Postprint: Construction of a Medical Blockchain Model for Healthcare Big Data Security Protection

Authors: Li Hongchen, Ma Jie, Hu Mo

Date: 2023-04-01T00:00:00+00:00

Abstract

[Purpose/Significance] In the context of rapid medical informatization development, information security protection for medical big data encounters challenges including data loss and sharing difficulties. To enhance the protection of health and medical big data, this study constructs a medical blockchain model oriented toward health and medical big data security protection, which addresses issues such as centralized storage, lack of traceability, and vulnerability to attacks, thereby providing a solution for further advancing the application of blockchain technology in the health and medical domain. [Methods/Process] The study develops an information security protection model and system architecture for health and medical big data based on blockchain technology, employs the PBFT consensus algorithm to ensure the immutability of medical blockchain data, utilizes asymmetric encryption technology to guarantee the security of personal medical information, and implements incentive mechanisms to encourage participation of various nodes in the medical blockchain. [Results/Conclusion] Compared with traditional medical information protection methods, the medical blockchain model oriented toward health and medical big data security protection offers advantages including data traceability, tamper resistance, equitable information sharing, security, and trustworthiness, thereby better facilitating the development of health and medical datafication.

Full Text

Construction of a Medical Blockchain Model for Healthcare Big Data Security Protection

Li Hongchen[1], **Ma Jie**[1,2], **Hu Mo**[1] [1]School of Management, Jilin University, Changchun 130022 [2]Resource Research Center, Jilin University, Changchun 130022

Abstract:
[**Purpose/Significance**] In the rapid development of medical informatization, traditional healthcare information security protection faces problems such as data loss and difficulty in sharing. To better protect health and medical big data, this paper constructs a medical blockchain model oriented toward healthcare big data security protection to solve problems of centralized storage, nontraceability, and vulnerability to attacks, providing solutions for further promoting blockchain technology applications in the healthcare field.
[**Method/Process**] This study constructs a healthcare big data information security protection model and system architecture based on blockchain technology. The PBFT consensus algorithm ensures the immutability of medical blockchain data, asymmetric encryption technology guarantees the security of personal medical information, and an incentive mechanism encourages various nodes to join the medical blockchain.
[**Result/Conclusion**] Compared with traditional medical information protection methods, the medical blockchain model for healthcare big data security protection offers advantages such as data traceability, tamper resistance, equal information sharing, and security credibility, which can better promote the development of healthcare digitalization.

Keywords: Healthcare Big Data; Blockchain Decentralization; Information Security Protection; PBFT Algorithm
Classification Number: G203
DOI: 10.13266/j.issn.0252-3116.2021.02.004

The rapid development of healthcare digitalization and informatization has provided convenience for people' s medical care, but simultaneously, the storage, utilization, and security of massive healthcare data have increasingly attracted attention. In recent years, the healthcare industry has experienced several "devastating" data loss and leakage incidents. For example, hackers breached the information system of Anthem, the second-largest health insurance provider in the United States, leaking information of over 78 million customers. The American health insurance company Premera Blue Cross also suffered a cyber attack, resulting in the leakage of 11 million customers' information [1]. Experts from Greenbone Networks in Germany discovered that over 600 unprotected servers were exposed on the internet, with the leaked content containing a large number of medical radiation images. Among these, China had 14 unprotected PACS server systems, leaking 279,000 data records [2]. Current vulnerabilities in healthcare information systems provide opportunities for hackers, with frequent incidents of cyber theft, data loss, and hacking, placing healthcare big data in constant information security crises.

Data security is not unique to the healthcare field, but healthcare big data is highly sensitive and private, containing citizens' most confidential physical and disease information, as well as personal life trajectories, residences, medical insurance, and property information. Once personal health information is leaked, the consequences are extremely severe. On October 24, 2019, the

Political Bureau of the CPC Central Committee conducted its first collective study on blockchain technology, where the "four requirements" proposed in the study pointed out the direction for how blockchain technology can bring substantive changes to social development [3]. The first requirement is to explore blockchain technology application scenarios in people' s livelihood fields and actively promote the integration of blockchain technology with healthcare. The data storage and block generation methods in blockchain technology give stored data characteristics of immutability, traceability, transaction privacy protection, and timeliness, which naturally endow blockchain with strong financial and transaction attributes. The information security and anti-leakage services provided by blockchain technology enable better integration with the financial field. Although healthcare differs from finance, in the healthcare field with complex information exchange, massive information volume, and numerous participants, information needs to be exchanged, added, and read multiple times in the system. This information transfer is similar to transactions in the financial field, and blockchain provides a new solution for healthcare big data information security issues.

1 Literature Review

Healthcare big data refers to all information related to natural persons' health status, disease prevention and treatment, and medical behavior that has privacy attributes [4]. This includes not only personally identifiable private information such as date of birth, name, contact information, and ID number, but also patients'physical characteristics, disease conditions, health status, drug allergies, and family medical history recorded during medical processes.

1.1 Healthcare Big Data Information Security Protection Research

Current management systems and data protection technologies for medical institution big data fail to meet the needs of healthcare big data information security protection, with problems such as data vulnerability to loss [5], leakage [6-7], and difficulty in sharing [8]. Domestic and international research on healthcare big data information security protection mainly focuses on access control technology, data encryption technology, and rule engine technology. Sun Baili et al. proposed using encryption algorithms and keys to encrypt data for storage, achieving the goal of protecting sensitive information at the data source level [9]. I. Blanquer et al. utilized ontologies for automatic authorization on medical imaging platforms to strengthen the protection and storage efficiency of medical information [10]. Liu Yimin et al. studied fine-grained access control models in relational databases, analyzed problems existing in hospital data application scenarios, and explored specific solutions [11]. Jia Ruilong et al. proposed a new fine-grained access structure G-CP-ABE with significant computational gains, improving medical data confidentiality and data access privacy to a certain extent [12].

With the advent of the healthcare big data era, the diversity of medical data

formats and rapid data growth pose new challenges to information security protection. Current information security protection solutions rely on a completely trusted, independent third party to ensure interaction reliability. Once a single third-party trust institution is attacked, all protected information becomes unsafe. Technical measures alone cannot fundamentally solve current information leakage and loss phenomena, and medical information protection requires a new, decentralized approach. Therefore, this paper proposes a blockchain-based healthcare big data information security protection strategy.

1.2 Healthcare Big Data Medical Blockchain Research

Domestic research on blockchain-based healthcare big data information security protection is still in its infancy. Wang Hui et al. constructed a decentralized medical data storage system, improved PBFT consensus algorithm, and data interaction system architecture, achieving medical data security, traceability, and tamper resistance [13]. Foreign research is relatively mature. E. Andy pointed out that blockchain technology can help users reliably collect and preserve data resources related to research activities, enhancing the repeatability of big data resources and data development processes by creating uncorrupted data trails that securely record release decisions [14]. S. Patel et al. used blockchain as a distributed data storage ledger through a cross-domain image sharing framework, allowing radiology research and patients to define different data access permissions [15]. C. Esposito et al. studied using blockchain technology to protect medical data stored in the cloud, solving problems arising from conventional encryption languages and access control [16]. H. Li proposed a novel blockchain-based medical data preservation system (DataPreservation System) that guarantees data originality and verifiability, meaning even if data is stolen, user-related information cannot be obtained [17]. M. Waal et al. proposed using blockchain technology to promote data resource sharing among different nodes and break barriers hindering continuous sharing for data information related to the current COVID-19 pandemic, thereby advancing data resource research and application progress [18].

Current blockchain-based research on healthcare big data information security protection mostly focuses only on the data storage system level, without incorporating patients, hospitals, and other related institutions such as township health centers, health records, insurance companies, public security, and scientific research institutions into the model scope. This paper constructs a medical blockchain model for healthcare big data security protection from an institutional perspective.

2 Healthcare Big Data and Blockchain Technology Characteristics

2.1 Healthcare Big Data Types and Characteristics

Healthcare big data generally refers to all data related to life and health [16]. In terms of data sources, it mainly originates from patients, hospitals, physical examination institutions, and third-party diagnosis and treatment, with broader sources compared to other industries. From the perspective of data coverage, it encompasses all relevant data generated throughout the entire life cycle from birth, vaccination, school and work physical examinations, hospital visits and hospitalization, exercise, sleep, until death. Healthcare big data has characteristics of massive volume and privacy. From the data transmission process, healthcare big data is transmitted among patients, medical insurance and commercial insurance institutions, health supervision departments, hospitals, pharmaceutical companies, and laboratories, with each organization being independent. Therefore, data transmission involves more independent nodes than in finance, manufacturing, and other fields.

2.2 Medical Blockchain Technology Characteristics

Medical blockchain is a distributed medical information database that can record data in chronological order and ensure data immutability. Its data structure consists of data blocks arranged in chronological order, with each block containing users' healthcare information for a period of time, timestamped and linked to the previous block. To address trust issues in healthcare big data sources and transactions, nodes in the medical blockchain system [19] do not need to understand other nodes' background information or rely on third-party guarantees, thereby ensuring credible recording, transmission, and storage of medical data transmission activities [20]. Distributed ledgers require medical information transaction bookkeeping to be jointly recorded by different nodes in different locations, with each participating node storing a complete medical ledger, thereby ensuring the legality of medical information transactions.

Compared with traditional medical information storage, the uniqueness of medical blockchain' s distributed ledger is mainly reflected in three aspects: (1) **Distributed Accounting**: Every node in the blockchain stores complete medical data according to the chain structure, allowing all nodes to participate in recording and verification. The protocol mechanism enables each node to verify the correctness of other nodes' medical information records while participating in recording. Only when more than half of the nodes in the system simultaneously consider a record correct will its authenticity be recognized by the medical blockchain system, and the medical data record will be allowed to be written into the medical block. (2) **Distributed Storage**: Storage in each node of the medical blockchain is independent and equal in status. The consensus mechanism ensures consistency among node storages, preventing any single node from independently recording the ledger and avoiding data loss caused by a single

bookkeeper being controlled or some nodes being attacked. When the number of nodes on the medical blockchain is sufficiently large, theoretically, unless more than half of the nodes are destroyed, the healthcare ledger will not be lost, thereby improving ledger data security. (3) **Distributed Propagation**: Every new information transaction in the medical blockchain adopts a distributed structure and propagates according to the open-source P2P network layer protocol. Medical information is directly sent from one node to all other nodes in the system through distributed propagation. These three characteristics ensure that no individual or organization can control this medical system, and the medical blockchain database can be jointly constructed once most participants reach consensus.

Blockchain consensus mechanisms can effectively solve the problem of numerous and relatively independent healthcare big data transmission nodes. The consensus mechanism' s function is to enable all participating nodes in the medical blockchain to reach agreement on how to update and maintain the ledger, requiring every participating node to copy the current latest complete medical database. Alterations to the medical database by a single node or even multiple nodes cannot change copies held by other nodes. Only by controlling more than 51% of participating nodes in the entire medical blockchain system to simultaneously modify the same content can the medical databases saved by remaining nodes be modified, which is almost impossible when the number of nodes is huge. Each medical information block transmitted in the medical blockchain is linked to adjacent blocks through cryptography, making it possible to trace back to the time and location of any information transmission, thereby ensuring at the data level that each user' s medical data entered cannot be altered by individuals or institutions.

3 Medical Blockchain Model for Healthcare Big Data Security Protection

Healthcare big data information security protection consists of three parties: medical information generators and users, medical information exchange intermediaries, and information exchange supervisors. Consequently, the constituent elements of the medical blockchain model for healthcare big data security protection include a regulatory center, information aggregation agencies, and information exchange entities, as shown in Figure 1 [Figure 1: see original paper].

3.1 Medical Blockchain Model Components

In the information security protection model, entities participating in information exchange include patients, hospitals, and other related institutions such as township health centers, health records, insurance companies, public security, and scientific research institutions. Information exchange entities can, according to their own wishes and actual needs, choose to grant access and usage permissions to hospitals and other related institutions. After diagnosis and treatment,

patients sign their personal healthcare data with their private key to confirm data accuracy and privacy. Each medical data entry contains the data owner' s public key (PatientPK), medical metadata, and data digest [21].

As shown in Figure 2 [Figure 2: see original paper], patient healthcare data includes a medical metadata block and a data digest block. The data digest block includes timestamp (Timestamp), doctor public key (DoctorPk), medical data description (DataDescription), and medical data type (DataType). The medical metadata block includes doctor public key, file path (PathToFile), and hash value. To generate a valid medical block, the assembled candidate medical block must undergo hash operation to calculate a suitable random number. Each medical block has a difficulty coefficient, through which a target value can be calculated. The medical block header contains a random string. Each medical information save requires hash calculation of the header. If the hash result is smaller than the target value, the block is authenticated as valid and can proceed with subsequent block broadcasting operations. If the hash result is not smaller than the target value, the block is considered invalid, the random string is modified, and the hash value is recalculated.

Hospitals upload patient-generated data to the blockchain and distributed database through the medical blockchain, ensuring data immutability. Insurance companies, scientific research institutions, etc., can retrieve patients' healthcare data through public keys with patient authorization, providing data support for insurance claims and research activities.

Information aggregation agencies serve as information exchange intermediaries, storing complete blockchain data of information exchanges and providing communication services for hospitals, patients, and other related institutions. Each information transmission must send a transmission request to the nearest information aggregation agency, which verifies the request and broadcasts the operation to all information aggregation agencies.

The regulatory center serves as the supervisory department for medical information transmission, authorizing information aggregation agencies and information exchange entities while supervising transmitted medical data. The healthcare big data information security protection model based on blockchain technology uses blockchain to achieve a user-centered, highly confidential medical data protection system that existing medical management systems cannot accomplish, promoting medical big data sharing among different medical institutions and data platforms while protecting users' medical data from leakage.

3.2 Medical Blockchain Layers and Their Relationships

The medical blockchain for healthcare big data security protection consists of six layers: healthcare data layer, medical chain network layer, medical consensus layer, user participation incentive layer, medical system contract layer, and medical chain application layer [22], as shown in Figure 3 [Figure 3: see original paper].

3.2.1 Healthcare Data Layer The healthcare data layer is the most fundamental data structure in the entire medical blockchain system. As healthcare data transactions continue to occur, the information volume generated among nodes in the medical data transaction chain will inevitably increase, and the flow among nodes will accelerate. According to healthcare system characteristics, information presented by each node on the medical blockchain is data blocks. Under transaction data, each node' s state data mainly records various states of medical information during transaction processes, which medical information managers can view at any time. Transaction data from each completed information transaction generates corresponding hash values through hash algorithms within a fixed period [23]. If transaction information volume is small and time intervals are short, all information transaction hash values can be retained and linked to the Merkle root in the medical block header. If the healthcare chain has huge information transaction volumes, the originally recorded hash values need further calculation through repeated iteration until the final generation hash value is linked to the Merkle root after meeting medical block storage requirements. The medical block header records current version, previous block address, timestamp, Merkle root, and transaction medical information quantity information. Linking the previous block address and current block' s data hash value connects various medical blocks to form a complete main chain traceable from the latest block to the latest healthcare data block. Figure 4 [Figure 4: see original paper] shows the medical information transaction block establishment process.

3.2.2 Medical Chain Network Layer The medical chain network layer consists of nodes including hospitals at all levels, township health centers, health records, insurance companies, health supervision departments, and scientific research institutions. Since current healthcare big data is generally stored in tertiary hospitals and high-level medical research institutions, tertiary hospitals and high-level research institution nodes are set as consensus nodes responsible for medical block assembly, generation, and broadcasting. Other hospital nodes do not participate in medical blockchain bookkeeping, only needing to synchronize the entire ledger and upload patient-signed healthcare data to superior hospitals. Since chain verification and new block recognition are guaranteed by information transmission mechanisms and protocols, the blockchain is essentially an equal-opportunity P2P network where all nodes have equal opportunities and shared responsibilities.

3.2.3 Medical Consensus Layer The medical consensus layer is the core technology of medical blockchain. Its main function is to enable highly dispersed nodes to efficiently reach consensus on block data validity in the decentralized medical blockchain network, effectively solving trust issues among nodes. This model adopts the PBFT consensus algorithm, which improves data accuracy while minimizing dependence on computing power, better adapting to healthcare big data characteristics of large volume and strong immediacy.

3.2.4 User Participation Incentive Layer When medical information publishing entities and other information receiving institutions encounter inconsistent interests, users' enthusiasm for participating in medical blockchain will greatly decrease [24]. This paper encourages user participation in medical blockchain through a credit point model [25]. When users share medical information on the medical blockchain, they receive corresponding benefits; when medical information users obtain medical information, they pay corresponding costs, ensuring equal benefit distribution in the medical blockchain model for healthcare big data security protection. To achieve equal benefit distribution, initial points are provided to nodes participating in medical information sharing blockchain establishment. Nodes receive point rewards for providing valid medical information and point penalties for providing false medical information.

The credit point model constructed in this paper enables users to conduct fair accounting of costs and benefits whether they store and publish personal healthcare information as information providers or use information as information users, ensuring equal benefit distribution among medical blockchain nodes. Nodes are scored based on their performance in medical information storage and sharing processes. Credit points can be used to obtain membership services and exchange for cash, enabling each node to obtain what they need during information sharing. This promotes healthcare data protection and mining while meeting individual rational needs. Additionally, a reasonable and convenient exit mechanism can be established on the medical blockchain based on the credit point system, allowing various nodes to exit at any time according to their wishes, eliminating users' concerns.

3.2.5 Medical System Contract Layer The medical system contract layer consists of various scripts, codes, algorithms, and smart contracts. Smart contracts require participants in medical data collection, storage, and utilization to sign and attach to medical blockchain or tokens in code form, thereby achieving blockchain ledger recording functions. Smart contracts encapsulate various conditions that trigger contracts. The system automatically judges whether contract conditions are met and immediately executes once certain conditions are reached without third-party confirmation, ensuring contract execution is not interfered with by any external factors from the source. Therefore, the contract layer is the technical foundation of blockchain' s trustless nature. For example, when hospitals and patients reach a medical information transaction smart contract, the contract is embedded in the medical blockchain in code form. The system automatically judges whether uploaded data meets contract conditions, and if so, the contract takes immediate effect.

3.2.6 Medical Chain Application Layer The medical chain application layer defines the application scope of medical blockchain, mainly responsible for medical information storage, query, and verification. All transaction information in the healthcare big data privacy information protection blockchain carries timestamps and information verification records. The application layer avoids

data loss by preserving transaction information and related information. Since transaction information itself, along with its timestamp and verification records, are retained, construction acceptance, hospital inspections, scientific research institution reviews, or government inspections can quickly locate information positions and prove information existence at any time.

4 Operation of the Medical Blockchain Model for Healthcare Big Data Security Protection

Information aggregation agencies consist of clients, information transaction servers, and service provision nodes. The client is responsible for sending medical information, usage requests, receiving information, and evaluating information. Compared with blockchain in finance, industry, and other fields, medical blockchain has numerous participating nodes that are independent of each other with huge differences in data volume requirements among different nodes. Therefore, according to different users' purposes and required data volumes for healthcare big data, the medical blockchain client is designed as three types to enhance model application feasibility: (1) **User-level Client**: This type is web-based. Patients apply for data record upload after diagnosis through the user client and can authorize queries to obtain their historical records during subsequent visits. The main purpose is to provide patients with simple self-query services. (2) **Doctor-level Client**: This type does not store patient healthcare data but only provides query interfaces for medical institutions and authorizes patient data operations. (3) **Hospital-level Client**: This type needs to store healthcare big data and provide external services for medical insurance and commercial insurance institutions, health supervision departments, pharmaceutical companies, and scientific research institutions.

The information transaction server is mainly responsible for receiving medical information, usage requests, and evaluation information from clients, providing verification services between clients and service provision nodes. Service provision nodes store verified blockchain information and send demand information blocks. The detailed medical information transaction process is shown in Figure 5 [Figure 5: see original paper].

(1) Information Production Process. Before new user registration, the regulatory center, as a third-party certificate authority, receives relevant information submitted by each new user. The regulatory center generates private key PatientSK and public key PatientPK using asymmetric encryption algorithms based on user-submitted information such as name, age, and ID number. Digital signature sign is formed by encrypting the user' s public key PatientPK with the generated private key PatientSK. After completing registration, new users become legitimate nodes of the blockchain. The legality of their digital signature sign can be verified by other users through the regulatory center' s public key PK. When new users participate in information transmission, they need to upload their accounts to information aggregation agencies and download the latest transmission data to synchronize block header data, greatly reducing

users' burden of receiving and storing data without requiring them to store all blockchain data already stored in information aggregation agencies.

(2) Information Transmission Process. Patients send personal medical information to local information aggregators in the form of smart contracts, encrypting transmitted medical files. The information transaction service center executes the PBFT consensus algorithm. The master node in the blockchain packages medical information received within a period and sends it to slave nodes for verification. Slave nodes verify the asymmetric encryption public key extracted from medical information. If verification passes, the information is recorded in the medical blockchain; if verification errors occur, indicating medical information has been tampered with, the personal medical information is returned and not recorded in the medical blockchain, while verification error results are returned to the user.

(3) Information Verification Process. After account selection, the information transaction service center packages request information and broadcasts it to all local information aggregators. The information transaction service center selects transaction accounts. After successful matching of information transaction parties, the information demander receives the contract submitted by the information provider from the local information aggregator and generates a new contract. The information provider verifies the transaction record, digitally signs it, and uploads it to the information aggregation agency for verification. After passing verification, users search for keywords on the medical blockchain, using searchable encryption algorithms to generate trapdoors. Users generate query bills and send search requests to consensus nodes on the blockchain database. After receiving the query request, blockchain database consensus nodes extract trapdoors from the query request and use retrievable encryption algorithms to match and retrieve results needed by users. After receiving returned results, users use keys to decrypt encrypted data and view plaintext medical information.

This paper specifically studies the blockchain technology used in the medical blockchain model for healthcare big data security protection, the model' s constituent elements and hierarchical relationships, and the model' s operational processes. By constructing the medical blockchain model, this study enhances data sharing and cooperation among medical institutions and between medical institutions and other related institutions, improves medical data accuracy and utilization, increases the possibility of effective patient treatment, and reduces the operational costs of the healthcare system and patients' diagnosis and treatment costs. However, due to the current immaturity of blockchain technology and incomplete underlying infrastructure, decentralized storage and computing of massive healthcare big data requires significant time, while medical scenarios have extremely high requirements for data timeliness. How to improve the efficiency of medical blockchain requires continued research.

References

[1] America' s second-largest health insurance company Anthem hacked, nearly 80 million users'data leaked [EB/OL]. [2020-02-11]. https://www.freebuf.com/news/60134.html.
[2] 737 million global medical data leaked, involving over 20 million people, affecting 52 countries [EB/OL]. [2020-02-19]. https://www.infoq.cn/article/8VZ8aVetNvRQ2VCmHl4u?utm_{s
[3] Xinhua News Agency. Xi Jinping emphasizes during the 18th Central Political Bureau collective study session: Take blockchain as an important breakthrough for core technology independent innovation and accelerate blockchain technology and industrial innovation development [EB/OL]. [2020-02-19]. http://www.xinhuanet.com/politics/leaders/2019-10/25/c_{1125153665}.htm.
[4] Hong Jian, Li Rui, Xu Wangquan. Overview of medical health data privacy protection technologies [J]. China Digital Medicine, 2015, 10(11): 83-86.
[5] Wang Tianyi, Liu Aiping. Research on medical data privacy protection strategies under big data environment [J]. Information Technology and Network Security, 2019, 38(8): 28-32.
[6] Zhao Hanqing, Luo Jie, Wang Zhiguo. Information security challenges in internet medical health service models [J]. China Digital Medicine, 2019, 14(8): 92-93, 117.
[7] Li Zhiqiang, Kang Lijun, Wang Wencui. Research on big data security management strategies for medical information [J]. Computer Security, 2014(4): 84-86.
[8] Xu Yan. On introducing blockchain technology to promote "Internet + Healthcare" development [J]. Chinese Journal of Medical Management Sciences, 2018, 8(4): 40-44.
[9] Sun Baili, Mi Haiying, Li Ling. Preliminary exploration of healthcare big data information security protection strategies [J]. Modern Information Technology, 2019, 3(19): 156-158.
[10] Blanquer I, Hernández V, Segrelles D, et al. Enhancing privacy and authorization controls scalability in the grid through ontologies [J]. IEEE transactions on information technology in biomedicine, 2009, 13(1): 16-24.
[11] Liu Yimin, Wang Zhiyong, Qiao Jin, et al. Application and prospects of fine-grained access control technology in medical databases [J]. China Digital Medicine, 2008, 3(11): 45-49.
[12] Jia Ruilong, Cao Yazhou, Miao Junqing, et al. Design and application of medical data privacy protection management based on improved CP-ABE model [J]. Computer Measurement & Control, 2020, 28(1): 200-204, 209.
[13] Wang Hui, Liu Yuxiang, Cao Shunxiang, et al. Research on medical data storage mechanism incorporating blockchain technology [J/OL]. Computer Science: 1-9. [2020-03-19]. http://kns.cnki.net/kcms/detail/50.1075.TP.20200225.1400.006.html.
[14] Andy E. Could bitcoin technology help science? [J]. Nature, 2017, 552(7685): 301-302.
[15] Patel S, Vishal M. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus [J]. Health informatics journal, 2018, 25(4): 1398-1411.
[16] Esposito C, Santis AD, Tortora G, et al. Blockchain: a panacea for

healthcare cloud-based data security and privacy? [J]. IEEE cloud computing, 2018, 5(1): 31-37.
[17] Li H, Zhu L, Shen M, et al. Blockchain-based data preservation system for medical data [J]. Journal of medical systems, 2018, 42(8): 141-154.
[18] Waal M, Ribeiro C, Ma M, et al. Blockchain-facilitated sharing to advance outbreak R&D [J]. Science, 2020, 368(6492): 719-721.
[19] Xu Peihai, Huang Kuangshi. Current status, problems, and countermeasures of healthcare big data in China [J]. China Digital Medicine, 2017, 12(5): 24-26.
[20] Hu Mo, Ma Jie. Research on the promotion mechanism of unbounded smart government from the perspective of information synergy [J]. Information and Documentation Services, 2019, 40(1): 44-51.
[21] He Pu, Yu Ge, Zhang Yanfeng, et al. Overview of blockchain technology and application prospects [J]. Computer Science, 2017, 44(4): 1-7, 15.
[22] Xue Tengfei, Fu Qunchao, Wang Cong, et al. Research on medical data sharing model based on blockchain [J]. Acta Automatica Sinica, 2017, 43(9): 1555-1562.
[23] Yuan Yong, Wang Feiyue. Development status and prospects of blockchain technology [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
[24] Hu Mo, Ma Jie. Research on multi-information synergy model for smart elderly care from the perspective of heterogeneous blockchain networks [J]. Library and Information Service, 2020, 64(7): 110-118.
[25] Shi Jin, Shao Bo, Miao Jie. Research on competitive intelligence sharing platform for SMEs based on blockchain [J]. Library and Information Service, 2019, 63(20): 112-120.

Author Contributions:
Li Hongchen: Wrote and revised the paper;
Ma Jie: Determined the topic and overall research framework, revised the paper;
Hu Mo: Revised the paper.

Note: Figure translations are in progress. See original paper for figures.