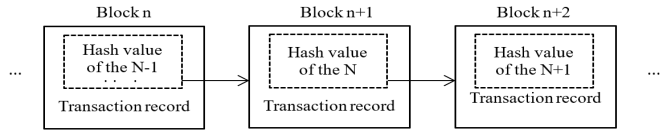

Fig. 1. Basic data structure of block chain

Personal private health data: Speeding up the electronization of personal private health data is a key step in achieving smart health care, which is conducive to improving the utilization rate of data and realizing the sharing of health data, so as to provide big data analysis for personal health through data analysis and fully explore the potential value of health data. However, there are still many problems as the following in the construction of personal electronic health files at this stage. The laws and regulations of medical privacy protection are still incomplete and patients cannot participate in the access control strategy of electronic health files, thus personal privacy cannot be well protected. Decrypted medical data is faced with many malicious attacks. The existing storage technology cannot achieve data traceability. Big data knowledge mining has the risk of predicting and leaking privacy. As more high-tech medical technologies such as portable wearable health monitoring devices, translational medicine and gene sequencing emerge and become popular, an increasing amount of personal electronic health information access networks, posing great impact on people's interest and bringing serious challenges, which has exceeded the scope of researches of traditional information security and privacy protection. Therefore, it is of high social value and important practical significance to study on how to improve the safe storage and protection of personal private health data.

Applicability study: Personal private health data and block chain technology have similarities in physical logic. The electronization of personal private health data can be attributed to the category of electronic files. An electronic file refers to a digital file which is converted from a file with storage value in text or images and stored on a computer disk device through computer-related technology, which become the electronic data processable by a computer system. By comparing block chain technology and personal private health data, it can be found that both need to store useful data with high security requirements. Block chain technology can guarantee the security of personal private health data, as the technology focuses on the trust and security in the transaction process, which can not only improve the convenience of private information management, but also improve the security of private data. More importantly, the block chain technology can guarantee the authenticity of personal private data, and prevent the illegal tampering of the data. The application of block chain technology to the safe storage and protection of personal private health data can guarantee the integrity of the original data, processed data and personal medical information in the actual application of current smart medical information.

Design of key applications

Hash algorithm: Hash algorithm is widely used in block chain network, which is constructed based on hash function and is mostly used for data integrity and encryption. A good hash algorithm can achieve fast forward, difficult reverse, input sensitivity, and collision avoidance. Two cryptographic hash functions, SHA256 and RIPEMD160, are commonly used in block chains, among which the latter is mainly used to produce Bitcoin addresses. In block chain technology, instead of saving data to be stored, the hash value of the data is stored. In addition, in order to guarantee the reliability, many signature mechanisms are applied in the block chain, and these signatures are mostly obtained by calculating the private key and the data need to be signed with hash algorithm.

Consensus agreement: Consensus protocol is the key technology used to solve the trust issue among network transaction users in network topology, which is also the key technology in block chain network. In Bitcoin applications, network nodes need to agree on the order and correctness of the transactions contained in the newly dug-out block to ensure the consistency of the block copy of the node and prevent the block chain from splitting. The choice of consensus algorithm is highly related to the application scenario, for example the trusted environment uses paxos or draft; the licensed alliance can use pbft; and the unlicensed chain can use the pow, pos and rip consensus, etc. The consensus mechanism can be freely selected according to the trust degree of the opposite party. In the Bitcoin network, more than half nodes are trusted nodes by default, and the network consensus mechanism of "minority obeying the majority" is generally adopted.

Smart contract: The term "smart contract" which dated back to 1995 at least, was proposed by Nick Szabo, a prolific and cross-disciplinary legal scholar. A smart contract is an event-driven, stateful program that runs on a replicable and shared ledger and is capable of keeping assets on the ledger [5]. In essence, the smart contract works like the if_then in programming language. When the assumed condition is met, the smart contract will be triggered to execute the set terms. It can assume different functions at each node, serving as an interface for each node in the block chain to interact with the outside world and using the consensus protocol for synchronization and consensus. The block chain support programmable contracts, thus has the advantage of de-centralization, non-tampering, transparent and traceable processes, etc.

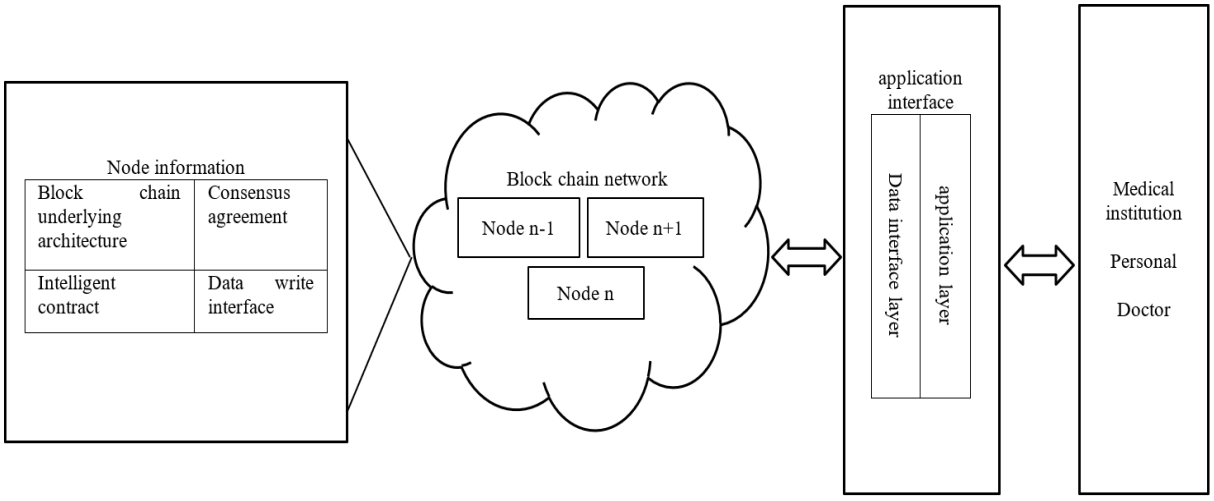

Fig. 2. Blockchain network architecture for smart medical information storage

It uses state machines and adopts transaction processing and preservation mechanisms to ensure that various smart contracts are accepted and processed on the block chain.

Time stamp service: Blockchain technology has been developed in the practical application of Bitcoin. In Bitcoin transactions, it is necessary to avoid double-spending or "counterfeit currencies", that is, the same Bitcoin cannot appear in two transactions at the same time. The centralized national monetary system ensures the authenticity of the currency through the mandatory of the national machinery, while the decentralized block chain system completely relies on the time stamp technology to avoid double-spending. During the transaction process, the block chain system marks each successful transaction with a time stamp to prove that the transaction hasbeen done and that the ownership of funds in the transaction has been transferred. If the previous owner uses the funds to trade again, it will report an error. In order to ensure that the linked list of the block chain develops correctly in time sequence, the system will also add the correct timestamp for each block.

Scheme design

Architecture design: This scheme uses block chain technology to realize the safe storage and sharing of smart medical information. The entire block chain is mainly composed of block chain networks formed by medical institutions, doctors, and individuals, with doctors and individuals as the main service targets. The overall design framework for the scheme is shown in Figure 2. Medical information can come from different medical institutions. After being authorized, the doctor can review the individual's medical information and give diagnosis, and then provide him with medical records and re-store these records in the block chain network. Individuals can visit different medical institutions and have ownership and control of personal medical information. In smart medical information storage, individuals use the access control and data storage to participate in transactions in an anonymous manner. The information stored in the block chain is public, and the sensitive personal medical information involved in the transaction will not appear in the storage area on the block chain network. Each node maintains its own data information in the block chain, and then the block chain network automatically synchronizes and encrypts this information, ensuring the consensus of all nodes in the block chain network. The block chain network provides the data entry interface to each node, and each node can complete the data addition, modification, query and deletion in the block chain by simply calling the data entry interface without changing the original service structure. Nodes in the application layer and block chain networks interact with the block chain network through smart contracts.

Network layer node design: The network layer includes smart contracts, consensus algorithms, distributed ledgers, point-to-point protocols, and ledger storage to ensure reliable communication between peer nodes in a P2P network. Smart medical information is stored on different blocks in the entire network. Each node in the block chain can generate information and receive configured smart medical information and they maintain consistency of communication by keeping a common ledger. Each node in the network in the block chain can create a new block and send it to the entire network through broadcast. The node that receives the new block information verifies the block information. If verified, the block information is forwarded to the network. If the block information can be recognized by most nodes, the block is added to the block main chain to realize the storage of medical information. A smart contract is an interface between a block chain network and an external interface, which can be added, queried, modified and deleted in a block chain network using HTTP/POST requests or command lines. The network where Bitcoin is located is a fully open block chain network, to which the consensus algorithm used must conform. Among them, PBFT and Raft are commonly used consensus algorithms in the alliance chain and private chain, while PoW (adopted by Bitcoin) and PoS in the public chain. The block chain network storing medical information is a kind of alliance chain, so Byzantine algorithm is adopted as the consensus algorithm in the block chain network. The distributed ledger is a database owned by each node in the block chain network. When each node enters the smart medical data information, the consensus protocol synchronizes the data of all the nodes in the network. Because the amount of medical information stored each time is not too large, using cksDB database to store the text in the account book can meet the requirements.

Application layer interface design: The application layer interface mainly refers to the interfaces designed respectively for individuals and doctors, which provide them with application interfaces for the input and query of smart medical information. Blockchain smart contracts already provide

HTTP/POST type request interfaces, which will be based on the WEB platform and uses Spring MVC as the architecture, Java and HTML as the development language, and MySQL as the database in the application layer design. Specifically, its applications include smart medical information input interface, information inquiry interface and information modification interface used by doctors. The system interface used by the individual includes the login interface and the information inquiry interface, where the doctor can add and modify the medical information of the individual after being authorized by him. The block chain operations specifically used for storing smart medical information are respectively implemented by Algorithm 1 for releasing medical information, Algorithm 2 for storing medical information, and Algorithm 3 for querying medical information.

Algorithm 1: Releasing medical information

begin

The doctor produces a case and its corresponding hash value;
It is broadcast to the block chain of smart healthcare, after the signature (hash value + medical institution private key) is done;

Encrypt (encryption (case + symmetric key) + personal public key) information;

Send encrypted messages to individuals;

end

Algorithm 2: storing medical information

begin

The individual uses his own private key to extract the symmetric key from the encrypted medical information;

The individual uses the extracted symmetric key to extract the hash value and the medical information;
The individual uses the public key issued by the medical institution where the doctor is located to verify the correctness of the signature;

If correct

The hash value is calculated from the medical information and compared with the hash value extracted with the symmetric key;

If hash value is consistent

The medical information is correct and the verification is successful;

else

abandon it;

else

abandon it;

if data validation is successful;

Store medical information in the block chain and record the storage location;

end;

Algorithm 3: querying medical information

begin

Extract the request public key and the demand information according to the received request data;

Search for the URL and the encryption key of the information in the block chain according to the information demanded;

Create an access control transaction and record response information in the transaction;

Broadcast the transaction in the medical block chain network

end

Conclusion

Block chain technology provides a highly secure distributed storage mechanism for the storage and recording of smart medical information, so that personal medical information can be owned and controlled by individuals. Medical information stored on the block chain can also be shared by medical and scientific institutions under the authorization of individuals, provides basic data support for big data analysis of the overall health status, and opens up the key link of safe storage of and access to smart medical information for comprehensive smart healthcare. There are many other Block chain technologies need to be studied in smart healthcare, such as the application of comprehensive analysis of medical information on block chain, the application of overall personal health assessment, etc., so that smart healthcare can truly realize the reliable, safe, convenient and efficient service for human beings through the researches on these technologies.

Acknowledgments

This work is supported by Science and technology project of Henan Province in 2016 (Item No.162102310248), Youth Fund Project of Pingdingshan University in 2013 (Item No. PDSU-QNJJ-2013001).

REFERENCES

Bandara HMND, Jayasumana AP. 2013. Collaborative applications over peer-to-peer systems—Challenges and solutions. *Peer-to-PeerNetworking and Applications*, 6(3):257-76-[doi:10.1007/s12083-012-0157-3]

Christidis, K., Devetsikiotis, M. 2016. “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, Vol.4, pp.2292-2303.

Godsiff P. Bitcoin: bubble or blockchain. In: Proceedings of the 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KES-AMSTA). Sorrento, Italy: Springer, 2015, 38: 191−203

Godsiff, P. 2015. “Bitcoin: Bubble or Blockchain,” *Agent and Multi-Agent Systems: Technologies and Applications. Springer International Publishing*, pp.191-203.

Guiding opinions on promoting the healthy development of smart city, 2014. People's Republic of China's national development and Reform Commission, 20140827.

He, P.,Yu, G.,Zhang, Y. F. 2017. “Survey on Blockchain Technology and It's Application Prospect,” *Computer Science*, Vol.44, No.4, pp.1-8.

Karame, G. O., Androulaki, E., Capkun, S. 2012. "Double-spending fast payments in bitcoin," *ACM Conference on Computer and Communications Security, ACM*, pp.906-917.

Kraft D. Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications, 2016, 9(2): 397−413

Kraft, D. 2016. "Difficultycontrol for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, Vol.9, No.2, pp.397-413.

Lewenberg, Y., Sompolinsky, Y., Zohar, A. 2015. "Inclusive Block Chain Protocols," *FC,* pp.528-547.

Mei, Y. 2017. "Research on blockchain method for safe storage of medical records," *Journal of Jiangxi Normal University*, Vol.41, No.5, pp.484-490.

Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proc.of the 1st Int'l Conf. on P2P'01. IEEE, 2001.101-102.[doi: 10.1109/P2P.2001.990434]

Sweeney, L. 2002. "K-anonymity: a model for protecting privacy," *International Journal of Uncertainty,Fuzziness and Knowledge-Based Systems*, Vol.10, No.5, pp.557-570.

Wilson D, Ateniese G. 2015. From pretty good to great: enhanc-ing PGP using Bitcoin and the blockchain. In: Proceedingsof the 9th International Conference on Network and Sys-tem Security. New York: Springer International Publishing, 9408: 368−375

Yuan, Y., Wang, F. Y. 2016. "Blockchain: The State of the Art and Future Trend,"*Acta Automatica Sinica,* Vol.42, No.4, pp.481-494.

Zyskind G, Nathan O, Pentland A S. 2015. Decentralizing privacy: using blockchain to protect personal data. In: Proceedingsof the 2015 IEEE Security and Privacy Workshops (SPW2015). San Jose, CA: *IEEE*, 180−184

Zyskind, G., Nathan, O., Pentland, A.S. 2015: "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Security and Privacy Workshops. IEEE Computer Society*, pp.180-184.

****