Healthchain: Secure EMRs Management and Trading in Distributed Healthcare Service System

Chaoyang Li, *Student Member, IEEE*, Mianxiong Dong, *Member, IEEE*, Jian Li, Gang Xu, Xiubo Chen, and Kaoru Ota, *Member, IEEE*

***Abstract*—Electronic medical records (EMRs) are the most critical data in human health management. As in traditional centralized healthcare service systems (HSSs), user privacy security, EMRs data leakage, tampering, and island are some significant problems. However, blockchain is a promising technology to protect the privacy and realize cross-institutional data sharing for solving these problems. In this article, a novel peer-to-peer EMRs data management and trading system called healthchain has been proposed based on consortium blockchain technology. Through this distributed system, the patient can access their EMRs in different institutions freely, and the EMRs can be traded among different users conveniently. Then, to balance EMRs data supply and demand, we establish a Stackelberg pricing model to evaluate EMRs data providers and consumers' interactions. The optimal unit price and data amounts can be found by applying the backward induction method, and the maximizing benefits of the participants can be obtained by achieving the Nash equilibrium in the proposed game. Moreover, security analysis shows the healthchain can provide secure EMRs management and trading, and the simulation results show that the proposed pricing model can help the healthchain achieve social welfare maximization.**

***Index Terms*—Cross-institutional data sharing, electronic medical record (EMR), healthchain, social welfare maximization.**

Manuscript received July 15, 2020; revised September 11, 2020 and October 29, 2020; accepted November 12, 2020. Date of publication November 17, 2020; date of current version April 23, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 92046001 and Grant 61962009; in part by the Natural Science Foundation of Beijing Municipality under Grant 4182006; in part by the Fundamental Research Funds for the Central Universities under Grant 2019XD-A02; in part by JSPS KAKENHI under Grant JP19K20250, Grant JP20F20080, and Grant JP20H04174; in part by the Leading Initiative for Excellent Young Researchers, MEXT, Japan; in part by the Open Research Project of the State Key Laboratory of Media Convergence and Communication under Grant SKLMCC2020KF006; in part by the China Scholarship Council under Grant 201906470024; and in part by the BUPT Excellent Ph.D. Students Foundation under Grant CX2019227. *(Corresponding author: Mianxiong Dong.)*

Chaoyang Li is with the Information Security Center, State Key Laboratory of Networking and Switching Technology and the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China, and also with the Department of Sciences and Informatics, Muroran Institute of Technology, Muroran 050-8585, Japan.

Mianxiong Dong and Kaoru Ota are with the Department of Sciences and Informatics, Muroran Institution of Technology, Muroran 050-8585, Japan (e-mail: mx.dong@csse.muroran-it.ac.jp).

Jian Li is with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Gang Xu is with the School of Information Science and Technology, North China University of Technology, Beijing 100144, China.

Xiubo Chen is with the Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Digital Object Identifier 10.1109/JIOT.2020.3038721

I. Introduction

HEALTHCARE service system (HSS) acts as a more important role in collecting and analyzing human health condition based on the large quantity of electronic medical records (EMRs). Depending on the historical EMRs, the doctor can provide an accurate diagnosis, and the patient can obtain a comprehensive treatment. In general, EMRs are stored and managed in many independent HSSs, which controlled by different medical institutions [1]. In general, the medical institutions are unwilling to share their data concerning their benefits. As shown in Fig. 1, the left part shows the current healthcare system, where the patients have limited access permission of their EMRs, and the EMRs cannot be freely transmitted among different medical institutions. The right part shows the future healthcare system where the cross-institutional sharing of EMRs is more convenient, as the patients can freely access their EMRs when they go to the doctor in another medical institution. Therefore, it is a great challenge to design an open and shared HSS to improve the ability of diagnosis and the quality of healthcare [2].

EMRs are the essential historical records of diagnosis and treatment in human healthcare, and they usually contain the patient's condition, diagnosis procedure, medications, and operation situation [3]. This information can provide enormous bits of help for the patient's subsequent treatment and rehabilitation, and they also can promote the development of the medical treatment level and medical technology. However, the EMRs also contain sensitive private information about the patients, doctors, and medical institutions. There are existing many problems in traditional HSS, such as user privacy security, EMRs data leakage, tampering, and island [4]. The centralized storage and management form cannot secure them, even making them vulnerable to many threats. For example, they are easily tampered by the malicious man-made purpose or destroyed by the natural disaster. Even worse, once criminals have stolen sensitive information, it will significantly damage the patients and medical institutions. Besides, the different data formats make it difficult to share the EMRs between the independent medical institution, and the sealed data in different professional institutions have little contribution to the research on pathogeny relatedness of different diseases.

When a patient wants to transfer his EMRs from one medical institution to another, the limitation of information content

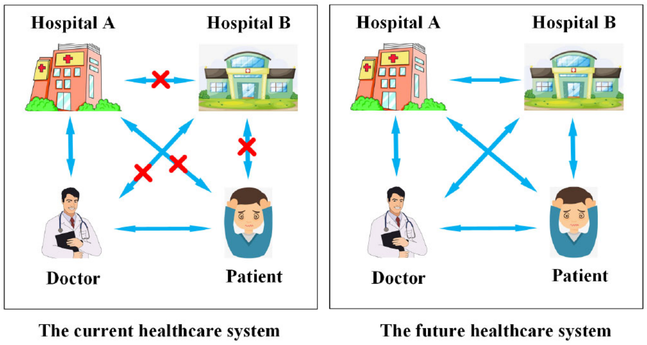


Fig. 1. Current and future healthcare system.

and recipient should be considered. As mentioned above, to protect the patient and medical institution's privacy, the EMRs owner should sign a consent that stipulates the type of EMRs data, the information of the recipient, the usage purpose, and the period that the data can be accessed legally. Therefore, it is tough to coordinate as the patient moves to another medical institution, which cannot be determined in advance. The city, region, and country where the medical institution is located are usually different from the original one.

In order to break though the limitation of data sharing in current healthcare system, it is urgent to seek a technology to promote cooperation and establish deep mutual trust between different medical institutions. Fortunately, an emerging technology called blockchain is a promising method to manage and share the EMRs among different HSSs securely and efficiently [5], [6]. Supporting by blockchain technology, the HSS will significantly benefit the healthcare industry. The distributed storage model can effectively weaken the malicious behaviors from centralized medical institution and avoid the EMRs data leakage by signal node storage failure. Then, transaction's the openness and verifiability can guarantee the authenticity and accuracy of the EMRs and prevent the manipulation and destruction of malicious third party. Moreover, the anonymous transaction address form can strictly protect the user privacy security without influencing the statistical property of the EMRs data. However, the delay of transaction confirmation in Bitcoin is low efficiency, which is not suitable for the abundant EMRs sharing in HSS. Consequently, it is severe to design a novel scheme for transaction confirmation to improve the efficiency of the current blockchain-enabled HSS.

This article first exploit a peer-to-peer EMRs sharing system called healthchain based on the consortium blockchain technology [7]. In this distributed system, the patients serve as the EMRs data creators who have the right to access their EMRs in different medical institutions. The medical institutions act as the authorized nodes to maintain the whole system. Meanwhile, they are responsible for collecting EMRs data resources and allocating them to satisfy the market demands. The data consumers, such as the researchers, medical companies, and other organizations, can utilize the aggregated EMRs data to research the medical drugs and technologies. Then, the index of EMRs and the sharing process will be recorded into the healthchain to be the immutable records, to establish a lightweight public ledger. Moreover, we propose a Stackelberg pricing game model between the EMRs data provider and consumer, then present a data pricing strategy to balance the EMRs data trading.

Following are three main contributions of this article.

1) *Unified Healthchain:* We propose a unified healthchain based on consortium blockchain to store and manage EMRs, providing distributed privacy preserving for users and EMRs data.
2) *Efficient EMRs Trading Model:* We establish an efficient resource trading model to realize EMRs cross-institutional sharing and present a Stackelberg pricing model to evaluate EMRs data providers and consumers' interactions.
3) *Effective Optimal Method:* We apply the backward induction method to solve the game model, which can help achieve market equilibrium and social welfare maximization. The simulation results also show this healthchain is secure, and the game model is efficient.

The remainder of this article is organized as follows. Some related works have been given in Section II. The framework of healthchain has been presented in Section III. Section IV presents the EMRs resource trading model in healthchain. Section V gives the performance evaluation and analysis of the proposed model. Finally, conclusion is given in Section VI.

II. Relate Works

We first present some introductions about the HSS in this section. Next, some descriptions of blockchain technology have been given. With the development of blockchain technology, some research about the blockchain-enabled HSS in recent years has been presented.

A. Healthcare Service System

HSS is the platform for collecting and managing the EMRs. Generally, the HSS is centralized, containing the public-key generator (PKG), third-party auditor (TPA), and the cloud storage server. The PKG generates the private key for the system users. The TPA is responsible for auditing the healthcare data. With the explosive increase of the EMRs data, some new methods based on the Internet-of-Things (IoT) technology have been proposed to improve the system's robustness and security. Fabian *et al.* [8] have given a novel architecture based on multiclouds, which can realize collaborative and secure EMRs sharing in semitrusted cloud computing environments. Yang *et al.* [9] proposed an IoT-based HSS for healthcare big data storage and presented a novel twofold self-adaptive access control system for EMRs sharing. However, these IoT-based HSSs are centralized, which cannot satisfy the increasing demand for security and efficiency.

As in these centralized systems, the medical institutions control the whole system, which may easily cause data deleting, tampering, and other problems, once the PKG or TPA becomes malicious. EMRs contain sensitive information about the patients and medical institutions, such as name, ID number, telephone number, address, etc. Therefore, the centralized cloud storage structure cannot provide full protection for EMRs. The inevitable software bugs, hardware faults, and human errors in the systems can easily lead to data corruption and loss. Moreover, the integrity of the EMRs also is easily destroyed by the inevitable software/hardware failures and human errors in the cloud. Besides, different medical institutions are loathing to share their data with privacy concerns and competitive pressure [10]. While the consistency and interoperability of the different data types from different medical institutions are also significant problems for data sharing [11].

B. Blockchain Technology

Blockchain technology is widely used for building a distributed consistent system in recent years, which was first proposed to develop the cryptocurrency called Bitcoin by Nakamoto in 2008 [12]. Unfamiliar users can trade with each other through this system, and the trading records are saved into blockchain ledger as the immutable records. In order to achieve distributed consistency among unfamiliar users, there exist some consensus algorithms, such as the Proof of Work (PoW) [13], Proof of Stake (PoS) [14], and Delegated PoS (DPoS) [15]. Meanwhile, the signature algorithms [16], [17] are also needed to authenticate user legitimacy and protect the privacy security of the user and transaction. Blockchain is usually considered as a public, decentration, distribute, and reliable hyperledger with high Byzantine fault tolerance [18], and used in finance, cloud computing, IoT systems, and other applications.

In general, the blockchain technology can be divided into three categories: 1) public blockchain; 2) private blockchain; and 3) consortium blockchain [7]. The public blockchain is public with no access restrictions, and anyone can create transactions with other users through the Internet. Bitcoin [12] and Ethereum [19] are the most successful application cases based on the public blockchain technology. In contrast, the private blockchain is closed, which is generally used for keeping accounts and controlled by the individual or private entity. The consortium blockchain is relatively closed with limited access permissions, which is more suitable for the same type of company and organization to build a union ledger. However, different from the public and private blockchain, it requires preselecting some mining nodes to build new block and maintain the whole system. It has many advantages, such as better control, fast trading, and data confidentiality. As long as most mining nodes have confirmed, the new transaction can be recorded, and even the historical record can be modified. Besides, consortium blockchain equipped with PoS or DPoS consistency algorithm is also more energy efficient compared with the PoW-enabled Bitcoin system based on the public blockchain. Ripple [20] is based on consortium blockchain, which is proposed for cross-border payment service among different financial institutions. Therefore, we apply the consortium blockchain technology to construct a distributed platform between different medical institutions to achieve secure and efficient EMRs sharing.

C. Blockchain-Enabled Healthcare Service System

The HSS performs the storage and management of EMRs, improving the medical efficiency and medicine level. However, centralized organizations easily bring about the data leakage problem because of human error and hardware damage. Moreover, the medical institutions are unwilling to share their EMRs relating privacy concerns and competitive pressure. Therefore, cross-institutional sharing of EMRs is a big challenge for current centralized HSS. Some blockchain-based strategies in the last few years for HSS have been reviewed in [21] and [22]. With the emergence of blockchain technology, it is predictable to achieve that the patients can freely access their EMRs in different institutions.

In recent years, some simple frameworks of blockchain-enabled HSS have been proposed [5], [6], [23]–[25], [27], [28]. Peterson *et al.* [5] presented a proof of structural and semantic interoperability algorithm to construct a blockchain-enabled model for EMRs sharing. However, this consistency algorithm is not practical for massive transaction processing in HSS. Dubovitskaya *et al.* [23] proposed an EMRs sharing scheme with the permission blockchain, which aims to improve the consistency and interoperability of EMRs data types from different medical institutions. Dagher *et al.* [29] presented a blockchain-enabled framework for secure and efficient access to EMRs by different users, while this scheme cannot support fast trading based on the Ethereum. Xu *et al.* [25] proposed a privacy-preserving scheme for large-scale health data, but they do not focus on how to share and evaluate the EMRs transmitting processes. Yazdinejad *et al.* [26] utilized blockchain technology to establish a hospital network, which can help patients accept decentralized authentication in different medical institutions. These literature works give a significant exploration for data sharing among different HSSs, and the blockchain technology has served as a distributed ledger to record the EMRs. However, most of these blockchain-enabled HSSs have stayed in the form of conception and framework. There is little research about implementing healthchain with current HSS and the efficient transmission mechanism between the patient, medical institution, and researcher. Moreover, privacy preserving of the user and the data security of EMRs are also significant issues that should be considered.

III. Unified Healthchain for EMRs Sharing

In this section, we give a detailed description of the healthchain. In this system, the patient creates and uploads his EMRs, and he also can verify whether his EMRs are recorded or not. Meanwhile, some different medical institutions serve as the mining nodes to maintain the whole system. They are responsible for collecting and verifying the EMRs, generating and recording them into the public ledger. The transparent and immutable data storage structures can make EMRs data more safe and convincing.

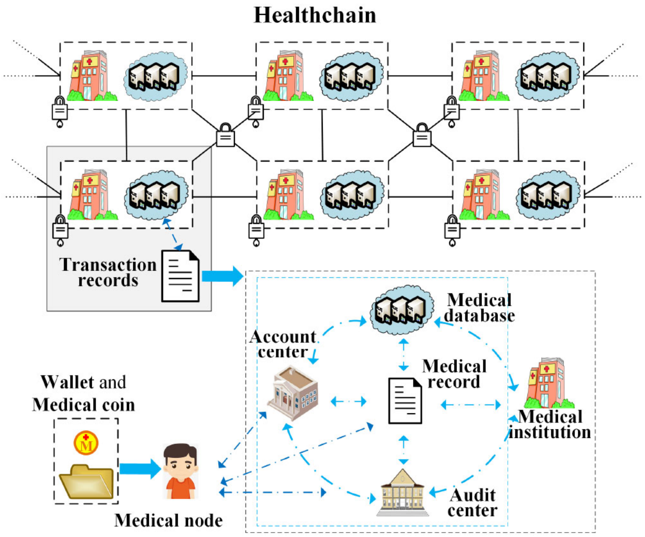


Fig. 2. Framework of healthchain.

TABLE I
MAIN TERMS IN HEALTHCHAIN

Items	Explanation
Medical records	The data of electronic medical records in the health-care blockchain.
Medical nodes	The entities that participate in the system of healthchain, such as the patient, doctor, researcher, auditor and medical institution.
Medical institution	The entity that composes and maintains the network of Healthchain, which is generally serving as the 'mining' nodes.
Medical coin	The token charging for the process of EMRs sharing between different medical nodes.
Account center	The entities that record wallets, wallet addresses and medical coin accounts.
Audit center	The entities that audit the transaction and the medical institution.
Wallets	The place to store the medical coins.
Transaction records	The data of EMRs transaction, store operation, verify operation, audit operation and so on.
Medical database	The entities that store the real EMRs data.

First, we present the framework of healthchain in Section III-A. Then, we describe the unified healthchain for EMRs sharing in Section III-B.

A. Framework of Healthchain

Different from traditional centralized HSSs, all the entities are serving as the nodes to constitute the whole system in the proposed healthchain. As shown in Fig. 2, the medical institutions' union and some other necessary institutions together compose the distributed EMRs sharing network. Meanwhile, one public blockchain ledger has been maintained by medical nodes, and real EMRs are stored in the database that has been managed by each medical institution. The general user should first register as a legal user, then create and share his EMR to the healthchain. In order to promote the execution of the EMRs sharing process, we introduce the medical coin for charging the process to balance the EMRs data supply and demand.

Then, some main items in healthchain have been listed in Table I. Moreover, three important parts: 1) medical records; 2) medical nodes; and 3) medical coin, which compose the main framework of healthchain, are described as the following.

1) *Medical Records:* EMRs are the records of the patient's whole therapeutic process at the medical institution. First, the patient sees a doctor and initializes a medical record. Next, the doctor makes a diagnosis based on the patient's condition. Then, the patient receives treatment according to the therapeutic schedule. More importantly, the index of EMRs will be recorded in the healthchain, but the real EMRs data are stored in the medical database managed by each medical institution. In this way, it can establish a lightweight public ledger among the medical union. If the patient goes to another medical institution, he can authorize the new doctor to access his EMRs, which can be downloaded from the index recorded in the medical database. Moreover, healthchain can help integrate the diversified EMRs data, which can help the disease diagnosis and contribute to the development of medical research, drug discovery, and medical device manufacturing. In addition, as EMRs are the patients' property, they will obtain some medical coins for rewards if they agree to share the EMRs to the healthchain.
2) *Medical Node:* This healthchain contains many users who serve as medical nodes with different functions. All the medical nodes should register as the legal users who can take part in the healthchain. The patients serve as the general nodes in healthchain who create the EMRs and share them with the system. The doctors serve as a participant for the EMRs creating who have rights to view the EMRs authorized by the patient, and they also can access other EMRs by obtaining the users' authorization. As the former described that the medical institutions act as the system mining nodes, they play essential roles to verify and record the EMRs. The medical institutions are responsible for sharing the collected EMRs into the whole healthchain, and they are also rewarded with the medical coins. The medical institution acts as the intermediary that has responsibility to guarantee the security of users' privacy and EMRs data, serve as the merchant to earn the income from data consumer, and pay the reward for the data creator. Meanwhile, the audit center, insurance center, and bank are essential for guaranteeing the EMRs to guarantee their legality. These entities also serve as the system nodes to participate in the management of EMRs in healthchain. Audit, insurance reimbursement, and fund settlement operations are also recorded in the public blockchain ledger. Moreover, the researcher and other organizations which want to use the EMRs data for research need to register as the legal nodes.
3) *Medical Coin:* When the EMRs are sharing between the different nodes, the remuneration is needed. In order to distinguish the general medical fee, we introduce a token called medical coin for the data exchange of EMRs. The MERs creators will be rewarded with some medical

coins to share their data, and the consumers of EMRs data need to pay some medical coins. This medical coin has been used to evaluate the EMRs sharing behaviors and balance the EMRs resource supply and demand relationship in the proposed healthchain. Moreover, these medical coins will be stored in the wallet, and they can be used to deduct part of the total medical fee with proper transformational relation. It can motivate the interagency of sharing the EMRs and guarantee the rights and interests of the original EMRs creator.

It is worth noting that one piece of EMR contains the patient's condition and the doctor's diagnose. So they should hide and protect the sensitive information of each other when uploading their EMRs data. Meanwhile, the wallet is an essential part of medical nodes to perform the EMRs sharing process. Just as that in Bitcoin system, the user will generate many wallets addresses for different transactions. It can store the property of medical nodes and protect their privacy security against the statistical attack. Moreover, the account center and audit center are also needed to manage medical nodes accounts and audit the trade authenticity in the healthchain, respectively. Besides, the medical institution has its medical database to store the real EMRs data and public ledger of the healthchain.

B. Secure EMRs Sharing in Healthchain

Supporting by the consortium blockchain technology, we exploit healthchain for EMRs sharing among different medical institutions. However, different from Bitcoin that all the nodes compete for constructing new blocks with high costs, the proposed healthchain selects some medical institutions as the mining nodes to realize system consistency with moderate costs. While these preselected mining nodes collect and share their local EMRs to maintain the whole system. Moreover, the behaviors for sharing and using EMRs data will be evaluated by the medical coins, which can make a strict balance and stability for system implementation.

Then, the details about the critical operations of the healthchain have been presented as follows.

1) System Initialization: In the healthchain, all nodes should be registered as legal users before their operations on EMRs data. As this healthchain system contacts the bank system, insurance system, and other government organizations, the users must register with their real identity ID_i from the account center. They will then get their public keys PK_i, private keys SK_i, and certificates Cert_i, which are used for identity authentication and transaction signature. Then, the medical nodes can derive a set of wallet addresses $W_{ID_{i,k}}$ based on the public and private keys, and the mapping list $\{\mathrm{ID}_i, \mathrm{PK}_i, \mathrm{SK}_i, \mathrm{Cert}_i, \mathrm{W}_{\mathrm{ID}_{i,k}}\}$ will be stored in the account center. Here, it also needs to generate enough wallet addresses for each transaction record like Bitcoin, preventing statistical attacks for deducing users' private keys and patients' condition.

2) EMRs Transmitting Among Different Nodes: In the healthchain, the EMRs data can be transmitted conveniently. As shown in Fig. 3, the EMRs data can conveniently transmit among different medical institutions. As the patient, he has full rights of his EMR, and he can obtain diagnosis and treatment in different medical institutions by authorizing different doctors to view his historical EMRs. Like the doctor, he can provide more professional and accurate treatments with integrated and periodic EMRs data. Meanwhile, the researcher can improve medical technology and medical level and provide disease prediction and prevention. Besides, the full line shows that the patient and doctor can freely access their EMRs data, while the dotted line shows that other actions that want to use EMRs data for research will have some limitations and rewards. All the sharing and transmitting behaviors will be recorded into a series of transactions and uploaded into the healthchain.

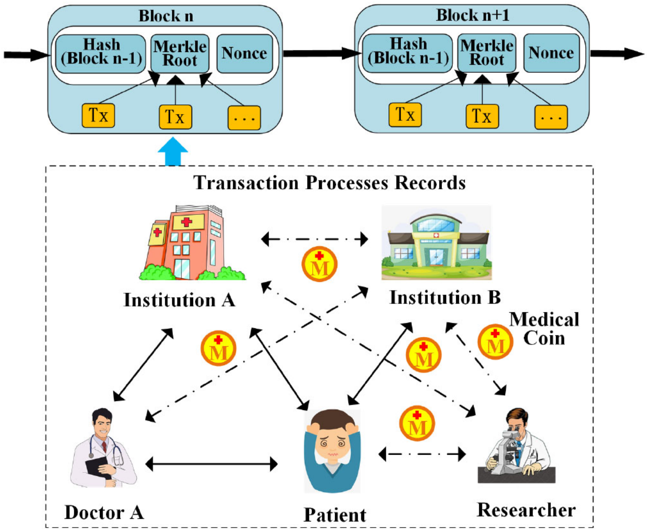


Fig. 3. Secure EMRs sharing in healthchain.

3) Payments Using Medical Coins: With the MERs data transferring in the network of healthchain, the medical coin acts as an important role to reward the sharing behavior and charge the employing behavior. As the patient and the doctor serve as the creator for the EMRs data, they will be rewarded with some medical coins for their sharing behaviors. Here, the rewards can be evaluated by the prospective value of EMRs data, and the corresponding medical coins will be sent to their wallets. On the other hand, someone who wants to use the EMRs data will be charged. As the researcher wants to take EMRs for scientific research, the medicine company wants to utilize them for drug development, and other organizations also want to employ them with lawful purposes. These cross-institutional sharing behaviors should be paid to protect the benefits of the EMRs creator. Therefore, the medical coin can protect the benefits of medical nodes and maintain the balance and stability of the healthchain system.

4) Building Blocks in Healthchain: During a certain period, the transaction records of EMRs sharing and employing are verified and collected into a temporary block by the mining medical institutions. The medical node who obtains the right to establish this block will perform the consistency

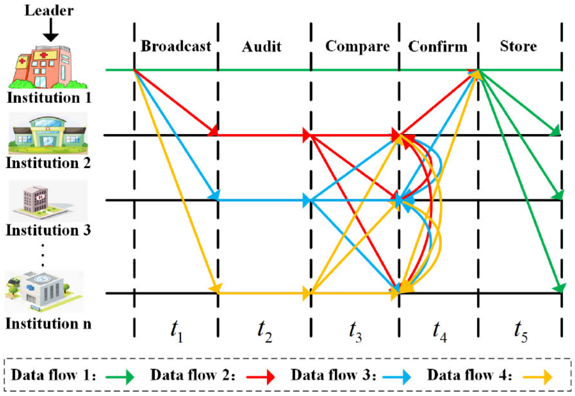


Fig. 4. Block data confirming processes.

validation process. After passing the validation, this block will be attached to the formal healthchain. Then, this medical institution will be rewarded with some medical coins. Here, when the creator of this block has been confirmed, all the medical institutions will try to compete for the rights of building the next new block. As the healthchain is a relatively closed network, we adopt the PoS to determine the leader for this period. Different from the resource-consuming consensus algorithm called PoW in Bitcoin, PoS is more efficient and resource saving for EMRs sharing among different HSSs.

5) Implementing Consistency Validation Process: In this healthchain, we apply DPoS as the consistency algorithm, which has short block time and high-efficiency properties. When one medical institution obtains the rights for building a new block, it will implement the consistency validation process among the whole healthchain network. As shown in Fig. 4, the verification processes for different medical institutions are shown in different colors. The leader first broadcasts block data and its DPoS certificate to other authorized medical institutions for audit and verification. Next, the medical nodes verify the received block data and broadcast the results with their signatures to each other for mutual verification. Then, they compare the received results with their results and feedback the final results to the leader. In the end, the leader checks the signed audit results, comparison results, and the received records of these results. If there are some different opinions on the block data, the leader should check and analyze another audit problem. When the block data pass the audit and verification, the leader will attach these block data with his signature on the main chain of healthchain and broadcast them to the whole network, as shown with the green line in Fig. 4. Until now, the transaction has been done, and it will become an immutable record stored in the blockchain ledger. After that, this leader can obtain some medical coins as rewards for building a new block, and then continue to work for the next block.

IV. EMRs Resource Trading in Healthchain

The healthchain can provide a distributed platform for EMRs sharing among different medical institutions and users. However, how to balance data supply and demand over some time, and optimize the benefits of the data creator and consumer. In this section, we present a secure EMRs resource trading model for cross-institutional data sharing. A pricing strategic game has been proposed, which can help the trading participants obtain the optimal data pricing and amount. Meanwhile, the social welfare maximization and market equilibrium can be obtained by achieving the Nash equilibrium in the proposed game. The following are detailed description of the pricing strategic game.

A. Entities in the Pricing Strategic Game

In this article, we take an economic strategy game called Stackelberg game to model this relationship between EMRs data providers and consumers [30]. Because the signal EMR cannot develop conspicuous value, we take the medical institutions as the EMRs data providers to perform data trading with the data consumers. As in the proposed healthchain system, the EMRs data provider serves as the "leader" that performs decision first, while the data consumers act as the "followers" who perform decision afterward.

First, we take one medical institution as the leader. The leader first sets the unit data price strategy $\{\lambda = [\lambda_i]_{i\in\mathcal{N}} : \lambda_{\min} \leq \lambda_i \leq \lambda_{\max}\}$, where λ_i is the price for ith ($i \in \{1, 2, \ldots, \mathcal{N}\}$) data consumer, and $\lambda_{\min}(\lambda_{\max})$ is the minimum(maximum) price. Here, the minimum price $\lambda_{\min}$ is the lowest benefits guarantee for every real EMRs creators. Therefore, by deducting the additional costs γ that contain the operating and maintenance costs, the expected rewards of this medical institution can be expressed as

$$R_{\mathcal{L}} = \lambda_i d_i - \gamma d_i \tag{1}$$

where d_i is the data resource demand of the ith data consumer.

The followers are the data consumer, such as the researcher, medical company, and other organizations who want to use the MERs data for research. They decide their demand amounts following the actions of leader. There are usually $\mathcal{N}$ data consumers who will compete with each other to purchase the medical data resource. By deducting the additional costs c_i that contain the operating and maintenance costs, the satisfaction function of the ith data consumer is described as follows:

$$S_{\text{sat}} = \alpha_i ln(d_i - d_{\min} + c_i) \tag{2}$$

where $d_{\min}$ is the minimum demand amounts of the ith consumer, and α_i is the predefined nonzero positive factor.

As the costs of each data that the ith consumer paid for EMRs are $\lambda_i d_i$. Therefore, the utility function of this data consumer can be expressed as

$$R_{\mathcal{F}} = S_{\text{sat}} - \lambda_i d_i. \tag{3}$$

According to the above pricing strategy, the EMRs data provider and consumers will perform a sequential decision-making process until reaching the final data price and amounts. The data provider first sets his price, and the data consumers then set their demand amounts depending on the pricing strategy. Next, the data provider tries to maximize his utilities while the data consumers want to minimize their costs. Therefore, the optimization problems of the data provider and consumers can be formulated into two problems A and B, respectively, which are shown as follows:

$$\begin{aligned} A:&\quad \max_{\lambda_i} \sum_{i\in\mathcal{N}} R_{\mathcal{L}}(\lambda_i|d_i) \\ &\quad \text{s.t. } \lambda_{\min} \le \lambda_i \le \lambda_{\max}, \lambda_{\min} \ge \gamma \ \forall i \in \mathcal{N} \end{aligned} \tag{4}$$

$$\begin{aligned} B:&\quad \max_{d_i} R_{\mathcal{F}}(d_i|\lambda_i) \\ &\quad \text{s.t. } \alpha_i \ge 0,\ d_i \ge d_{\min} > 0 \ \forall i \in \mathcal{N}. \end{aligned} \tag{5}$$

Furthermore, assume there are $t \in \{1, 2, \ldots, \mathcal{T}\}$ medical institutions that act as the EMRs data collectors and traders in the healthchain network. Meanwhile, by serving as the system maintainer, they want to make market equilibrium for the whole system and try to maximize the social welfare. The medical institutions allocate the EMRs data to the data consumers, and pay for the original data creators' rewards. Then, the social welfare maximization problem of the healthchain can be formulated as the following optimization problem C:

$$C: \quad \max_{\lambda_i, d_i} \left\{ \sum_{t\in\mathcal{T}} R_{\mathcal{L}} + \sum_{i\in\mathcal{N}} R_{\mathcal{F}} \right\}$$
$$\text{s.t.} \begin{cases} \lambda_{\min} \le \lambda_i \le \lambda_{\max}, \ \forall i \in \mathcal{N} \\ d_i \ge d_{\min}, \ \forall i \in \mathcal{N} \\ \alpha_i \ge 0, \ \forall i \in \mathcal{N} \\ c > 0. \end{cases} \tag{6}$$

In addition, we mainly consider the balance between EMRs data supply and demand in a period that may come from many medical institutions. The proposed pricing strategic game is executing dynamically with the time. The data supply and demand in the last period have decided the unit data price in the current period. Whatever some medical institutions participate in or leave from the system influence the unit data price in the current period. Therefore, it can always achieve the data balance in the proposed system. Then, the EMRs data are the reusable resources so that the data supply will be increased with the newly shared EMRs data. It will not influence the unit data price until it extends the time limit or has no practical value. Moreover, in the proposed healthchain, the EMRs data have only a server address for storage and inalterable transaction record for sharing. It can also efficiently prevent the double sharing operations from some malicious user. Hence, the shared EMRs data cannot be shared for another time.

B. Optimal Price Analysis

As the formerly described problems A and B, the maximize rewards of the leader and followers can be achieved when the proposed Stackelberg game reaches Nash equilibrium [31]. The EMRs data provider and consumers will be motivated by this principle to achieve their respective optimal rewards. Therefore, the Nash equilibrium between problems A and B can be described as the following definition.

Definition 1: The point (λ^*, d^*) is the Nash equilibrium point if the following condition satisfied, where λ^* represents the optimal unit price of resource data, and d^* represents the data demand of the consumer

$$\begin{cases} \partial R_{\mathcal{L}}(\lambda^*, d^*) \ge \partial R_{\mathcal{L}}(\lambda_i, d^*) \\ \partial R_{\mathcal{F}}(\lambda^*, d^*) \ge \partial R_{\mathcal{F}}(\lambda^*, d_i). \end{cases} \tag{7}$$

Here, we apply the backward induction method to solve the above Nash equilibrium problem [32]. First, we compute the optimal data demand amounts of the ith data consumer. Concerning resource demand d_i, the one- and second-order derivatives of its utility function $R_{\mathcal{F}}$ are shown as follows:

$$\frac{\partial R_{\mathcal{F}}}{\partial d_i} = \frac{\alpha_i}{d_i - d_{\min} + c_i} - \lambda_i \tag{8}$$

$$\frac{\partial^2 R_{\mathcal{F}}}{\partial d_i^2} = -\frac{\alpha_i}{(d_i - d_{\min} + c_i)^2} < 0. \tag{9}$$

Therefore, we can derive that $R_{\mathcal{F}}$ is a strictly concave function from (9). Meanwhile, the optimal data demand d^* can be generated by solving $\partial R_{\mathcal{F}}/\partial d_i = 0$

$$d_i^* = \frac{\alpha_i}{\lambda_i} + d_{\min} - c_i. \tag{10}$$

Second, we compute the optimal unit price of the data resource. We substitute (10) to (1), and the reward function $R_{\mathcal{L}}$ of data provider has been transformed as follows:

$$R_{\mathcal{L}} = (d_{\min} - c_i)\lambda_i - \frac{\gamma\alpha_i}{\lambda_i} - \gamma(d_{\min} - c_i) + \alpha_i. \tag{11}$$

Then, we differentiate the reward function $R_{\mathcal{L}}$ with respect to λ_i, and the one- and second-order derivatives of (11) are shown as follows:

$$\frac{\partial R_{\mathcal{L}}}{\partial \lambda_i} = \frac{\gamma\alpha_i}{\lambda_i^2} + d_{\min} - c_i \tag{12}$$

$$\frac{\partial^2 R_{\mathcal{L}}}{\partial \lambda_i^2} = -\frac{2\gamma\alpha_i}{\lambda_i^3} < 0. \tag{13}$$

When $d_{\min} < c_i$, we have $\lim_{\lambda_i \to 0} R_{\mathcal{L}} = -\infty$ and $\lim_{\lambda_i \to +\infty} R_{\mathcal{L}} = -\infty$. Meanwhile, we can derive

$$\begin{cases} \dfrac{\partial R_{\mathcal{L}}}{\partial \lambda_i} > 0, \ if \ 0 < \lambda_i < \sqrt{\dfrac{\gamma\alpha_i}{c_i - d_{\min}}} \\ \dfrac{\partial R_{\mathcal{L}}}{\partial \lambda_i} < 0, \ if \ \lambda_i > \sqrt{\dfrac{\gamma\alpha_i}{c_i - d_{\min}}}. \end{cases} \tag{14}$$

Therefore, the trend of the reward function $R_{\mathcal{L}}$ increases first and then decreases. So it is strictly concave, and the optimal unit price of the data resource can be achieved when $\partial R_{\mathcal{L}}/\partial \lambda_i = 0$

$$\lambda^* = \sqrt{\frac{\gamma\alpha_i}{c_i - d_{\min}}}. \tag{15}$$

When $d_{\min} > c_i$, $\lambda_i < 0$. However, this situation is not practical.

In the proposed Stackelberg game, the medical institution serves as the data distributor to communicate with every data consumer, and the Nash equilibrium point between the data providers and consumers can be obtained by performing Algorithm 1.

Theorem 1: The healthchain can maximize social welfare when the Nash equilibrium has been realized in the proposed

Algorithm 1 Optimal EMRs Data Pricing Algorithm

```
Initialize: $R^*_{\mathcal{L}} = 0, R^*_{\mathcal{F}} = 0, \lambda^*_i = 0, d^*_i = 0$
for Each data consumer $i \in \mathcal{N}$ do
    for The unit price $\lambda_i$ from $\lambda_{\max}$ to $\lambda_{\min}$ do
        if $d_{\min} < c_i$ then
            $\lambda^*_i = 0, d^*_i = 0$
            Break
        end if
        The data consumer $i$ adjusts its demand amounts $d_i$ depending on $d_i = \alpha_i/\lambda_i + d_{\min} - c_i$.
        The data consumer $i$ adjusts its utilities depending on $R_{\mathcal{F}} = \alpha_i ln(d_i - d_{\min} + c_i) - \lambda_i d_i$.
        The data provider adjusts its rewards depending on $R_{\mathcal{L}} = \lambda_i d_i - \gamma_i d_i$.
        if $R_{\mathcal{L}} \geq R^*_{\mathcal{L}}$ then
            The data provider records the optimal unit price and reward $R^*_{\mathcal{L}} = R_{\mathcal{L}}, R^*_{\mathcal{F}} = R_{\mathcal{F}}, \lambda^*_i = \lambda_i, d^*_i = d_i$.
        end if
        if $R_{\mathcal{L}} \leq R^*_{\mathcal{L}}$ then
            Break
        end if
    end for
end for
The Stackelberg game achieves Nash equilibrium $(\lambda^*_i, d^*_i)$.
```

Stackelberg game between the EMRs data provider and consumers.

Proof: The social welfare maximization problem of the healthchain can be equivalent to two optimal problems: 1) problem A of the expected rewards for the medical institutions and 2) problem B of the utilities for the data consumers. From (9), the utility $R_{\mathcal{F}}$ of data consumer is strictly concave with relating to demand amount d_i. Meanwhile, from (13), the expected reward $R_{\mathcal{L}}$ of the medical institution is also strictly concave with relate to unit data price λ_i. Therefore, the medical institution can find an optimal unit price λ^*_i for the data resource, while the data consumers also choose their unique data amounts d^*_i. Here, (λ^*_i, d^*_i) is the Nash equilibrium point for the proposed Stackelberg game in the healthchain. Therefore, the medical institution and data consumers can obtain optimal benefits when the Nash equilibrium point has been achieved. Moreover, healthchain can realize social welfare maximization. ■

V. Security Analysis and Simulations

Now, we give the security analysis of the proposed healthchain and perform the EMRs data sharing scheme.

A. Security Analysis of the Healthchain

Compared with traditional centralized HSS, this healthchain changes the centralized pattern into the distributed pattern, and helps the patients freely access their own EMRs in different medical institutions. Then, compared with the Bitcoin system, the transaction processes can be more efficient with the consensus algorithm of PoS. Moreover, the consortium blockchain helps construct an openness and shared EMRs exchanging platform and improves the data security and protects the users' privacy security.

TABLE II
Simulation Parameters

Parameter	Value
Unit data price λ_{min}	[10,1000]
Factor α_i	(10000,11000]
Minimum data demand d_{min}	[200,2000]
Factor c_i	(100,1000]
Factor γ_i	10

1) *Privacy Preserving:* The user's registration and data trading precesses are securely stored as the transaction in the healthchain. As the transaction structured with the counterparty's addresses, the adversary cannot obtain any user's privacy. Moreover, the user creates a new address for the next transaction to prevent the statistical attacks.
2) *Decentration Advantage:* The distributed storage form provides strong robustness against the single node failure and centralized authoritarian control. Moreover, it can improve data security and promote the data cross-institutional sharing process.
3) *Data Nontampering:* Once the data have been recorded in healthchain, they will become the immutable records. Then, no one can tamper them with the immeasurable computation burden and resource consumption.
4) *No Double Spending:* The medical coin is signed with the owner's private digital signature, and a chronological history use of medical coin is publicly recorded in the healthchain. Therefore, there impossibly exists the double spending.
5) *Energy Saving:* The medical institutions compose an alliance based on the consortium blockchain technology, and they apply the PoS to achieve system consensus, which can effectively save the computing resource compared with the PoW-based Bitcoin system.
6) *Rights Protection:* This healthchain can help the patients take control over their EMRs. They can access them wherever they go to see doctors, and the rewards of EMRs sharing also can ease the burden for treatment and medicine fees.

B. Numerical Results

Before the performance of the EMRs data sharing scheme, some necessary parameters are shown in Table II. To describe different pricing strategies, we introduce $N = 10$ data consumers with one data provider into this simulation.

First, we analyze the performance of the healthchain. In the PoW-enabled Bitcoin system, one new block needs 10 min to be built, and only seven transactions can be processed in 1 s. In the PoS-enabled Ethereum system, the transaction processing peaked at 15 transactions per second. However, it cannot satisfy the demand for massive transactions. In the proposed healthchain, some medical institutions have been elected as the mining nodes by the PoS consistency algorithm. PoS can

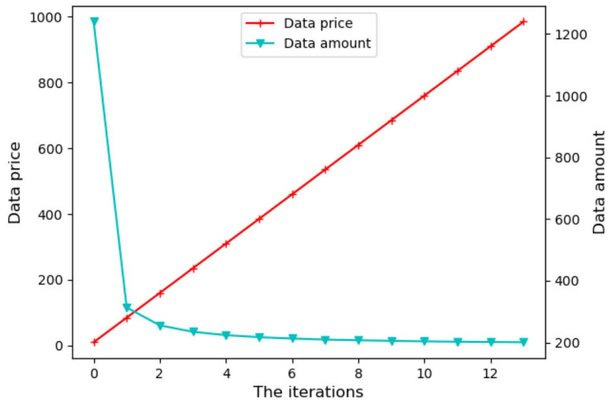


Fig. 5. Variation trend of the data price and amount.

support the fast and massive trading for the EMRs transmitting among different medical institutions and users.

Then, we evaluate the proposed optimal pricing algorithm. The variation trends of the EMRs data price and demand amounts for one data consumer are shown in Fig. 5. The EMRs data amount of the ith consumer will be decreased with the increase of the data price. When the unit data price increases from the minimum price of $\lambda_i^{min} = 10$ to the maximum price of $\lambda_i^{max} = 1000$, the data consumer adjusts its demand amount to achieve the optimal utility. On the contrary, if the unit data price depreciates, they will increase the data amount. Both the data provider and consumers want to obtain optimal benefits, and the data price and demand amount influence the Nash equilibrium point. The optimal data price and demand amount are close to the maximum data price and minimum demand amount, respectively. Therefore, the Nash equilibrium point is close to the maximum data price and minimum demand amount.

In the following, the benefits of the data provider and consumer are changing according to the variation trend of the data price and amount, which are shown in Fig. 6. However, the data provider's expected rewards and the data consumer's optimal benefits are also constrained to the maximum data price and minimum demand amount, respectively. Therefore, along with the increasing of data price, the data consumer's optimal utility will tend to be stable. As the EMRs data is the reusable resource, the data provider's reward will increase with the usage counter. Here, we consider the transaction reward for one kind of EMRs data. The data provider's reward will tend to maximum by reaching the maximum data price unless there are new users who attended to buy this kind of EMRs data. Moreover, the total amount represents the social welfare in the healthchain. When the data provider and consumer have obtained their optimal benefits, the healthchain can achieve social welfare maximization.

In addition, the value of α_i has an influence on the optimal utility of consumers, and the variation trend of optimal utility for different data consumers with different α_i's value has shown in Fig. 7. As the data consumer's utility function is decided by the transaction amount d_i, α_i is also the variable factor that can significantly influence the final utility.

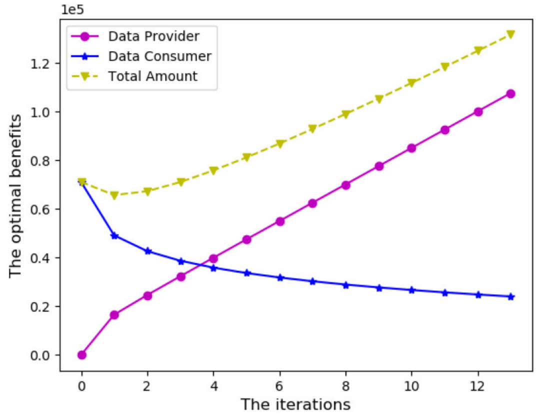


Fig. 6. Optimal benefits and social welfare.

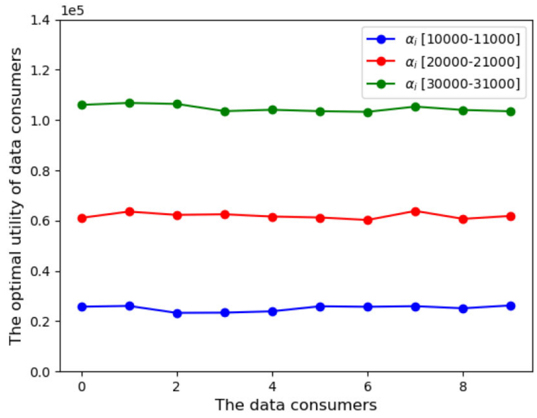


Fig. 7. Optimal utility of data consumers with different α_i.

Generally, the real value of α_i is influenced by the data amount, demand amount, and consumer amount. Hence, it should be preset according to the real scenario.

VI. Conclusion

In this article, a unified healthchain system has been proposed for EMRs sharing among various medical institutions. We take consortium blockchain technology to establish a more secure and energy-saving platform. Then, we introduce a token called medical coin in healthchain to sufficiently perform the EMRs data sharing trades. In the data sharing scenario, we construct a Stackelberg game between the medical institution and consumers, which helps them achieve the optimal unit resource price and data amount. Meanwhile, they can obtain each optimal benefit, and the healthchain also can achieve social welfare maximization. Moreover, we analyze the system security and perform the simulation for the EMRs data sharing scheme. Security analysis shows that the medical coin can well help to perform the EMRs data trading, and the proposed healthchain can well protect the EMRs data and patient's privacy.

Besides, this healthchain can make full use of the MERs, which can create more benefits for patients to maximize social welfare and provide the unalterable evidence for medical conflicts. However, in future works, we will discuss how to establish a practical real-time EMRs data exchanging system and perform our proposed pricing strategic model, how the medical coin acts as the value exchange weights, and how to allocate and optimize the EMRs data sharing process for the situation with many medical institution participants. With the increase of the health detection devices, some burning questions should still be considered, such as privacy preserving among edge network, fine-grained access control during EMRs sharing process, and system security against quantum attacks.

REFERENCES

[1] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, pp. 754–764, Jun. 2010.

[2] J. Vest and L. Gamm, "Health information exchange: Persistent challenges and new strategies," *J. Amer. Med. Informat. Assoc.*, vol. 17, no. 3, pp. 288–294, 2010.

[3] R. Hillestad *et al.*, "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs*, vol. 24, no. 5, pp. 1103–1117, 2005.

[4] K. Hossein, M. Esmaeili, T. Dargahi, and A. Khonsari, "Blockchain-based privacy-preserving healthcare architecture," in *Proc. IEEE Can. Conf. Elect. Comput. Engi. (CCECE)*, Edmonton, AB, Canada, 2019, pp. 1–4.

[5] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.

[6] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Serv. (Healthcom)*, 2016, pp. 1–3.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

[8] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[9] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019.

[10] Y. Ge, D. Ahn, B. Unde, H. Gage, and J. Carr, "Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations," *J. Amer. Med. Informat. Assoc.*, vol. 20, no. 1, pp. 157–163, 2013.

[11] W. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, Jan. 2018.

[12] S. Nakamoto. (2008). *Bitcoin: A Peer-To-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[13] A. Gervais, G. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 3–16.

[14] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *Self-Published Paper*, vol. 19, pp. 1–6, Aug. 2012.

[15] D. Larimer, "Delegated proof-of-stake," Bitshare, Murska Sobota, Slovenia, White Paper, 2014.

[16] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, 2001.

[17] C. Li, Y. Tian, X. Chen, and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Inf. Sci.*, vol. 546, pp. 253–264, Aug. 2020.

[18] C. Miguel and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. Symp. Oper. Syst. Design Implement.*, vol. 99, 1999, pp. 173–186. [Online]. Available: https://www.usenix.org/legacy /events/osdi99/full_papers/castro/castro_html/castro.html

[19] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project, Zug, Switzerland, Yellow Paper, 2014.

[20] F. Armknecht, G. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *Proc. Int. Conf. Trust Trustworthy Comput.*, 2015, pp. 163–180.

[21] E. Aguiar, B. Faical, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surveys*, vol. 53, no. 2, pp. 1–27, 2020.

[22] P. Zhang and M. Boulos, "Blockchain solutions for healthcare," in *Precision Medicine for Investigators, Practitioners and Providers*. San Diego, CA, USA: Academic Press, 2020, pp. 519–524.

[23] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *Proc. AMIA Annu. Symp.*, vol. 2017, Apr. 2018, pp. 650–659. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/citedby/

[24] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Vienna, Austria, Aug. 2016, pp. 25–30.

[25] J. Xu *et al.*, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[26] A. Yazdinejad, G. Srivastava, R. Parizi, A. Dehghantanha, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020.

[27] N. Witchey, "Healthcare transaction validation via blockchain proof-of-work, systems and methods," U.S. Patent US20 150 332 283 A1, 2019.

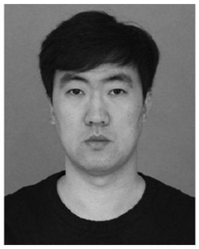
[28] L. Chen, W. Lee, C. Chang, K. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Futer Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.

[29] G. Dagher, J. Mohler, M. Milojkovic, and P. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[30] W. Huang, W. Chen, and H. Poor, "Request delay-based pricing for proactive caching: A Stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 18, no. 16, pp. 2903–2918, Jun. 2019.

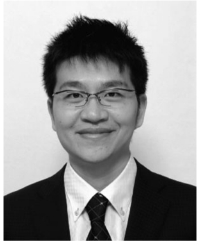
[31] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 192–202, Jan. 2008.

[32] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A Stackelberg game approach," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar. 2013.



Chaoyang Li (Student Member, IEEE) received the M.S. degree from Zhengzhou University of Light Industry, Zhengzhou, China, in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications, Beijing, China.

He is a visiting student with the ENeS Lab, Muroran Institution of Technology, Muroran, Japan, supported by the China Scholarship Council Program from October 2019 to September 2020. His research interests include information security, cryptography, and blockchain.



Mianxiong Dong (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan, in 2006, 2008, and 2013, respectively.

He is the youngest ever Vice President and a Professor with Muroran Institute of Technology, Muroran, Japan. He was a JSPS Research Fellow with the School of Computer Science and Engineering, University of Aizu and was a Visiting Scholar with the BBCR Group, University of Waterloo, Waterloo, ON, Canada, supported by the JSPS Excellent Young Researcher Overseas Visit Program from April 2010 to August 2011. He was selected as a Foreigner Research Fellow (a total of three recipients all over Japan) with NEC C&C Foundation, Tokyo, Japan, in 2011.

Dr. Dong is a recipient of the IEEE TCSC Early Career Award 2016, the IEEE SCSTC Outstanding Young Researcher Award in 2017, the 12th IEEE ComSoc Asia–Pacific Young Researcher Award in 2017, the Funai Research Award 2018, and the NISTEP Researcher 2018 (one of only 11 people in Japan) in recognition of significant contributions in science and technology. He is Clarivate Analytics Highly Cited Researcher (Web of Science) in 2019.

Jian Li received the Ph.D. degree from Beijing Institute of Technology, Beijing, China, in 2005.

He is currently a Professor with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing. His current research interests include information security and quantum cryptography.

Gang Xu received the Ph.D. degree in software engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2019.

Since 2015, he has been a visiting Ph.D. student with the Department of Computer Science, University of Calgary, Calgary, AB, Canada. He is currently a Lecturer with the School of Information Science and Technology, North China University of Technology, Beijing. His current research interests include quantum cryptography, quantum network coding, and blockchain.

Xiubo Chen received the Ph.D. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2009.

She is currently an Associate Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications. Her research interests include cryptography, information security, quantum network coding, and quantum private communication.

Kaoru Ota (Member, IEEE) was born in Aizu-Wakamatsu, Japan. She received the B.S. and Ph.D. degrees in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan, in 2006 and 2012, respectively, and the M.S. degree in computer science from Oklahoma State University, Stillwater, OK, USA, in 2008.

She is currently an Associate Professor and the Ministry of Education, Culture, Sports, Science and Technology Excellent Young Researcher with the Department of Sciences and Informatics, Muroran Institute of Technology, Muroran, Japan. From March 2010 to March 2011, she was a Visiting Scholar with the University of Waterloo, Waterloo, ON, Canada. She was a Japan Society of the Promotion of Science Research Fellow with Tohoku University, Sendai, Japan, from April 2012 to April 2013.

Dr. Ota is a recipient of the IEEE TCSC Early Career Award 2017, the 13th IEEE ComSoc Asia–Pacific Young Researcher Award 2018, and the 2020 N2Women: Rising Stars in Computer Networking and Communications. She is Clarivate Analytics Highly Cited Researcher (Web of Science) in 2019.