# Automatic Encryption Algorithm of File Sensitive Information Based on Blockchain Technology

**Xuliang Yang**

Guangzhou University Sontan College, Guangzhou, 511370, Guangdong, China

249082550@qq.com

**Keywords:** Blockchain, Files, Security

**Abstract:** Through the design of the electronic health archive information system based on the blockchain technology, this paper explains how to apply the blockchain technology to ensure the safety and integrity of the electronic health archive, protect personal privacy and promote the sharing of the electronic health archive, so as to realize the promotion of the electronic health archive.

## 1. Introduction

The 13th five year plan of the State Council, which promotes the equality of basic public services, establishes the objective requirements of electronic health records service for the residents of cities and places in the population of residents under its jurisdiction in order to unify the standardized residents. The filing rate has gradually reached more than 90%[1]. Electronic health records are based on the personal health of residents and realize the whole process of residents' life. It covers a variety of health-related factors, realizes the dynamic collection of multi-channel information, and satisfies the information resources of residents' self-health, health management and health decision-making. Electronic health records can improve the quality of medical services, reduce medical costs, meet the needs of disease management, and promote the rational distribution of medical resources. The current research focuses on the practical application information system with core EHR. The data structure of these information systems is mainly the traditional centralized database[2]. They face the integration of security, privacy and electronic health records. The problem is. Bitcoin application based on blockbuddy technology fully proves that blockchain technology solves the above problems. This paper introduces the independent design of electronic medical record system based on blockchain technology, and explains the method of promoting the application of electronic medical record.

## 2. Blockchain Overview

The blockchain Technology launched in 2008 is Nakamoto. It is based on the continuous combination of data blocks by encryption to form a constant time series of improper data. It uses P 2p protocol to store data on network nodes, and uses consensus algorithm to update and share metadata. Ethereum puts forward intelligent contract operation data by blocking chain stores to record changes of state. Generally speaking, blockchain encryption technology and similar blockchain structure are implemented through data validation and storage, and the assigned nodes are generated and refreshed through protocol algorithm data. Distribute infrastructure and distribution through automated scripting code (smart contracts)[3]. 3. Technical basis of blockchain: 1. Blockchain cannot be changed or deleted. It can add data records to ensure its consistency and reliability. In order to ensure the robustness of data, local decentralization is not weaker than attack, so it must be blocked. Four. Nodes in the network can share data equally[4]. Three blocks, using encryption and consensus algorithm, audit the user identity, verify the validity of the data, and confirm the reliability of the data. In addition, the security blockchain is now divided into public block, joint block and private block. March 81. Public blockchain refers to the process that any

DOI: 10.25236/cseem.2020.062

individual or group can participate in the blockchain based record, and each node stores the blockchain and participates in consensus update[5]. Block refers to the process of specifying a pre selected node in the industry. The pre selected nodes store the blockchain and participate in the consensus update process. Other users please participate in the transaction process and save, not in the blockchain update process. The storage update right of private blockchain is similar to that of storage update system. The application of block is still in the exploration stage. Research 191 based on Xiaoou et al applies blockchain technology to manage health information system. One percent of the study was conducted by Zixia et al. The authorization management system based on blockchain technology is designed. This system allows the invited and effective users to see the health profile information[6]. Designed by azaaria and other Med RECs. N use information block technology to establish the true owner of the patient's electronic health record. At the same time, the application of smart contract realizes the functions of authorization, authentication and automatic supervision. The research based on these technologies is that the use of health archive information in the decentralized system of blockchain stores can promote the proof. However, most of these systems are recognized and managed, and the implementation of information storage is also centralized database mode. The system studied in this paper also uses blockchain technology to store health files[7]. This is a centralized network deployment, used to encrypt health files, protect information security, and promote the use of health files.

Table 1 Comparison of public chain, private chain and alliance chain

|  | Public chain | Private chain | Alliance chain |
|---|---|---|---|
| Centralization | No center | Centered | Multicenter |
| Participant | All | Control center decision | Preset members |
| Bookkeeper | All participants | Control center decision | Consult |
| Trust mechanism | Proof of work | Endorsement on its own initiative | DPOS |
| Advantage | To the center, to trust | Low energy consumption | Can control permissions |
| Shortcoming | Limited trading capacity | Access node Limited | Can't solve the information problem completely |

## 3. Definition and Characteristics of Blockchain

Blockchain Technology: data validation, hydraulic, for the use of blockchain data structure, data generation between nodes is assigned, in order to update the algorithm used consistently, the safe communication and operation of data, and to determine the use of encryption algorithm. Bblast is not an innovative technology, but a way to integrate the recording, storage and performance of existing technology data. In today's situation of lack of trust, blockchain network can reach a consensus without reliable nodes and channels. Blockchain network has the following four characteristics.

### 3.1. Distributed and Decentralized

The nodes in the network are completely distributed. The network is highly free, weakly coupled, highly available and scalable. There is no third party to manage the whole network.

### 3.2. Traceability and Anti Tampering

The matching algorithm used in the blockchain can ensure the matching and matching of all data in the system. When a block enters a block, it is the only one that can be browsed, broken, or changed. This form of distributed record ensures the authenticity of data, so the database based on blockchain has great security advantages in the traditional database.

### 3.3. Autonomy and Reciprocity

Because blockchain network is essentially a P2P network, the nodes in the network are all homologous. Nodes can freely join or leave the blockchain network without being constrained by the network. When some nodes are shut down, the network can still operate normally.

### 3.4. Automatic Execution in Accordance With the Contract

Data or fund transactions, records, queries, etc. in blockchain network are automatically executed according to the pre written procedures, transforming the trust of each institution into the trust of network and code, greatly reducing the cost of human and financial resources.

## 4. Blockchain Classification

Blockchain can be divided into three types: public chain, private chain and alliance chain. A common chain is a common block. Anyone can read and write a transaction and confirm that the transaction is valid[8]. Everyone can participate in the consensus process of blockchain. The consensus mechanism will determine whether blocks can be added to the blockchain to indicate the current situation. Because its security is a very important feature of this public management chain, it is correct. Therefore, the common consensus mechanism of public chain is the proof of working mechanism, which is a fair authentication mechanism to compete in computing power. How it works: participating nodes make more contributions and get more rewards. The problem of public chain is that the number of nodes is not fixed, the number of online nodes cannot be guaranteed, and the nature of nodes cannot be judged. General public chains are: bitcoin, Ethereum and other private chains are completely private blocks, that is to say, block read and write permissions are completely controlled by individuals or organizations and are not public[9]. Different from the public chain, after entering the private chain, the manager needs to perform authentication, and the authenticated individual or group has read permission. The closed environment of private chain can control the number and state of nodes, and has high security. If the competition method of calculating power is used to reach a consensus, the calculation cost is relatively large[10]. Private chain enterprises can use equity to reach consensus among nodes, such as POS, and entrust equity certification with higher cost efficiency and efficiency. The problem brought by private chain is that the concentration is too high, which violates the original intention of blockchain. Alliance chain is the block of two alliances and the block form between public chain and private chain. Generally, it refers to the management of blockchain by multiple organizations or institutions, recording transactions and data together. Only these organizations can record transactions and data. Like the private chain, the alliance chain also has access permission setting and identity authentication functions, which can dynamically change the number of nodes in the whole system. Because the number and state of nodes can be controlled, the consensus mechanisms suitable for reaching consensus of sensor chain nodes include DPO, practical Byzantine fault tolerance (pbft), etc.

## 5. Fundamentals of Cryptography Technology

The security of blockchain technology is based on cryptography. Therefore, encryption technology is very important for blockchain. Using correct and secure encryption method can improve the ability of blockchain to prevent tampering. Common encryption algorithms can be divided into symmetric encryption and asymmetric encryption

### 5.1. Symmetric Encryption Algorithm

In the symmetric encryption algorithm, the data encrypted text of the data sender is converted into the use of the key, and then the password key is sent to the receiver through the receiver for the public channel. After receiving the key and ciphertext, the receiver uses the inverse algorithm of encryption algorithm to decode the key to obtain the plaintext of the data. The typical feature of symmetric encryption algorithm is that encryption and decryption keys are the same. Therefore, the key must be transmitted reliably, or in order to ensure the confidentiality and integrity of the data, the receiver and the receiver must know the key in advance. Because of encrypting and decrypting the shared key, the algorithm has less computation and high speed and efficiency. However, when encrypting a large amount of data, the key transmission and management are difficult, the security is difficult to guarantee, and the symmetric encryption algorithm cannot verify the signature. It represents the process of basic symmetric encryption algorithm.

### 5.2. Asymmetric Encryption Algorithm

Asymmetric encryption algorithm is also known as public key encryption system. Different from the symmetric encryption algorithm using the same key for encryption and decryption, the asymmetric encryption algorithm has a public key pair and uses different keys between encryption and decryption. Therefore, compared with symmetric encryption algorithm, the speed of encryption and decryption of public key is slower, but there is no problem of key transfer and security. At the same time, public key encryption can be used for digital signature verification. A simple public key cryptosystem model. Alice, the sender, sent Bob a message, but she didn't want anyone except Bob who knew her message. So Alice uses Bob's public key to encrypt the information she sends. With his private key, he can read the message sent by Alice normally. Similarly, if Alice wants to let her know that Bob didn't come from another identity, but sent the message herself, Alice can use the private key to encrypt the message.

## 6. Conclusion

The rapid development of Internet technology, not only provides a broad market for Internet applications, but also brings a lot of convenience to our life, but also more or less there are some problems. Every field is closely related to our life. With the transformation of big data from cabinet storage to electronic medical record, more and more fields use the third-party cloud server to store and share user personal data.

## Acknowledgements

Fund project: education department of guangdong province/young innovative talents project (natural science)/exploration and practice of education informatization based on block chain technology project No. : 2018KQNCX355

## References

[1] Engelenburg, S. H. V., Janssen, M. F. W. H. A., Klievink, A. J. Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology. no. 5, pp. 1-24, 2017.

[2] Shi-Cho, Cha., Shih-Cheng, Hung., Jyun-Fu, Chen. On the Design of a Blockchain-Based Reputation Service for Android Applications. Advanced Science Letters, vol. 23, no. 3, pp. 2179-2184, 2017.

[3] Singh, Madhusudan., Kim, Shiho. Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain. Optical Engineering, vol. 33, no. 1, pp. 701-709, 2017.

[4] Shufan, Zhang., Lili, Wang., Hu, Xiong. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. International Journal of Information Security, no. 2, 2019.

[5] Zhang, Chenggang. The Era of Blockchain: Technological Development, Social Progress and Risks and Challenges. Frontiers, 2018.

[6] Ivan, Tarkhanov., Denis, Fomin-Nilov., Michael, Fomin. Application of public blockchain to control the immutability of data in online scientific periodicals. Library Hi Tech, no. 4, 2019.

[7] Nurzhan, Zhumabekuly, Aitzhan., Davor, Svetinovic. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840-852, 2018.

[8] Gaoqi, Liang., Steven, et al. Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks.

[9] YongJoo, Lee., Keon, Myung, Lee. Sang, Ho, Lee. Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment. Peer-to-Peer Networking and Applications, no. 4, 2019.

[10] Xu, Y., Zhao, S., Kong, L., et al. ECBC: A High Performance Educational Certificate Blockchain with Efficient Query, 2017.