A Blockchain Application for Medical Information Sharing

Jieying Chen, Xiaofeng Ma, Mingxiao Du, Zhuping Wang
Department of Control Science and Engineering,
Tongji University
Shanghai, China
1531789@tongji.edu.cn

***Abstract*—Medical information are private and medical data are valuable for medical research. Medical information sharing is challenging as the data might be manipulated improperly and revealed during the whole operational process. Medical institutions need shared information for scientific research and develop, on the contrary, privacy issue inhibits the sharing process. In this paper, a new business process and a novel architecture for medical information sharing based on blockchain are proposed. Exploiting the advantage of blockchain in recording transactions, information can be shared and verified among parties like a distributed ledger. On the other hand, medical information can be shared securely between users without an intermediary. The main benefit is that both the information and the traces of the transaction can be distributed stored which avoid manipulation and fraud. Consequently, the value of information can be fully utilized.**

Keywords—blockchain; medical sharing; distributed ledger; hyperledger;

I. INTRODUCTION

Health issue has always been the focus of social concern, as it is the foundation of a happy life [1]. Medical information is private and medical data are valuable source for medical research, hence medical information sharing is significant and meaningful [2]. The improvement of EMIS (electronic medical information systems) and the establishment of EHRS (electronic health record systems) can effectively provide the information resources for people's medical treatment and health management decision-making. EMIS makes the work of medical institutions more efficient and offered service quality improved. With the development of the Internet and big data technologies, the interconnection between technology and medical treatment is becoming closer, however it brings many new challenges[3]. Most of the current systems are typically centralized. All of the data and the information are often controlled and managed by a third party, which makes them vulnerable. Electronic medical information systems need a more secure, reliable, and transparent technology to solve the existing problems. The blockchain technology has the potential power to solve these issues.

Blockchain is also called distributed ledger. The core feature of blockchain is a decentralized information infrastructure[4]. Blockchain can provide security [5], anonymity and data integrity without any third-party institution in control of the transactions. In a blockchain network, all nodes collectively verify a transaction before it can be recorded and approved. Data stored in a blockchain are like bills recorded in a ledger and copies of the ledger are distributed over the whole network. If most of nodes in the network approve, information of transactions will be completely stored in various ledgers, which ensures that any manipulations of a node in the system can be easily detected.

Blockchain technology emerged from the treatise "Bitcoin: A peer-to-peer electronic cash system" by Satoshi Nakamoto in 2008[6]. Blockchain is viewed as one of most important trends that will influence business and society in the coming years[7]. Blockchain is gaining massive momentum and has been embraced by many companies and entrepreneurs in different domains these years, largely due to the success of bitcoin[8]. Blockchain is the underlying technology of bitcoin. Blockchain has been applied in many fields, such as financial services, supply chain management, cultural entertainment, public administration etc. In early 2015, some European large financial institutions have explored the application of blockchain in security transactions. NASDAQ was the first to launch Linq, a securities trading platform based on blockchain technology, in December 2015. The British government released a blockchain research report in January 2016. World Economic Forum predicted that 10% of the world's GDP will be stored in the blockchain network by 2027.

Though more and more researchers start to research blockchain, blockchain applications are still scant, especially in medical and healthcare domain. Asaph Azaria et al proposed MedRec, a record management system using blockchain for medical data access and permission management[9]. MedRec suggests two mining models, the first needs to consume ether, while the second model suggests the use of medical records as rewards. Yin Mei proposed a method for secure storage of medical records based on blockchain[10], it 'mines' based on PoW (Proof of Work) which will waste a lot of unnecessary resources. Tengfei Xue et al proposed a blockchain-based medical data sharing model and discuss the principles and components of it[11], but this design encounters implementation problems. Xiao Yue et al proposed an App based on blockchain for healthcare intelligence and privacy [12], and a US startup launched the Gem Health Network based on the Ethereum.

Supported by Tongji-Qianbao fintech lab.

Most work in blockchain focusses on the systems and little attention is given to application models Hence, this paper focusses on the broader context of applications and the design of business processes. In this paper, we introduce blockchain technology and analyze the characteristics of blockchain frameworks in chapter II. Then we propose a business process in chapter III. Next, we design a blockchain architecture for medical information sharing platform and implement it in chapter IV. Finally, we evaluate the platform and summarize this paper in chapter V and VI.

II. BLOCKCHAIN TECHNOLOGY

A. A Brief Introduction of Blockchain

Blockchain technology is a comprehensive application of computer technology, which combines encryption algorithm, P2P network, distributed storage, consensus algorithm and smart contracts. The blockchain technology is decentralized, transparent, traceable, tamper-resistant and anonymous. At first, blockchain was just regarded as the data structure to record the bitcoin transactions history, while currently blockchain technology is a kind of universal underlying framework. Blockchain technology is still developing and will be applied in more fields. Wikipedia defines blockchain as a distributed database technology. Blockchain can maintain unmodifiable and continuously growing data records. Transaction is an important concept in blockchain. Blockchain is a special database where transactions can be added to but cannot be deleted, and all the operations will be recorded as transactions. The basic data structure of blockchain is a linear linked list which is linked with blocks, as shown in Figure 1. Each block contains information such as hash of pre-block, hash and address of the block, information of transactions and so on. New transactions should be added into a new block. All the nodes should reach an agreement on transactions by consensus algorithm and then transactions can be added to the blockchain. All nodes can check the validity of blocks by computing hash. A blockchain is executed in a distributed peer-to-peer network. Nodes in the blockchain network can interact with each other without needing a trusted intermediary.

B. Selection of Blockchain Framework

There are many frameworks for blockchain technology. Depending on the participants, blockchain can be divided into public chain, private chain and consortium chain. Everyone can join and maintain the public chain. Only members of one institution have access to the private chain, and the information in the private chain is not public. Consortium chain can be jointly maintained and used by several institutions, and these institutions should be authorized. Bitcoin, Ethereum and Hyperledger Fabric are the most popular frameworks. Bitcoin and Ethereum belong to public chain, Hyperledger Fabric is classified as one example of Consortium chain. The smart contract arose first with Ethereum, and it makes blockchain useful for any applications. A smart contract is a program that can automatically perform, and nodes can manipulate blockchain by it. Our platform is only available to authorized users, so we choose Hyperledger Fabric as the underlying technology for the platform. Hyperledger Fabric was designed for actual business scenarios. It has two main parts, as shown in Figure 2, including blockchain architecture and authority management. The blockchain architecture mainly includes consensus, P2P protocol, chaincode (the smart contract in the fabric is called chaincode), ledger and database. Authority management decides who can become a node of the blockchain and what permissions a node has.

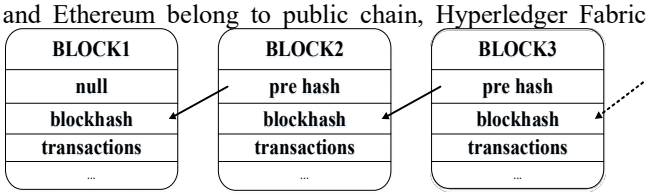

Fig. 1. Basic data structure of blockchain

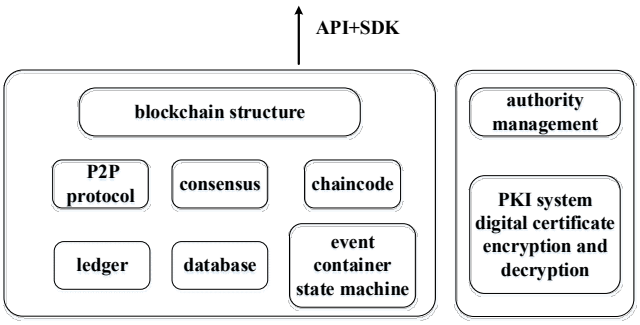

Fig. 2. Structure of Fabric

III. BUSINESS DESIGN

A. Pain points of the current medical system

Nowadays EMIS are widely used in hospitals. Meanwhile, HERS are gradually being established and improved for medical health. But there still exists some nonnegligible problems as follows:

1. The patient has no right to use his own medical records

The patient's detailed medical records are saved in the database of the hospital. Although the information in medical records belong to the patient, he is not able to get the detailed information at any time[13]. Medical examination reports are inconvenient to carry and may be lost.

2. Privacy and access

Third-party institutions lack legal approaches to pay patients for data in the medical records, so they might purchase privately. As a result, the medical records in hospitals may be abused and traded. The patient even does not know whether his medical records are used and has no right to decide whether the medical records are allowed to be used by third parties or not. All these will lead to private information leaks[14].

3. Existing medical records are not reliable

In some cases, the patient might tamper with the medical records if he has access to it, and hospital might do that as well. The existing general information system is a central system. Whether the information is reliable or not entirely depends on authoritative institutions (such as hospitals) for endorsement. Besides, the traditional database cannot guarantee the

authenticity of the electronic medical records. If the data in the database is tampered, it's difficult find it.

4. Regional constraints for platforms

It's rare that several hospitals can use the same information system today. Different hospitals rarely can share information online. If a patient is treated in different hospitals, doctors of other hospitals often do not accept previous information and examinations. Because once medical disputes occur, it's hard to distinguish responsibility. As a result, a patient needs to repeat the examination, which wastes the hospital resources and increases the cost of treatment.

5. Fails to fully utilize the value of medical records

In this era, information is value. Medical information and related statistics are great resources for medical research. The medical information is the patient's privacy, which is valuable. On the one hand, patients cannot get reword when their information is utilized. On the other hand, the third parties like research institutions cannot obtain comprehensive data.

6. High cost and low efficiency

At present, the medical insurance reimbursement requires relevant departments to review the information, which results in heavy workload. Some of the patients need to pay first, and then take relevant vouchers to apply for reimbursement, which is quite time-consuming. At the same time, the cost for complex process is high[13].

B. Bussiness process design

In order to solve the above problems well, a medical information sharing platform based on blockchain is designed. It can and mainly serves patients, hospitals and third-party institutions. There are two auxiliary objects of regulatory authorities and IoT (Internet of things) devices[15]. The structure of the platform is shown as Figure 3. Users can use the platform through the application platform, and the process and the important information will be recorded in the blockchain. The platform can provide a reliable information sharing without relying on an authority agency. In addition, the original hospital databases will still be used.

Meanwhile, this platform achieves the idea: data are values. Patients can get some rewards if they allow some institutions to view the medical data. In this way, shared ecology comes into being, as everyone can benefit from the platform[16]. A patient may go to several hospitals for treatment and have several medical records. Through the platform, he can use his medical records and authorize other institutions to view them anytime, anywhere. The hospital will generate electronic medical records and upload important information to the platform. A third-party institution can pay for medical information they need for research systematically. Activities like generating medical records, application for authorization, the use of medical records and so on will be recorded as transactions and traced in the blockchain through the platform. Regulatory authorities (medical and health management departments) and high-grade hospitals exist as nodes in the blockchain. The nodes in the blockchain can regulate the legal members of the platform and monitor the use of the medical records. A new user needs to register and be authorized by nodes in the blockchain, then he can use the platform together with other existing users. This approach greatly enhances system scalability and provides a great convenience for patients treated in different hospitals even regions.

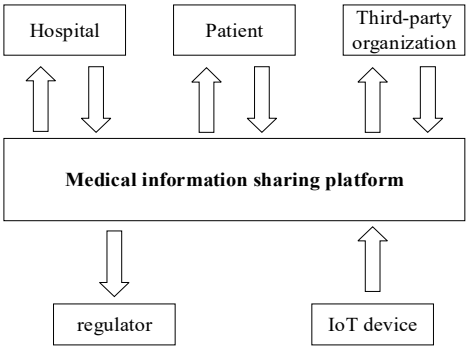

Fig. 3. Structure of platform

The core functions of the platform are as follows, and the main function process is shown in Figure 4:

1. User management. All patients can register in the platform with real name and identity ID. And the medical records correspond to patients, so that they can be easy to manage.

2. Medical records management. Patients can view their medical records on the platform, and doctors can only view the medical records of their hospital without the need to apply. Meanwhile, the history of doctors viewing medical records will be recorded in the blockchain through the addition layer so that the data can be more secure. When a doctor completes a new medical record on the platform, the key information will be recorded in blockchain.

3. Authorized management. Both patients and hospitals can authorize others to view their own medical records. It is divided into two cases.

Firstly, third-party institutions (such as medical analysis institutions, insurance institutions, etc.) apply for medical records. The steps are as follows:

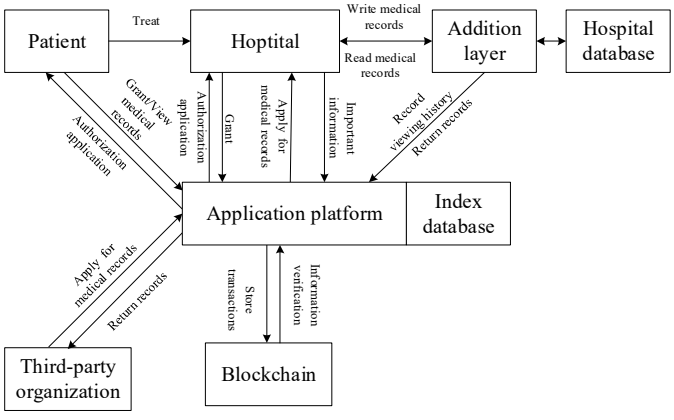

Fig. 4. Functions of platform

(1) Third parties search a type of disease through the platform, and the platform returns the brief information of the medical records that meet the requirements.

(2) Third parties apply for paying for viewing some medical records. In order to protect patients' privacy, the application notices will be sent to the hospital first.

(3) Hospitals verify and authorize the applications. With the approval of the hospital, the application notices will be sent to the patient.

(4) Patients verify and authorize the applications. With the approval of the Patient, the applications are approved.

(5) The chaincode will be triggered. The medical record is sent to the third parties and the cost is paid to the patient.

The process of application as well as authorization is fully recorded in the blockchain.

Secondly, the patient voluntarily authorizes third parties or hospitals to view the medical records. The patient can give the authorization code and the patient ID to a third-party institution or a hospital. With the authorization code, they can directly view the information of medical records. The platform ensures the authenticity of the medical records.

4. Online real-time settlement. The platform provides an interface to the medical insurance department. When a medical record is generated, the audit of medical insurance and reimbursement proportion will be completed automatically by the chaincodes that deployed on the blockchain. So patients can complete the cost settlement directly on the platform. The payment that the third-party institution has paid will also be directly deposited into the patient' account through the platform.

5. Health monitoring through the IoT. The user's IoT equipment with authentication can connect to the platform, and it can upload the recorded data. The platform can give the user early-warning about health by data analysis technology.

IV. Platform Design and Development

A. The Framework of the Platform

The framework that we proposed is a reliable medical information sharing platform based on blockchain, as shown in Figure 5. It can also be used for other information sharing scenarios, and this paper takes medical information as an example. Relevant regulatory authorities and high-grade hospitals are the nodes on the blockchain network, they have same status and connect with each other through a P2P network. And the ministry of health is CA (certificate authorization) node, it is responsible for authority management. Every node should be authenticated through digital certificate mechanism and then it is admitted to the blockchain.

chaincodes is designed for the whole business processes, it runs in the docker container for safety and efficiency. Chaincodes can be triggered once conditions are satisfied, e.g. the chaincode for online settlement will be executed automatically. And external application can also interact with blockchain by gRPC API, using POST/HTTP to execute chaincodes, which can add and query information in the block-

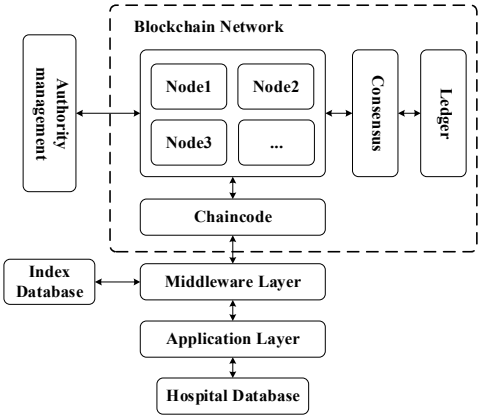

Fig. 5. Framework of platform

chain. According to the complexity of the business, each blockchain have different chaincodes and different numbers, and each node can execute several chaincodes.

Consensus is an important part of blockchain structure. It can decide how a block comes into being. The consensus has a significant influence on the security and efficiency of blockchain. All of the nodes will use the consensus algorithm to verify whether the transactions are legal or not. If a certain percent of nodes reach a consensus, the transactions will be added into blockchain. It is to say that every node will add the transactions into its ledger. PBFT (Practical Byzantine Fault Tolerance) can tolerate one third of nodes that are malicious[17], and it has higher efficiency than PoW which is used in Bitcoin[18]. Meanwhile, PoW consumes a large amount of power, which will waste much resources. As for private chain and alliance chain, PBFT is a better choice, so the consensus of our system is PBFT.

There is a middleware layer between blockchain and application layer which can do some frequent but tedious operations. It also serves as an interface layer, when a chaincode is deployed, we should do some serialization of the parameters between application layer and blockchain layer. In order to reduce the complexity of blockchain operations and application layer operations, middleware layer takes the work of data format conversion for the business layer. Meanwhile, middleware is connected to an index database which doesn't store complete medical records but only the index between hospital database and blockchain database. The middleware layer can provide privacy encryption service for the information in the blockchain. Instead of understanding the transaction content, all voting nodes only need to verify the encrypted information. This will ensure the safety of the medical records and improve efficiency when third parties select medical records or he system finds the selected records.

The application layer is designed for the main business functions. Users (like patients, hospital, etc.) and hospital database connect with this layer. All operations from users will be performed on this layer, and the layer will response correspondingly. The patient can send requests to view his own records, and hospitals will inform the platform that a new medical record has been generated. Third-party can search for medical records and apply for viewing through this layer.

Authorization code verification is also done on application layer.

B. System implementation

The medical information sharing platform is based on blockchain, and we implemented it to verify our ideas. The application layer is a web platform. We use Node.js+Express as the Back-end framework. The front page uses the CSS+ Html5 as static pages, and dynamic part is based on the bootstrap framework, the data exchange part uses jQuery, which will make the platform more compatible with both PC and phone access. The blockchain provides gRPC APIs for applications, as well as encapsulated SDKs for provisioning calls. The hospital database uses MySQL. Index database uses mongodb which is a database based on distributed file storage belonging to NoSQL.

Chaincodes are programmed by Golang. Each chaincode has a fixed structure, and it needs to implement the interface, as shown in Figure 6. The data that should be recorded are stored as key-value pairs, and some APIs are used to change the state of the ledger. We create several chaincodes, such as recording the application history, automatically settlement and so on. Hospital also use the chaincode to upload the key data to the blockchain after a medical record is generated. The steps of generating a new medical record are as follows:

(1) The hospital will generate a new electronic medical record and it will be stored in the hospital database. Meanwhile, an authorization code will be generated both for the hospital and the patient. The code is composed of Arabia numbers and letters, and it is modifiable.

(2) The application layer will generate hash value of the electronic medical record by using the hash algorithm or other digital summarization algorithms. The hash in blockchain can be used to compare with the hash of the information in the hospital database, which can tell whether the information has been changed.

(3) The key data such as the hash value, number of medical record, the owner and index stored in index database, will be sent to the blockchain by middleware. These data will be stored as a transaction in the blockchain by chaincodes. These transactions are stored using the structure of merkle tree, and the hash of the root will be stored in the block head.

```
// ====================================================================================
// This is an example of a chaincode.
// The structure and interface of a chaincode is shown.
// ====================================================================================

package main

//Import pakages
import (
    "errors"
    "fmt"
    "github.com/hyperledger/fabric/core/chaincode/shim"
    pb "github.com/hyperledger/fabric/proto/peer"
)

//Declare a structure
type SimpleChaincode struct {
}

// Implement the Interface:Init and  Invoke
func (t *SimpleChaincode) Init(stub shim.ChaincodeStubInterface) pb.Response {
    // Initialize the chaincode
    …
}
func (t *SimpleChaincode) Invoke(stub shim.ChaincodeStubInterface) pb.Response {
    // Logical process for main function or query
    …
}

// main function,call the method shim.Start()
func main() {
    err := shim.Start(new(SimpleChaincode))
    if err != nil {
        fmt.Printf("Error starting Simple chaincode: %s", err)
    }
}
```

Fig. 6. Chaincode example

(4) The middleware layer will create index and record it in the index database.

A blockchain explorer, which is the most straightforward way to view information of blockchain, is set up. Part of the Fabric explorer is shown in Figure 7. Everything that is recorded in block can be viewed from the blockchain explorer. On the explorer, we can see the number of nodes and blocks, block specific information, transaction specific information, etc.

The platform can be browsed on phones as well as on PC. Firstly, users can login the platform from the interface shown in the Figure 8(a). Different types of users will have different permissions. For Example, when a patient login, there are three main functions, as shown in Figure 8(b). The first tab is medical history, and he can view the medical history. The second tab is authorization, he can authorize the requests or not. The third tab is history of authorization. Analogous to a patient, the hospital can also perform several functions after logging in and view medical history that it generated. It can authorize the requests, and this operation will be recorded in blockchain. Since there are too many records in a hospital, the platform can also find medical records according to the conditions (such as doctor ID, patient ID, data, etc.), which can improve search efficiency. The interface that third-party agencies login in has four tabs, such as application for view, application history and so on.

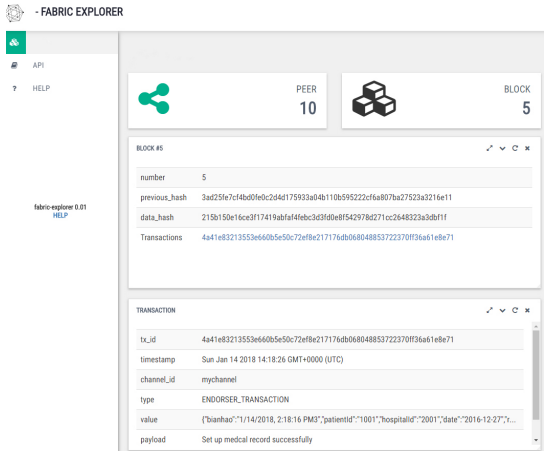

Fig. 7. blockchain explore

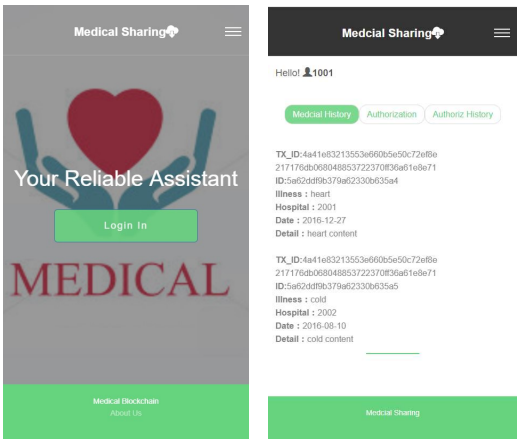

Fig. 8. platform interface(a) and (b)

V. EVALUATION

The platform is designed for solving the existing problems. Firstly, we will compare this platform with other solutions, as shown in Table I, and analyze its pros and cons. There are four solutions compared from six dimensions in Table I. The first one is a centralized EHRS over cloud, and MedRec and MDSM have been introduced in chapter I. It can be seen that our platform has some advantages. Compared with EHRS, our platform has the advantage of decentralization and tamper resistance. And there exists some differences between our platform and the other solutions. The hospital databases are still used and the platform record the actions of hospital viewing medical records, this way can minimize the effects on hospitals and reduce the difficulty of implementation. Moreover, the middleware layer which can reduce the pressure on the platform and blockchain is designed. But our platform also has some shortcomings, e.g. the data analysis module is not good enough.

Secondly, the functions as well as the solved problems of the platform are shown clearly in Table II. Our platform has a role in medical information sharing.

VI. SUMMRY

Since modern people pay more and more attention to health and privacy, a safe and reliable medical information sharing platform will be in great demand in market. In this paper, a novel medical information sharing platform is proposed based on blockchain technology. And it makes full use of blockchain. By combining blockchain technology with information systems, authorized users can jointly maintain the information in the blockchain network through consensus mechanism. The blockchain can prevent information from being tampered. All transactions can be traced, so it can locate the hidden dangers more accurately. It creates a shared ecology where information can be converted into value, so that everyone involved can benefit from it. It is a way to maximize the value of informational data. If the Internet can convey information, blockchain can convey value.

This paper explores business processes and technology framework for blockchain application. It is quoteworthy for the development of information sharing platform based on blockchain. However, the development of blockchain technology and its application still have many challenges, and more effort should be made on it.

TABLE I. COMPARISON OF CURRENT SOLUTIONS

	EHRS[19]	***MedRec[9]***	***MDSM[11]***	***Our platform***
decentralized	No	Yes	Yes	Yes
damper-resistant	No	Yes	Yes	Yes
privacy protection	Yes	Yes	Yes	Yes
consensus	None	PoW	DPoS	PBFT
the pressure of the main chain	None	greater	less	less
the difficulty of implementation	easiest	hard	hard	easier

TABLE II. FUNCTIONS OF THE PLATFORM

Users	***Functions***	***The solved problems***
patients	view their own medical records more freely;	no right to use his own medical records;
	decide which instition can view his;	privacy leaks;
	get rewards for providing medical data;	
	treat in different hospitals even regions	regional constraints;
hospitals	carry out treatment with fewer worries;	current medical records are not reliable
	Previous records can help to treat;	
third-party research institutions	have a more formal platform to get more comprehensive data;	No legal access to get medical data
Regulatory &audit departments	Most of the work can be finished automatically by smart contracts	High cost and low efficiency

REFERENCES

[1] M. A. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," 2017.

[2] A. Pazaitis, P. D. Filippi and V. Kostakis, "Blockchain and value systems in the sharing economy: The illustrative case of Backfeed," Technological Forecasting & Social Change, vol. 125, 2017.

[3] J. Zhang, N. Xue and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," IEEE Access, vol. 4, pp. 9239-9250, 2016.

[4] T. T. Kuo, H. E. Kim and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," J Am Med Inform Assoc, vol. 24, pp. 1211-1220, 2017.

[5] Y. Yuan and F. Y. Wang, "Blockchain: The State of the Art and Future Trends," Acta Automatica Sinica, vlo.42, pp.481-494, 2016.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2008.

[7] M. Swan, Blockchain: Blueprint for a New Economy: O'Reilly Media, Inc., 2015.

[8] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. L. Tan, "BLOCKBENCH: A Framework for Analyzing Private Blockchains," 2017.

[9] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in International Conference on Open and Big Data, 2016, pp. 25-30.

[10] Y.MEI, " Blockchain Method for Safely Storage of Medical Record," Journal of Jiangxi Normal University (Natural Science Edition), vol. 41, pp. 481-487, 2017.

[11] T. F. Xue, F. U. Qunchao, C. Wang, and X. Y. Wang, "A Medical Data Sharing Model via Blockchain," Acta Automatica Sinica, vlo.43, pp.1555-1562, 2017.

[12] Y. Xiao, H. Wang, D. Jin, M. Li, and J. Wei, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," Journal of Medical Systems, vol. 40, p. 218, 2016.

[13] M. A. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," Technology Innovation Management Review, vol.7, pp.22-34, 2017.

[14] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare,", 2017, pp. 1-4.

[15] A. M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen, "Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in Consumer Communications and NETWORKING Conference, 2015, pp. 826-834.

[16] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in IEEE International Conference on E-Health Networking, Applications and Services, 2016, pp. 1-3.

[17] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Symposium on Operating Systems Design and Implementation, 1999, pp. 173-186.

[18] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in IEEE International Congress on Big Data, 2017.

[19] A. Ibrahim, B. Mahmood and M. Singhal, "A secure framework for sharing Electronic Health Records over Clouds,", 2016, pp. 1-8.