Design of traceability system for medical devices based on blockchain

Xiaoling Xia¹, Xiaolin Lin¹, Wenbin Dong² and Zhi He²

¹ College of Computer Science and Technology, Donghua University
² Shanghai Shengfutong Electronic Payment Service Co., Ltd.

Xiaoling Xia: sherlysha@dhu.edu.cn
Xiaolin Lin: linxl0627@163.com
Wenbin Dong: dongwenbin@shengpay.com
Xiaoling Xia: hezhi@shengpay.com

Abstract. Aiming at the centralization problem of the traditional medical device traceability system, this paper proposes a medical device traceability system based on blockchain technology. By integrating the traditional tracing system with the blockchain technology, based on the decentralization and non-tamperability of the blockchain, the alliance chain and the smart contract construction system are adopted. Manufacturers, distributors, hospitals and consumers in the system can access product information and trace the entire circulation process of the product through RFID. In addition, consumers do not need to register an account number, but directly through the RFID query products related to the main information, such as the shelf life, production enterprises, production time, product price, etc. This system solves the problem that the traditional system is vulnerable to network attack due to centralization, which can improve the robustness of the system, enhance the reliability of data and realizes the traceability of the production, sales and use of medical devices. Therefore, it ensures that the source of medical devices can be traced, the flow can be tracked, the information can be inquired and the responsibility can be investigated to ensure the public consumption safety.

1. Introduction

The quality and safety of medical device products is related to human life and health, and has been widely valued by the society. Its high risk determines the necessity of establishing a traceability system. Tracking medical devices not only reduces medical accidents, but also prevents the spread of counterfeit or unqualified medical devices. It also helps companies find the source of the problem and determine the flow of the same batch of products, and ensure the rights of consumers. A perfect medical device traceability system can improve the brand reputation of enterprises, control the quality and safety of medical devices, and facilitate the rapid and accurate recall of problem products, which has important theoretical significance and application value.

At present, the existing medical device traceability system is a medical device tracking system based on the Internet of Things technology designed by radio frequency identification technology [1-2]. The system is based on centralization with one database in the system, which can not completely solve the problem of centralized management of product traceability system and easy tampering of data. There are doubts about the true of traceability information. If the data is tampered with, it will
seriously affect the recall of products and the circulation of counterfeit products. The occurrence of this situation will be related to the safety of patients. Therefore, the problem of centralization in the system needs to be solved urgently.

This paper proposes a medical device traceability system based on blockchain technology. It uses a blockchain consensus mechanism, distributed storage, encryption and other technical features to establish a decentralized traceability system, which can solve the problems of malicious tampering of intermediate link data and unknown data sources in the traceability system for medical devices.

This study adopts the form of smart contract to integrate into the alliance chain, so as to achieve partial decentralization while guaranteeing the transaction speed, while ensuring the security and transparency of the system.

2. Blockchain technology

2.1. Blockchain Overview
Blockchain is a new application mode based on distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other computer technologies. It is essentially a decentralized database. At the same time, as the underlying technology of bitcoin, it is a series of data blocks associated with cryptographic methods. Each data block contains a batch of information of a bitcoin network transaction, which is used to verify the validity of its information (anti-counterfeiting) and generate the next block with the characteristics of data consistency, tamper-proof, traceability and decentralization[3].

2.2. Blockchain model and platform
The blockchain mainly includes three types: public chain, private chain and alliance chain, which have different characteristics and are adapted to different occasions. The public chain is the earliest blockchain and the most widely used blockchain. Any individual or group in the world can send transactions, and the transaction can obtain valid confirmation of the blockchain. Anyone can participate in the consensus process. It has the characteristics of decentralization, low access threshold and data can not be tampered with. Private chain: only use the blockchain general ledger technology for accounting, a company or an individual, exclusive access to the blockchain. This chain is not much different from other distributed storage solutions. However, its transaction speed is very fast, which provides protection for privacy. Ant Financial is a typical representative of the private chain. The alliance chain is a kind of multi-centralization, which is between the public chain and the private chain. Multiple pre-selected nodes within a group are designated as bookkeepers, and the generation of each block is decided by all pre-selected nodes (pre-selected nodes participate in the consensus process). The respective characteristics of public chain, alliance chain and private chain are shown in Table 1.

| Table 1. Three different forms of blockchain comparison analysis table. |
|---------------------------------------------------------------|
| Participant                                      | public chain | alliance chain | private chain |
| Consensus mechanism                                | PoW/PoS/DPoS | Distributed consistency algorithm | Distributed consistency algorithm |
| Bookkeeper                                       | All Participant | Alliance member determined | customize |
| Incentives                                       | need          | Optional        | No need |
| Degree of centralization                          | Decentralization | Multi-centered | (Multi)centered |
| Carrying capacity                                | 3million -20 million times per second | 1000-1 million times per second | 1000-10 million times per second |

Main technical features of blockchain: (1) non-tampering. Once the information is verified and added to the blockchain, it will be stored permanently. Unless more than 51% of the nodes in the
system can be controlled at the same time, changes to the database on a single node are invalid, so the data stability and reliability of the blockchain are extremely high. (2) decentralization. Due to the use of distributed accounting and storage, there is no centralized hardware or management organization in the system, and the rights and obligations of any node are equal. Data blocks in the system are jointly maintained by nodes with maintenance functions throughout the system. (3) traceability. Blockchain is a decentralized database that records the input and output of each transaction of blockchain, so that it can easily track the changes in the number of assets and transaction activities [2].

Bitcoin, Ethereum and Hyperledger are the three major blockchain technology platforms. Bitcoin provides a prototype of blockchain technology application for digital currencies represented by Bitcoin. As a public blockchain platform, Ethereum further expands the functions of Bitcoin for digital currency transactions. Hyperledger project that supports smart contracts is the first distributed blockchain platform for enterprise application scenarios [6].

In conclusion, by using the blockchain consensus mechanism, distributed storage, encryption and other technical features, the problems of possible malicious tampering of intermediate link data and unknown data source in the medical device traceability system can be solved. This study intends to adopt the organizational mode of publishing to the blockchain alliance chain in the form of smart contract, so as to achieve partial decentralization while ensuring the transaction speed and ensure the security and transparency of the system at the same time.  

3. Research on Traceability System

3.1. System Architecture Design
The basic structure of the blockchain-based medical device traceability system proposed in this study is divided into data layer, network layer, consensus layer, incentive layer, contract layer and application layer. Block chain technology is mainly used in data layer, network layer, consensus layer and application layer of the framework. The data layer is responsible for distributed storage of the digitally collected data, and records the data in the Merkle tree of the block body. All the data in the Merkle tree is hashed to the root of the Merkle tree, and the root value is saved. In the block header, the 80 bytes of data of the previous block header are SHA256-operated as the parent hash value of the current block, forming a hash chain structure, and the block is time stamped with a digital signature. Once the block is formed, it cannot be tampered with. The network layer is responsible for data dissemination and verification. The source location, attributes, authentication and other data involved in the entire life cycle of the product are connected to a specific project or batch ID. The certificate authority uses the key owned by the participant and the medical device ID number to determine the node's authority. After receiving the data uploaded by each link, the node broadcasts to the entire network through the P2P network. During the process of data transfer, the ownership of the product is transferred. After the agreement is reached between the two nodes, digital signature (multi-signature) and time stamp are used to ensure that the information will not be tampered with. The consensus layer uses the Practical Byzantine Fault Tolerant Protocol (PBFT) to ensure that data is not tampered with by malicious nodes during network propagation and storage. Even if there are unknown nodes in the network, consensus can be reached. At the same time, unlike PoW and POS mechanisms, PBFT protocol does not need to rely on digital currency and can reduce the waste of resources caused by a large number of calculations [3].

The application layer provides corresponding permissions and interfaces for different entities. Manufacturers, distributors and hospitals can input relevant information about medical devices to the blockchain through the system interface. At the same time, enterprises and consumers can query and trace products through the system platform.

3.2. System platform Design
This design is based on the blockchain as the underlying technology, connecting the entire process of medical device traceability, and constructing a decentralized medical device traceability system. The
system is developed on the Ethereum, and Figure 1 shows the system's decentralized application architecture based on Ethereum. The Ethereum blockchain not only stores data and code, but also contains a virtual machine in each node to execute the contract code. To facilitate the construction of a web-based DApp, the system uses a very convenient JavaScript library web3.js provided by Ethereum. Web3.js encapsulates the API protocol of the Ethereum node, allowing developers to easily connect to blockchain nodes without having to write a cumbersome RPC protocol package. At the same time, the library is directly introduced into the commonly used JS framework (such as reactjs, angularjs, etc.) to construct the decentralized application [10].

Figure 1. Decentralized application architecture based on Ethereum.

The blockchain-based medical device traceability system will be traced to the system, and it is safer to complete the registration and transaction of medical devices than the traditional traceability system. The design mainly includes five major functional modules: user management, medical device information registration, medical device information query, and retroactive transaction records. The overall function diagram of the system is shown in Figure 2.

Figure 2. System Function Module Diagram.
3.3. System flow Design

3.3.1. First of all, in the traceback process, the enterprise needs to register an account in the system with identity information, and the system administrator confirms the authenticity of the identity information. After the confirmation is correct, the system automatically assigns a corresponding pair of keys, and the key determines the authority corresponding to the identity of the participant.

3.3.2. The manufacturer identifies all medical devices and inputs data such as product attributes and production companies into the system. The blockchain automatically generates a unique ID based on the obtained information and stores it in the blockchain. The system will automatically generate a time-stamped product information electronic file for each medical device.

3.3.3. After the medical device is completed, the manufacturer sells it to the dealer and finally uses it in the hospital. In this process, dealers and hospitals must check the source of the obtained medical devices in the system, and then write the manufacturer, batch number, price and other information into the blockchain to ensure the integrity and coherence of data in the block chain.

3.3.4. In the end, consumers, enterprises and related organizations can access the electronic information files of products through RFID to trace and query the entire circulation process of products. In addition, consumers do not need to register an account, they can directly query the main information related to the product through RFID, such as shelf life, production company, production time, product price, etc.

4. Conclusion

In this paper, the blockchain technology is integrated with the existing medical device traceability system, and the design of the medical device traceability system based on blockchain is proposed. Compared with traditional medical devices, it has the characteristics of decentralization, which avoid the problem of being vulnerable to cyber attacks due to the center. Moreover, the chain structure of the blockchain can effectively prevent the possibility of data being tampered with, which can improve the credibility of the data and ensure medical safety. Although this design can ensure that the data input by the system cannot be tampered with, there is no verification method and guarantee mechanism for whether the data has tampering behavior before input. Therefore, we will focus on this issue and strive to increase the practicality of this design in the subsequent research.

References
[1] Xu Zhengchao 2016 Research on medical device tracking technology based on Internet of Things technology (Changchun: Changchun University of Technology)
[2] Tian Can 2017 Design and implementation of traceability system for medical device products (Harbin: Harbin Institute of Technology)
[3] Sun Jun, He Xiaodong and Chen Jianhua 2018 Study on the Structure of Agricultural Products Traceability System Based on Blockchain vol 47 (Zhengzhou: Henan Agricultural Sciences) pp 149-153
[4] Shan Jinyong and Gao Sheng 2018 Research Progress of Blockchain Theory vol 5 (Beijing: Journal of Cryptography) pp 484-500
[5] Cao Guozhen and Yuan Zhenhui 2018 Building a traceable source innovation system based on blockchain vol 20 (Beijing: Chinese modern Chinese medicine) pp 1465-1470
[6] Nakamoto Satoshi 2008 Bitcoin: A peer-to-peer electronic cash system
[7] Xiwei Xu, Qinghua Lu, Yue Liu, Liming Zhu and Haonan Yao 2018 Designing blockchain-based applications a case study for imported product traceability (Amsterdam: Future Generation Computer Systems)
[8] Shen Xin, Zhai Qingyu and Liu Xuefeng 2016 Overview of Blockchain Technology vol 2 (Beijing:
[9] Wang Jiye, Gao Lingchao and Dong Aiqiang 2017 *Research on data security sharing network system based on blockchain* vol 54 (Beijing: Computer Research and Development) pp 742-749

[10] Zhang Dayong 2018 *Design of Community Information Resource Sharing System Based on Blockchain* vol 14 (Hefei City: Computer Knowledge and Technology) pp 37-39

[11] Lu Wei and Wen Jie 2017 *Supply Chain Management and Traceability Based on Bitcoin Technology* vol 11 (Shanghai: Computing Engineering)

[12] Yuan Yong and Wang Feiyue 2016 *Development status and prospects of blockchain technology* vol 42 (Beijing: Journal of Automation) pp 481-494