Global Business and Management Research: An International Journal
Vol. 15, No. 3s (2023)

Research on the Sustainability of Medical Services based on Blockchain Technology

Meiwen Guo [1 *]
[1] *Graduate School of Business, Universiti Sains Malaysia, 11800, Penang, Malaysia,*
[2] *School of Management, Guangzhou Xinhua University, 510520, Guangzhou, China*
[3]*School of Business, Sun Yat-sen University,510275, Guangzhou, China*
** Corresponding Author*: *meiwenguo@student.usm.my*

Cheng Ling Tan [2]
[1] *Graduate School of Business, Universiti Sains Malaysia, 11800, Penang, Malaysia,*
[2] *Department of Information Technology & Management, Daffodil, International University, Dhaka 1207, Bangladesh*

Abstract

Purpose: This study discusses the core technology of blockchain and its application in the medical field. At the same time, the characteristics of the application of blockchain technology in medical information sharing, drug traceability, telemedical monitoring, and diagnostic analysis were also discussed from the perspective of blockchain technology and security. Through the discussion, the promotion of this technology to medical services and the existing problems were understood. It aims to provide a reference for promoting research on the sustainable development of blockchain technology in the field of medical services.

Methodology: Qualitative research was conducted using the methods of literature reviews and case studies. After introducing the development background of blockchain, combined with the application cases of blockchain technology in the medical service field, this article introduces and analyzes the application of blockchain technology in the medical field from the perspective of privacy protection and security.

Findings: This study analyzes the application of three scenarios from the perspective of blockchain technology principles, security, and related theories: data sharing services, drug traceability, and remote monitoring and diagnosis. This article analyzes the different application situations and problems of three scenarios from the perspective of technical theory and practice, providing research references for the theory and practice of blockchain technology in this field. In addition, it also conducts a preliminary discussion on the conflicts between privacy protection and security issues and applications and proposes some preliminary solutions.

Research limitations: Regarding the conflict between privacy protection and security issues in the application of blockchain technology to medical services, the study only provides some preliminary issues and solutions, but does not provide a more in-depth discussion of technical solutions. Currently, this aspect is still a relatively thorny issue, and further research is needed in the future to strengthen the sustainable application of this technology in the medical field.

Practical implications: The study not only explores the feasibility of applying blockchain technology in the medical field from a technical perspective but also proposes some ways to address the conflict between privacy protection and security issues and technology applications, points out issues that need to be resolved, and offers some preliminary ideas for the sustainable application of blockchain technology in this field in the future.

Value: As an attempt to enrich the extant literature, this study considers both the impact of technology on improving medical services' sustainable development and the influence factor that motivates enterprises or related institutions to choose medical services with technology. This research is an exploration of blockchain technology in the sustainable development of medical services through the rich expansion of technical theory and practice. It also points out the security issues that need to be addressed in sustainable applications, and discusses their solutions in a preliminary way.
Keywords: blockchain, medical service, sustainable development, data sharing, privacy protection, security

1. Introduction

In contemporary society, blockchain technology is an innovation. Due to its technical attributes like decentralization, distribution, and traceability, it can successfully address data and information islands, privacy leakage, etc. It has outstanding benefits for managing patient data privacy, security, and integrity and has created a new path for the advancement of contemporary medicine and health care.

Medical records, such as personal basic health files, preventive health care service files, and medical record files of the entire diagnosis and treatment process, are the main types of files that contain comprehensive medical information. As part of the general trend of hospital development and health care, promoting the sharing of medical archive information is a necessity for citizen health management and precision medicine (Sun S., 2016). Traditional medical file information sharing has serious issues, including ineffective information exchange and simple privacy leaks, which not only harm patient-physician relationships but also impede and restrict the healthy advancement of health care.

In the medical industry, the regulation of medicine is crucial because it affects the legitimacy of channels, the control of drug distribution, the reliability of data, and the ease of user inquiries. Certain gaps exist in channel supervision, quality supervision, and data management in traditional medical supervision. Patients and users are negatively affected by drug counterfeiting and channel issues, and serious health risks are present. The tamper-proof, decentralized, etc. technologies will be heavily involved in the management of medical data, real-time channel tracking, and quality control.

The cloud-based ward inspection system boosts the effectiveness of medical administration. However, the data in the cloud-based ward inspection system cannot be made impenetrable and private. The implementation of blockchain technology helps it to exert its overall benefits. The combined technology ward round system enhances the cloud ward round system's data security and privacy protection. It has promising application possibilities.

The study is based on the application and research status of blockchain in the medical industry, combs through current literature related to blockchain technology in this field, and comprehends the technology's combined effect in the medical field of theory and practice. We described and analyzed the ward system as an example, and then we discussed the applicative advantages of blockchain technology in these aspects, the technical connection, and the problems that will be encountered. The research aims to provide a theoretical and practical basis for the medical business or related institution.

The research framework is divided into five sections: the first is the introduction, which introduces the current status of medical service, the development and application of blockchain technology, and the challenges faced by its application in medical data sharing and security, drug traceability, and telemedical monitoring. The second section presents the

relevant literature and its results from four aspects: Blockchain security technology in the medical field, medical data sharing, medical traceability, and telemedical monitoring, and reveals research from three perspectives and deeply analyzes the characteristics and gaps of research from each perspective in depth, which is carried out to provide a basis for revealing the research significance and research questions of this study and pointing out the necessity and importance of the research. The third part presents the methodology and material, which provides a comprehensive introduction to the main methods and sources of information for this study. The fourth section is the findings of this study, which are theoretical and practical findings based on literature research and case studies. The fifth section is the case, discussion, and conclusion. Firstly, three scenarios of medical information sharing, drug traceability, and telemedical monitoring are introduced as the case study, and the initial description of blockchain technology is given. The discussion is then based on the three scenarios, and the discussion is accompanied by the analysis of technical principles and practices, which provides a reference and basis for the combination of technical practice research and technical theory research. This is also the focus of this study. The corresponding insights of this study come from analyzing data sharing, drug traceability, and telemedical monitoring services from the perspective of blockchain technology and security. By analyzing the technical principles to explore the characteristics of its application in the field of medical services, to promote its sustainable application in this field. The logical structure of this study is shown below:

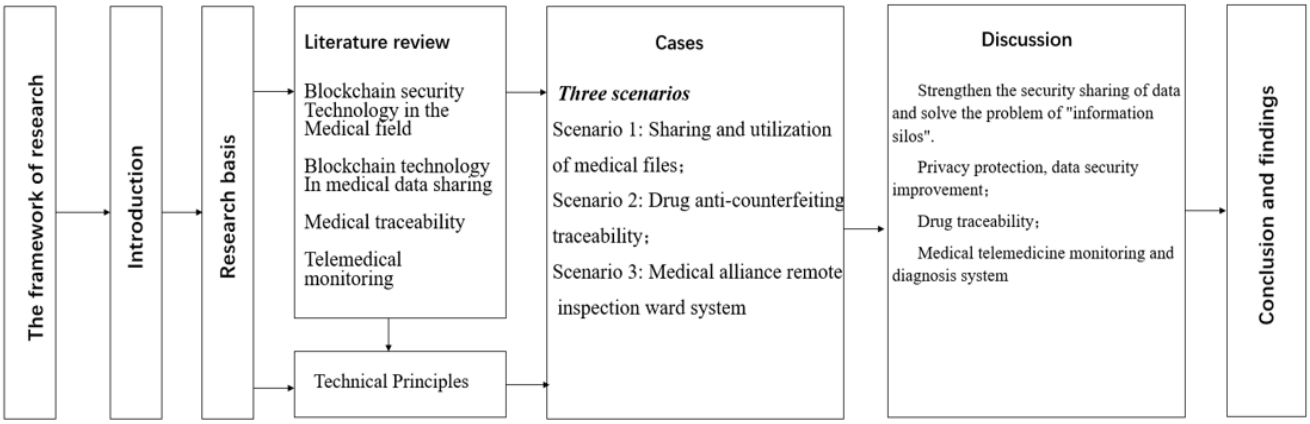


Figure 1 Research Framework

2. Literature Review

2.1 Blockchain security technology in the medical field

In the past few years, countries all over the world have put a lot of effort into researching how blockchain technology can be used in medicine. A significant amount of research has been carried out by industry professionals and academics regarding the opportunities and challenges presented by blockchain in the field of the sharing of medical information, as well as the privacy and security of data sharing. Researchers from the Massachusetts Institute of Technology and the BethIsrael Deaconess Medical Center in Israel collaborated in 2016 to develop and design a platform called MedRec for the management of sensitive medical data. The platform is based on the infrastructure of Ethereum smart contracts and uses a distributed method. Carry out studies on the authentication, encryption, sharing, traceability, and storage of medical data, as well as any other aspects of data security

that are relevant (Azaria, A., Ekblaw, A., Vieira, T., et al., 2016; Ekblaw, A., Azaria, A., Halamka, J. D., et al., 2016). eORders is a blockchain-based medical data management platform that was developed and designed by the American company Healthnautica. This platform improves the efficiency of the surgical process. The entire diagnostic and treatment process records cannot be easily modified, the identification of doctors and patients is made more convenient, and the traceability of treatment records is made more standardized, all of which contribute to a significant increase in the level of trust that exists between physicians and their patients (Shrier, D., Wu, W., Pentland, A., 2016). The efficiency of blockchain PHR management was demonstrated by Park et al. in their study, which utilized the blockchain principle (Park, Y. R., Lee, E., Na, W., et al., 2019). Zonyin Shar and colleagues used a technology called zero-knowledge proof to propose a data sharing scheme for clinical trials and precision medicine. This technology ensures that users on the chain remain anonymous. The authentication process is now easier to use and takes less time (Shae, Z. & Tsai, J. J. P., 2017). A well-known Swiss innovation company in the field of global digital health called Healthbank has developed and designed a variety of cutting-edge wearable smart devices (Peter, B. N., 2019). These cutting-edge wearable smart devices can easily monitor personal health data and combine blockchain technology to make medical data storage more convenient. Safety. PengZ, et al. carried out extensive research on collaborative cancer care, and using the fundamentals of blockchain technology, they proposed a big data scheme that could be specifically applied to identity verification (Jiang, S., Cao, J., Wu,H., Yang,Y., et al., 2018). Fu, et al. proposed a more effective encryption algorithm based on the credibility proof mechanism and the research results of others' blockchain (Fu, D. & Fang, Liri., 2016). At the same time, they simulated and analyzed the data attack scenarios perpetrated by criminals, and they optimized and improved the scheme for sharing medical data. Improve the safety of storing data and sharing it with others. Jiang S., et al. conducted extensive research on the sharing of medical data from various data sources (Zhang, P., White, J., Schmidt, D. C., 2018). Based on their findings, they proposed that during the process of health information exchange, the combination of offline storage and online verification can help to make the patient's private information more secure.

Tang Yanjun, etc. pointed out that using the technical characteristics of blockchain, such as the asymmetric encryption algorithm, timestamp, and distributed ledger, can ensure that medical data is not tampered with, and can effectively maintain the security of medical information (Tang, Y., Song, S., Jiang, C., 2020). This is in reference to the security assurance of blockchain technology. According to He Bo, et al., the utilization of a blockchain consensus mechanism, distributed storage technology, and asymmetric encryption technology can ensure the secure storage of medical data information as well as achieve the goal of efficient data sharing (He, B., & Wang, G., 2018). Zhou Lifeng, et al. designed a certificate-free aggregated signature scheme for wireless medical sensor networks (Pang, Z., Yao, Y., Zhang, X., 2021). The scheme is based on smart contract technology and a distributed hash table storage mechanism. This scheme can not only identify and authenticate users quickly and accurately, but it can also ensure that the sharing of medical data is accurate and secure. Using a hopping consensus hashing algorithm, a Byzantine fault-tolerant consensus mechanism, and asymmetric encryption technology, Li Li, et al. proposed a searchable encryption sharing scheme for multi-keyword association retrieval (Li, L., Wu, Y., Yang, Z., et al., 2022). This scheme realized the encryption protection of sensitive information in electronic medical records. fine-grained retrieval. Ji et al. proposed a blockchain-powered multi-level location sharing scheme (Ji, Y., Zhang, J., Ma, J., et al., 2018). It was based on the technology behind blockchains. Alibaba Cloud developed and designed a national physique monitoring model called Med-PPPHIS (Zhou, T., Li, X., &

Zhao, H., 2019). The model is based on blockchain closed-loop management of chronic diseases. Alibaba Cloud also conducted trial operations and promotion in Anhui Province (Zhou, T., Li, X., & Zhao, H., 2019). Using blockchain, digest chain, and structured P2P network technology, Shen Bingqing et al. developed and designed a medical data sharing scheme they called MedChain (Fan, K., Wang, S., Ren, Y., et al., 2018). This scheme significantly improved the effectiveness and adaptability of the process of sharing medical data.

The application of blockchain in healthcare system. Healthcare data is crucial personal privacy information data, and numerous industry experts have conducted extensive research on the security and privacy of access control for healthcare data. The concept of storing data in encrypted form to realize access control of patients' electronic health records and enable users to access control policies in accordance with fine-grained access control was invented by Goyal, et al. in 2006 after conducting in-depth research on medical data security (Goyal, V., Pandey, O., Sahai, A., et al., 2006). In order to achieve the privacy protection and keyword search functions of timed start. Yang, et al. developed a new keyword search mechanism in 2015 by combining the tester's designation and the proxy re-encryption technology to start regularly (Tang, Y. L., Xiang, W. U., et al., 2017). To address user anonymity and identity untraceability in electronic medical systems, Zhang, et al. proposed a three-factor key agreement in 2017 (Zhang, L., Zhang, Y., Tang, S., et al., 2018). In order to implement access control for patient electronic health records, Yang et al. used attribute-based approach encryption (ABE) (Yang, Y., Liu, X., Deng, R. H., et al., 2020). To address the issue of access control policy updates, they also proposed a brand-new access policy update mechanism based on keyword matching. Hua et al. created CAMPS, a medical privacy protection scheme based on the skyline diagnosis model, using partial decryption and security comparison techniques to safeguard the security and privacy of user healthcare data (Hua, J., Shi, G., Zhu, H., et al., 2020).

The blockchain is distinguished by the presence of anti-tampering measures, smart contracts, and multi-node management capabilities. It has obvious technical advantages in the management of medical data, particularly in the control of access to electronic medical records. Ekblaw, et al. proposed a healthcare data model that they called MedRec (Ekblaw, A., Azaria, A., Halamka, J. D., et al., 2016). This model allows users to gain access to and manage their personal healthcare data with smart contracts such as registration service contracts, patient-provider relationship contracts (PPR), and summary contracts. The hash index of the data is stored in the blockchain by Culver et al., which effectively expands the storage function of the blockchain (Culver K., 2016). The elliptic curve algorithm was utilized by AlOmar, et al. in order to develop and design the data privacy protection scheme known as MediBchain (Al Omar, A., Rahman, M. S., Basu, A., et al., 2017). This scheme is utilized for the storage management of patients' electronic health records, which further improves the security of data management.

2.2 Medical data sharing

Many professionals in the industry as well as academics have carried out in-depth research on the medical data privacy sharing model in order to facilitate further improvements in the utilization of data privacy. Zhang, et al. used the designed secure search protocol to build a medical data sharing architecture dedicated to sharing patient health data among various medical institutions (Zhang, A., & Lin, X., 2018). This architecture allows for physicians to search an index of interested patients while effectively protecting patient privacy. To realize data interaction and optimize interaction between authorized users and hospitals, Xu et al. built a health chain architecture using a key transaction data structure and

a fine-grained access control strategy (Xu, J., Xue, K., Li, S., et al., 2019). This improved the efficiency of data sharing as well as its level of security. Huang Jingying, et al. elaborated on how to apply blockchain technology in medical alliances and proposed the problems and challenges encountered in the specific application process and how to deal with them based on the connotation of medical alliances and the characteristics of blockchain (Huang, J., Fan, Q., 2019). The medical and health data security sharing model and circulation process, which combine chain and cloud computing, are designed, as are the functions of the medical consortium medical and health data sharing platform, which are based on the alliance chain, including medical and health data sharing, patient referral, medical and health data supervision, user management, medical and health data query, and other functions that provide reference and reference for the circulation and safe shredding. Song Bo et al. designed the layered architecture of the medical alliance based on the alliance chain, proposed the workflow of the medical alliance blockchain system, and implemented the blockchain-based medical alliance platform using the Go language, which effectively solved the problem (Song, B., Liu, Z., Feng, Y., 2020). The medical alliance's data cannot be shared, and data security is inadequate. According to the problems that exist in the medical alliance's information construction process, Li Yiyu, et al. present some challenges in the application of blockchain technology to the medical alliance's information construction, as well as the characteristics and advantages of blockchain technology (Li, Y., Yang, X., 2020). Some possibilities for combining blockchain and medical alliance information technology. Wang Jianguo et al. proposed an electronic prescription sharing and circulation model (Wang, J., Li, S., 2021). Wang Tianyu, et al. proposed a blockchain-based method for analyzing problems in the circulation and sharing of medical and health data in the medical alliance, as well as the current state of medical and health data sharing in the medical alliance, using blockchain and related technologies (Wang, T., Wu, M., Zhou, Y., 2022).

2.3 Medical traceability

An RFID-based regulatory traceability system was proposed by Huang, et al. in the year 2010 (Huang, G. Q., Qin, Z., Qu, T., 2010). This system offers advantages in terms of electronic genealogy and traceability not only to medical managers and patients, but also to other individuals involved in the supply chain. A quality traceability system for traditional Chinese medicine based on a two-dimensional code was proposed by Cai Yong, et al. in the year 2016 (Cai Yong, Li Xiwen, Ni Jingyun, et al., 2016). This system can track both the external information, such as the production, processing, and circulation processes of medicines, and the internal quality changes of traditional Chinese medicines. Through a comparative study of several different product traceability systems in 2018. Benatia, et al. proposed a data management system that is based on big data technology for the collection, storage, analysis, and visualization of data (Benatia, M. A., Sa, V. E. D., Baudry, D., et al., 2018). This system can ensure communication between various supply chain participants. Yu Zhong, et al. have developed a Blockchain-based medical anti-counterfeiting traceability system to solve the issues that are present in traditional methods of medical anti-counterfeiting traceability, such as information centralization and the ease with which it can be tampered with, insufficient storage information, and information privacy concerns (Yu, Z., Guo, C., Xie, Y., et al., 2020). The system encompasses a variety of upstream and downstream terminal links, such as hospitals, distributors, and pharmaceutical factories, amongst other establishments. Consumers are able to obtain all traceability information, which includes information on drug production, logistics, and usage, and the functions of the pharmaceutical anti-counterfeiting traceability system can become more comprehensive. Using the interstellar file system to carry out the combination of on-chain and off-chain, Li

Manyu, et al. proposed a drug traceability scheme based on Fabric and IPFS for the centralized data storage and easy tampering in the current drug system (Li, M., Yu, P., 2022). They realized that the production and processing of drugs, transportation, and use are monitored throughout the process.

Wei Anqi, et al. claim that the application of blockchain technology in the field of medical treatment has the potential to effectively and efficiently gather and integrate pertinent medical and pharmaceutical data information (Wei, A., Chen, M., 2019). While distributed storage technology enables the information to be stored in multiple locations, timestamp technology ensures that the circulation information of medicines is accurately recorded and cannot be changed. This system makes it possible to implement multi-agent accounting for the entire process and real-time drug monitoring, which greatly aids in finding a solution to the issue of one-way traceability of drugs. According to Xue Tengfei, et al. interpretation, the storage and modification of medical data information that is present on the chain require the digital signature of the hash tree in the block body (Xue, T., Fu, Q., Wang, J., et al., 2017). The block header uses the root value of the hash tree while the timestamp technology is used to add the time stamp. These two processes happen at the same time. A blockchain is used to store the transaction records of how instructions are carried out and data is calculated. The security and traceability of information relating to medical data can thus be achieved. By creating a medical data share model (MDSM) based on blockchain technology, it is possible to realize decentralized storage and secure sharing of pertinent medical information data. The use of blockchain technology in healthcare, according to He Bo, et al. has the potential to completely record all the relevant details and data of an operation on the blockchain (He, B., Wang, G., 2018). The records that are stored on the blockchain can be used to identify the parties at fault for a medical accident because the data that is stored on the chain cannot be altered in any way. According to Tang Yanjun, et al. research, applying blockchain technology to the distribution and use of medical supplies and taking advantage of its traceability can also aid in identifying the perpetrators of medical malpractice.

2.4 Telemedical monitoring

The application of blockchain in the field of telemedicine monitoring. It was proposed by Dey T., et al. that intelligent medical equipment could be used to monitor and collect data on patient health, and that blockchain technology could be used to share, analyze, and calculate the data (Dey, T., Jaiswal, S., Sunderkrishnan, S., et al., 2017). This information could then be used to assist physicians in the process of remotely monitoring and diagnosing patients. When abnormal patient health data is found, the background data center triggers alarms as appropriate to give early warnings to doctors and patients, thereby improving the efficiency of medical monitoring. These three smart contracts were deployed in the design of the telemedicine monitoring model by Griggs et al. based on the Ethereum platform (Griggs, K. N., Ossipova, O., Kohlios, C. P., et al., 2018). This allowed the background data center to collect, judge, and preprocess patient health data in a timely manner. PCAO is a blockchain-based telemedicine monitoring scheme that was proposed by Uddin, et al. (Uddin, M. A., Stranieri, A., Gondal, I., et al., 2018). This scheme's primary objective is to strengthen the protection of patient privacy information during telemedicine monitoring. In response to problems in the process of remote hierarchical diagnosis and treatment, Zhong Liwei, et al. designed a blockchain-based hierarchical diagnosis and treatment system for remote medical institutions, and provided specific solutions (Zhong, L., Chen, C., Song, J., et al., 2018). Wang Wei, et al. developed and designed a telemedicine privacy protection scheme that they called TMS (Wang Wei., 2019). This scheme makes it possible for users, hospitals, and doctors to interact with data in a manner that is both secure and effective. This is

accomplished by strengthening the design of the user chain, medical chain, and identity chain, each of which has certain practices. Balistri, et al. and others attempted to store the health data of patients on the blockchain, designed a new health data privacy protection and sharing scheme, and used the technology of smart contracts to solve the problem of data silos in the field of telemedicine data sharing (Balistri, E., Casellato, F., Giannelli, C., et al., 2020).

Through literature review and in-depth study, we understand that most studies are conducted from the perspective of technological breakthroughs and innovations, which enrich the research on blockchain applications in healthcare from the technical theoretical level and provide research references for the theoretical applications and practices of blockchain technology in more fields. The research on privacy and security also provides a reference for the stable application of blockchain technology. Through combing through much of the literature and exploring it in depth, there are generally three research gaps that need attention, as follows:

First, research from the perspective of blockchain security technology applications can be divided into two categories. One category is the research that does not address the contradictions of blockchain technology in healthcare data sharing, i.e., the discussion on how to balance the conflict between distributed data storage and privacy protection, which are the characteristics of blockchain technology, and the balance countermeasures. This is one of the important contradictions affecting the sustainable development of blockchain technology in healthcare, which is worth exploring with a new approach in this study. Another type of research is the prospective application of blockchain security technology in healthcare systems, which focuses on privacy protection, secure storage and access services for patients or users, and efforts to improve the quality of security services. Most of the studies have not focused more on how patients and users can share and apply data effectively. This also leaves certain research gaps in terms of where and how blockchain security technologies can be applied, how they are shared, and how secure they are, which also affects the issue of sustainability in the field. Research in this area will provide a new and innovative perspective.

Second, the role of cryptography in blockchain applications is explored from the perspective of technical principles and practices. For example, asymmetric encryption algorithms ensure that medical data are not tampered with and reduce security risks; security is verified from the perspective of data storage. Most studies optimize algorithm performance and improve security by improving encryption algorithms to increase algorithm efficiency, computational power, and effectiveness. In the sharing and application of medical data, more data sharing models and analysis are explored from the perspective of technical principles, and rarely involve the analysis and study of integrated medical application scenarios using a case study approach. With the continuous development of science and technology and medical services, patients' or users' medical data will be widely shared and utilized across time and space constraints, which will also facilitate the continued development of medical research and bring new health care experiences to human beings. Therefore, deep innovation in this field is fundamental to promote its sustainable development and is worth exploring.

Third, the application of blockchain security technology in different application scenarios. For example, research from the perspective of medical data sharing, drug traceability, telemedical monitoring, and treatment. In such research, blockchain technology usually solves the shortcomings of time and space limitations on some medical services. For example, medical traceability usually addresses the security of drugs from production to delivery and distribution, realizing the irreversibility of recording methods and enabling retrospective review across time constraints; telemedical monitoring needs to address the problem of grasping and monitoring remote information and data across time and space due

to distance constraints; remote therapy involves the application of scenarios such as remote diagnosis or remote surgery, especially the data security in this process and traceability issues in this process. Various studies have addressed different issues from different perspectives from different medical clinical needs to reflect the safety and effectiveness of blockchain technology in addressing multiple medical service needs. Its rich application scenarios and good security test results deserve in-depth study. However, there are few studies on case scenarios with integrated multiple healthcare services based on blockchain technology, and this study can also reflect its differences and innovations in this regard.

In summary, we present the problem statement as follows:

First, to sort out the relevant technical principles of medical privacy protection and data security under blockchain as the theoretical basis of this study, especially the relevant technical principles that can correspond to the subsequent case studies.

Second, analyze the application of medical scenarios based on blockchain security technology, mainly focusing on the application of three scenarios: medical data sharing, drug traceability and telemedicine monitoring.

Thirdly, the application characteristics of blockchain security technology in scenario application analysis are sorted out, and suggestions are made for theoretical research in this field from the perspective of practical analysis to provide reference for the sustainability research of medical data services.

3. Methods and material

3.1. Methods

This study's use of literature research and case study is motivated by three factors. To begin with, the study combed the literature on blockchain development in the medical field; blockchain applications in medical data sharing and privacy protection; blockchain application challenges; and so on. This can inform the reader about the current state of research, challenges, and opportunities in the use of blockchain technology in medical services. Second, there are few research studies on the multi-scenes but most research focuses on one scene. The case we use includes three scenes. Third, the study of blockchain applications in medical services is a complex multidisciplinary study that includes interdisciplinary studies in computer science, blockchain technology, information science, medical services, health management, and so on. As a result, employing the case study method aids in the advancement of theoretical research. This study used a multi-scene approach as well as a mixed method of literature research and case study to explain the hints of the development of this area.

3.2. Materials

The data sources of the study are mainly data released by Internet information platforms such as Google, Baidu, and research report. For example, the development of blockchain, the application of blockchain in medical, hospital network news. In addition, the theories and cases used in this study are authentic, and relevant literature is provided by authoritative databases, such as the Web of Science, EI, Scopus, etc. Nearly 100 papers have been consulted and studied, including more than 50 journals, and nearly 60 key papers have been cited in this study.

4. Findings

This study analyzes the application of three scenarios from the perspective of blockchain

technology principles, security, and related theories: data sharing services, drug traceability, and the use of remote ward technology. Through research, the following findings were made:

To begin with, decentralized data management can be realized using blockchain-based data sharing technology, which can be widely used both inside and outside medical and other related enterprises and institutions to effectively realize the intelligent flow and application of data and effectively solve the unfavorable situation of information islands and insufficient data utilization.

Second, the use of blockchain Traceability Technology would encourage firms to constantly enhance the quality standard system of medications in response to market demand. At the same time, the deployment of this technology in the industrial value chain's production, wholesale, and sales linkages can increase supply chain management efficiency. Data information flows can be generated during the drug production and financing processes, making it easier to control drugs information flow accurately.

Finally, remote data sharing, monitoring, and utilization can help medical firms give better remote services to users, which is favorable to sharing high-quality medical information services globally, establishes the groundwork for medical firms or institutions to undertake a global strategy and deployment.

The study not only explores the feasibility of applying blockchain technology in the medical field from a technical perspective, but also proposes some ways to address the conflict between privacy protection and security issues and technology applications, and points out issues that need to be resolved and preliminary ideas for the sustainable application of blockchain technology in this field in the future.

5. Case studies, discussion, and Conclusion

5.1 Cases studies

Three scenarios are described and analyzed: medical data sharing and utilization, drug anti-counterfeiting traceability, and the current status of the telemedicine monitoring and diagnose system. The potential applications of blockchain in the medical field are discussed.

5.1.1 Three Scenario

Scenario 1: Sharing and utilization of medical files

There are some storage and computing capacity issues with the conventional medical system. It is kept in a specific place, usually in facilities that produce medical file data, like hospitals, and centralized storage makes it difficult to share and use information effectively. Additionally, a single point of failure will increase the risk of data loss and manipulation, which is unavoidable even in the case of management supported by cloud technology. Furthermore, the user's medical data is quite unique, involving their privacy and necessitating access control of data privacy. In order to meet the user's health needs, the user's data may be shared within a reasonable range; however, the use of the data necessitates reasonable grant and security controls. It is more challenging to guarantee data security for users' cross-institutional needs services because the data services based on cloud technology, which are widely used today, have not been able to achieve the functions of privacy protection and anti-tampering.

Scenario 2: Drug anti-counterfeiting traceability

The public's awareness of the significance of drug quality in people's lives and health is growing. Now, some drug manufacturers, distributors, medical institutions, and so on are pursuing economic benefits at the expense of drug quality and safety, posing a significant

threat to public safety. With the continuous advancement of the global medical system's improvement, it is critical to strengthen the construction of the drug visualization process, strengthen drug traceability, and continuously improve drug safety, thereby ensuring people's health. The advent of blockchain technology provides strong technical support for the authenticity and validity of drug data, as well as drug traceability from production to circulation and use, opening a new development path for medical anti-counterfeiting traceability.

Scenario 3: Medical alliance telemedicine monitoring system

Telemedicine monitoring system is a new medical model in which experts from higher-level, high-quality medical institutions use modern information technology to connect with lower-level designated hospitals to provide services such as remote disease diagnosis and patient treatment for patients. Patients can overcome geographical time and space limitations and achieve "minor illnesses not in the hometown," "serious illnesses in the county," and "critical illnesses in the city" through the remote ward round system, allowing them to enjoy high-quality medical service resources while not only reducing the number of patients in the hospital. Traveling back and forth on the way to seek medical treatment and medicine reduces patients' medical expenses, frequency of going out, and cross-infection of new coronary pneumonia against the backdrop of epidemic prevention and control normalization. Furthermore, remote ward inspections can improve academic exchanges between medical institutions at various levels and between doctors, resulting in strong data support for medical research.

However, the medical and health data storage in the medical alliance is currently dispersed, and the data of different medical institutions are independent of each other and in an "isolated island" state; the diagnosis and treatment records and inspection data of different medical institutions cannot be guaranteed not to be tampered with or forged. The sharing of medical and health data does not have effective control methods for the trust of medical workers across institutions, which will lead to the abuse of patients' medical and health data or cause privacy leakage for a long time. The a forementioned issues have had a significant impact on the services of medical and health data within the medical alliance. It provides a policy and technical foundation for the circulation and safe sharing of medical and health data within the medical alliance through the widespread application of advanced information technologies such as cloud computing, Internet of Things, blockchain, artificial intelligence, and so on. More and more countries place a high value on the development of "Internet + medical health" and "blockchain + medical health," encourages medical institutions to strengthen policy and technological alliances, and aggressively develops telemedicine services such as remote consultation and remote ward inspection.

5.1. 2 The sustainability of medical services based on blockchain technology

Blockchain technology has three characteristics of traceability, non-tampering and decentralized distributed accounting, and has broad application prospects in the field of medical file information sharing.

5.1.2.1 Strengthen the security sharing of data and solve the problem of "information silos".

The blockchain based on distributed ledger technology provides a clearly visible network for data information, enabling the recording, storage, and sharing of medical data to be completed under the mutual supervision and joint maintenance of multiple parties, which is equivalent to adding several checks to the data to ensure that the information sharing is open, transparent, and scientifically accurate. At the same time, distributed ledger technology

simplifies complex multi-party reconciliation, effectively solves the problems of low work efficiency and chaotic working status in traditional file information management, and makes data sharing more accurate and efficient. In addition, the smart contracts of the blockchain help to build a market for mutual information sharing and make medical data sharing more convenient and secure (Ren, Y., 2018).

Blockchain data is a chain structure. The multi-node data chain has a consistency ratio and optimizes the basic process of traditional information processing, which greatly improves the management and use efficiency of data information. It is very suitable for residents' medical activity records and health care records. such as many scattered isolated nodes for medical file information storage (Zhao, J., Ma, J., 2019). The data on each block node is marked with the corresponding hash value, which can help users verify the integrity of the information and can quickly trace back to when, where, and who reviewed and modified the information, which is convenient for information tracking, traceability, and auditing. Since different nodes are independent of each other, the data entry of a single or multiple nodes will not affect the data of other nodes, and the data is jointly maintained and controlled by multiple nodes. It greatly improves the security of information sharing and ensures the sharing of medical file information. Therefore, the hospital can store, share, and circulate key medical data and bills safely. As shown in the figure:

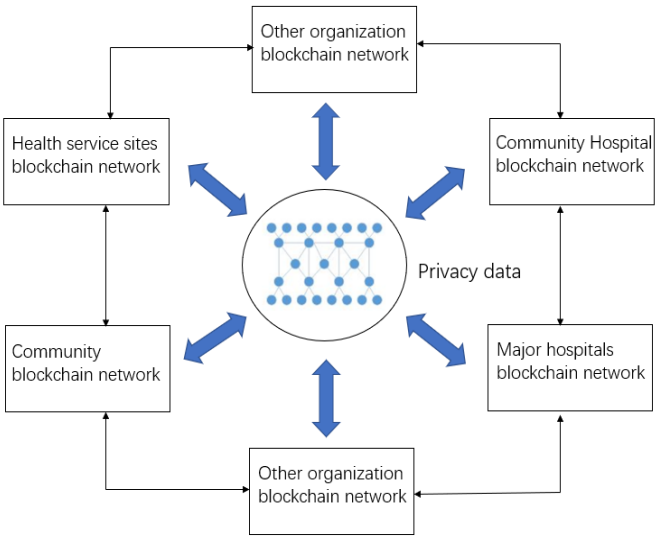


Figure 2. Cross organizations data sharing and privacy protection based on blockchain technology

As shown in Figure 2, the model involves multiple heterogeneous blockchain networks, including health service station blockchain networks, community blockchain networks, community hospital blockchain networks, large hospital blockchain networks, and other organizational blockchain networks. Together, these heterogeneous networks form a large health blockchain network. Every medical data institution node will have a local server.

Blockchain technology provides a solution to the problem of data sharing. Each institution in the model stores the original data in its own database, submits a small amount of private data to the blockchain network for storage. If there are any data query requests, they are forwarded to the original data provider through the blockchain network for query. If there is a need to share medical data, Patients and users who also need to ensure privacy are a better solution for data storage and utilization. It mainly utilizes the data tamper ability of the blockchain to achieve data security and reliability. This feature is also the foundation for

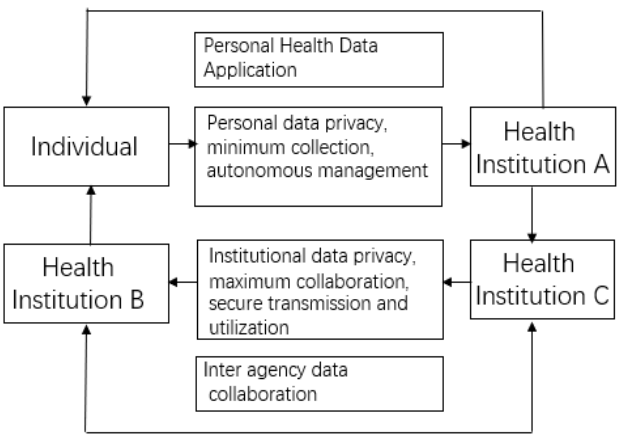
building a technical architecture. In the model, various institutions are interconnected, forming a blockchain interconnection network. In this network, private data can be stored and managed by providers, while in the blockchain network, sharable data is distributed. Another type of request is for sharing detailed data, such as more detailed disease or health data of patients or users. This type of data can be requested and transmitted point-to-point. Due to limited access, query requests for this type of data only correspond to health institutions that have this portion of data. Health institutions that provide data also need to encrypt the transmitted data to prevent theft when intercepted by third parties, The providers of this part of data also define it as non-open data, and formulate targeted provision plans for shared and protected data.

5.1.2.2 Privacy protection, data security improvement.

The issue of medical data privacy protection is an important issue related to the life and health of patients. From the perspective of access control, all node data in the alliance chain must be authenticated before they are allowed to join the network, and all authorized nodes in the alliance chain share the transaction ledger. Relying on the hash value marked on the data of each node, the source and use of medical data can be traced, and the non-tampering of the data ensures the security and integrity of the data. Each data record is verified by the consensus mechanism, which can effectively prevent data tampering and repeated operation problems and build a bridge of trust for all parties on the chain (Li, X., 2019). In addition, relying on different encryption algorithms, the information sharing and exchange of the blockchain is more secure and reliable.

According to relevant statistics, the average annual medical data generated by the entire medical industry system is about 40 trillion GB. Since there is no efficient and convenient data exchange and sharing mechanism between hospitals and medical organizations, such a huge amount of medical data is not only lacking. Fully utilized, on the contrary, it will cause greater pressure on the operation and maintenance of the back-end systems of medical institutions, which is very unfavorable to the development of hospitals, medical institutions, and even the entire medical and health industry. In addition, because medical data contains a large amount of personal privacy data, in the process of medical data management and sharing, due to the traditional data management center's storage capacity and computing power not keeping pace with the explosive growth of data, data loss, data sharing information islands, etc., the problem is more prominent. In addition, the traditional data management platform lacks a security protection mechanism, which makes it easy to cause malicious node attacks and is prone to other risks such as single-point data tampering and data leakage.

In order to solve the problem of inefficient storage and operation and maintenance of the medical service sharing system in the traditional way, building a personal health data and medical service data sharing platform using blockchain technology is one of the most effective ways to solve the above drawbacks (Zhang, C., Zhu, L., Xu, C., et al., 2018). By providing a public, digital, and distributed ledger, blockchain technology not only ensures the integrity of data but also ensures that data security is not easily tampered with, opening a new world for medical service data storage (Wright, C., S., 2008).



Resource：Jiazi Light Year

Figure 3 "Double loop" for privacy protection and data value

As shown in Figure 3, we can see a "double-loop" model of privacy protection and data value, which gives the user the power to manage important data from the user's perspective, and the user can decide whether to share the data and to which organizations. Since the application scenarios of medical data faced by users will change, users can also selectively disclose content according to the needs of the scenario and the level of security when the scenario changes. Since the service provider can provide services based on a small amount of verified data from the user in a distributed environment, the user does not affect the service relationship and agreement established between the service provider and the user, even if the user treats the critical data confidentially. This is an effective and safeguard the privacy of users. In addition, the service provider can adopt techniques such as federated learning to collect, process and analyze the health data authorized by the user. The closed-loop value system in the figure is conducive to safeguarding users' personal privacy and respecting their wishes while improving the quality of their medical or health services, and it provides a reference for promoting personalized medical or health services.

5.1.2.3 Drug traceability

From production to patients, drugs need to go through the processes of production and processing, logistics and transportation, and retail use. During this process, different upstream and downstream parties in the supply chain, including drug manufacturers, distributors, hospitals, and patients, jointly participate. In the traditional medical anti-counterfeiting traceability system, medical data is stored in the central database. Due to the insufficient data information storage system, it is difficult to complete the query of the production, circulation, and use of drugs through the drug traceability source code, and the data privacy is poor. It is easy to cause the leakage of personal privacy data of users. In addition, due to the central accounting mode used for traceability authentication, the risk of data being tampered with during uploading, storage, and querying is high (Li, M., Wang, D., Zeng, X., et al., 2019). The Blockchain has the characteristics of being difficult to tamper with, time stamp and transaction traceability, which provides a new development direction for solving the traditional medicine anti-counterfeiting traceability system (Hao, K., Xin, J., Huang, D., et al., 2017).

(1) The decentralization and distributed storage characteristics of blockchain technology ensure the openness and transparency of drug data information and the integrity and reliability of data flow. In the drug traceability system based on blockchain technology, drug manufacturers, distributors, hospitals, etc. are authenticated as independent node organizations, and then deployed to different operating environments with chain codes. The production and circulation of drugs and usage and other related information are uploaded to the blockchain through the internal authentication and encryption of each node organization, and the data of each process has a corresponding hash value. Based on the decentralization of blockchain technology, data is difficult to tamper with and transactions are traceable. It ensures that drugs can be traced back to every participant on the chain, and the entire process of drugs can be traced back, ensuring the reliability of drug data. Since Yaoping anti-counterfeiting traceability information is transparent, consumers can use the drug traceability source to initiate a drug query request, and they can clearly and completely query all the information about the drug from production to circulation to use.

(2) The combination of cryptography and decentralization technology of blockchain technology ensures the reliability of drug data and effectively solves the problem of

counterfeiting and shoddy in the drug supply chain. Decentralization is the core advantage of blockchain technology, which makes data tampering and other illegal acts impossible to hide (Chen, Y., Ding, S., Xu, Z., et al., 2018). Combined with cryptography and distributed ledger technology, the data of each block node has a hash value, which is encrypted and stored in the same ledger. All the data stored on the chain cannot be easily tampered with (Dong, G., Chen, Y., Zhang, Z., et al., 2018). In addition, each participant in all chains of drug production information, data flow, and other information can query and monitor each other to ensure the reliability and integrity of drugs (He, P., Yu, G., Zhang, Y., et al., 2017). Therefore, whether it is a manufacturer or a distributor, it is necessary to certify that if you want to make a fuss about medicines, you have nowhere to hide, you will pay the corresponding price, and to a certain extent, the problem of counterfeiting and shoddy medicines has been eliminated.

(3) The characteristics of blockchain technology data tamper-proof and time stamp can realize evidence and accountability, and solve medical malpractice disputes in various Chinese medicines. Using blockchain technology such as anti-tampering and time stamping technologies and applying it to electronic medical record information storage, disease diagnosis and treatment process, drug use, and other links, it can easily and accurately trace the relevant responsible parties and responsible persons in medical malpractice disputes for the health of medical and health care. Development provides more favorable guarantees (Xiao, L., Tan, X., Xie, P., et al., 2017).

5.1.2.4. Medical telemedicine monitoring and diagnosis system

From the current point of view, it has become an effective way to let patients stay at the grassroots level, realize the desire for hierarchical diagnosis and treatment, and form a close medical consortium through vertical integration. As an innovative attempt, the medical consortium has made active explorations in promoting the hierarchical diagnosis and treatment system and coordinating the supply and demand of medical resources, and has become an important way for patients to enjoy high-quality medical services nearby.

Remote information sharing not only facilitates viewing of the ward, but also facilitates the interaction between patients and doctors. The doctor who sees the patient issues the patient's medical and health data sharing request, and the patient authorizes it to determine whether to share the personal medical and health data. After the patient agrees to share, his medical and health data will be stored on the alliance chain. In order to ensure the patient's privacy, The patient ID on the chain is generated by the alliance chain according to the patient's ID number and medical ID. At the same time, the patient's medical and health data abstract and storage address are stored in the alliance chain. All authorized users of the alliance chain can view the medical and health data of patients. Patients can also cancel the shared medical and health data at any time, fully respecting the wishes of patients and ensuring the rights and interests of patients.

Blockchain smart contract is a computer program that can be automatically executed without manual intervention under certain conditions (Yang M., Ding L., Xu Y., 2019). Its working principle is like the function of the if-then statement in computer programming languages. According to different conditions , perform different operations (Ma X.F., 2020); then, according to the patient's condition, the hospital to which the referral is made can choose remote consultation and remote outpatient clinic, and the patient can also come to the referral hospital on the spot to make appointments, see a doctor, pay fees, and view electronic medical records, etc. , the receiving doctor further diagnoses the patient's condition based on the patient's examination results, treats the patient, and can also refer the patient according to the patient's condition.

The patient referral service requires the patient to submit a patient referral application on the sharing platform, and the doctor who sees the patient confirms the referral, and then the hospital where the patient visits again. All records, combined with the actual condition of the patient at the time of the doctor's visit, can be used for re-diagnosis and treatment of the patient, which improves the efficiency of the doctor's consultation and diagnosis and treatment, and avoids the repeated examination of the patient and reduces the cost of the patient's medical treatment.

The competent department of health supervision shall supervise medical institutions and the medical information of patients shared by the hospital. For problems found in the supervision process, the source of the problem shall be traced, and the health supervision department shall give feedback to the hospital. Report the problems solved, and give corresponding treatment measures according to the instructions of the superiors, which further ensures the standardization of doctors' diagnosis and treatment and improves the quality of doctors' diagnosis and treatment. In the medical health data security sharing model proposed by Wang Tianyu, et al. (Wang T.Y., Zhang K.X., 2022), the hospital information system, laboratory information management system, image filing and communication system, electronic medical record management system, and some other clinical. The system is deployed on different cloud servers with high security and reliability to ensure the security of the original record storage of medical and health data. After the patient's authorization, the hash value and storage address of the medical and health data of patients in hospitals at all levels stored in the cloud platform are uploaded to the chain, that is, stored in the medical consortium medical and health data sharing alliance chain. The nodes in the alliance chain include tertiary hospitals, secondary hospitals, primary hospitals, community hospitals and health supervision departments. The patient medical health data uploaded to the alliance chain can be shared by hospitals, doctors and health supervision departments at all levels, and the health supervision department can audit the patient medical health data stored in the alliance chain.

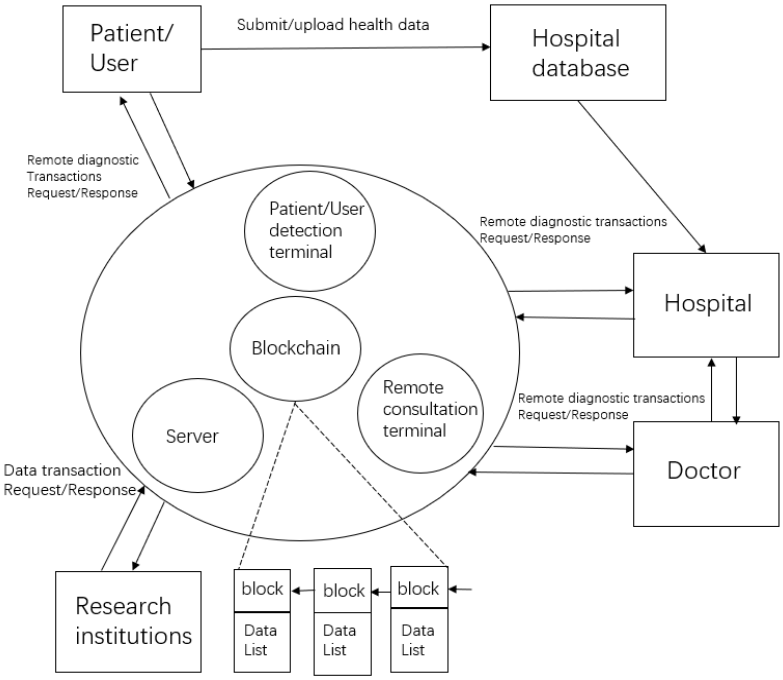


Figure 4 Telemedicine monitoring and diagnosis using blockchain technology

In a smart mobile medical system based on blockchain technology, as in Figure 4, patients or users can send or upload health data to the hospital database through the network as the collection source for data processing, and the hospital can be the main privacy information management center, responsible for the management of this part of non-open authorized data, and the patient or user holds the authorization of the private data, while the open data can be written into the smart mobile. The open data can be written into the intelligent mobile medical system, stored in the server, and the data backed up to the server will be sent to the doctor's remote consultation end for monitoring and diagnosis, and the diagnosis results and treatment plan will be sent to the server through the system; then the patient and the user can get the diagnosis results and treatment plan through the server. At the same time, the basic information of patients, such as patient ID, etc., contained in the data, monitoring data, diagnosis results and treatment plan, are written into the blockchain with corresponding time stamps, which is useful for monitoring and reviewing the data in the future, and each record written is irreversible, which plays a key role in preventing data tampering and ensuring data security.

5.2 Conclusion

This study discusses the core technology of blockchain and its application in the medical field. At the same time, the application characteristics of blockchain technology in medical information sharing, drug traceability, telemedicine monitoring and diagnostic analysis were also discussed from the perspective of blockchain technology and security. Through the discussion, the promotion of this technology to medical services and the existing problems were understood.

First, through data sharing services, people can transmit health data to doctors or medical institutions through the medical service data sharing system, monitor their own health data around the clock through intelligent medical equipment, and conduct operation and maintenance analysis on patient health data by the big data processing center. By giving health advice or preliminary diagnosis and treatment plans, doctors can also use the telemedicine system to diagnose patients, to protect the life and health of patients. And the safe and effective sharing of data provides a security guarantee for the traceability of medicines.

Second, blockchain has the advantages of immutability, decentralization, distributed storage, and advanced authentication management, which can effectively solve the problem of circulation and safe sharing of medical and health data within the medical alliance. It can realize the circulation and safe sharing of medical and health data of patients in different hospitals in different medical alliances, and record patient diagnosis and treatment data through blocks of blockchain, which can ensure the security and originality of data. Circulation between medical institutions in the consortium can promote the rational allocation of medical resources, avoid repeated medical treatment for patients, reduce medical costs, and improve the service efficiency of medical consortium medical institutions. The diagnosis and treatment of medical institutions in the body can be further accurately treated.

Third, blockchain technology is useful for building a platform for hospital-institution cooperation and medical service data sharing, and realizing the effective sharing of medical service data such as public health information, outpatient business information, clinical diagnosis information, patient health information, medical service equipment management, and medical traceability, can greatly improve the efficiency of medical research, better serve patients, serve the society, and also contribute to the further development of medical and health care.

Finally, regarding the conflict between privacy protection and security issues in the application of blockchain technology and medical services, the study only provides some preliminary issues and solutions, but does not provide a more in-depth discussion of technical solutions. Currently, this aspect is still a relatively thorny issue, and further research is needed in the future to strengthen the sustainable application of this technology in the medical field.

References

Azaria, A., Ekblaw, A., Vieira, T., et al. (2016) Medrec: using blockchain for medical data access and permission management [Paper presentation]. *International Conference on High Performance Computing and Communications*, Vienna. Austria.

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data [Paper presentation]. *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Cham.

Balistri, E., Casellato, F., Giannelli, C., & Stefanelli, C. (2021). BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. *ICT Express*, *7*(3), 308-315.

Benatia, M. A., Sa, V. E. D., Baudry, D., Delalin, H., & Halftermeyer, P. (2018). A framework for big data driven product traceability system [Paper presentation]. *4th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Sousse, Tunisia.

Cai Yong, Li Xiwen, Ni Jingyun, et al. (2016). Quality Traceability System of Traditional Chinese Medicine Based on QR Code. *Chinese Materia Medica, 39*(2), 275-280.

Culver K. (2016). Blockchain Technologies: A whitepaper discussing how the claims process can be improved. *Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States.

Chen, Y.，Ding, S.，Xu, Z.，et al. (2018). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems, 43*(1), 5.

Dong, G., Chen, Y., Zhang, Z., et al. (2018). Research on identity management and authentication based on blockchain. *Computer Science, 45* (11), 52-59.

Dey, T., Jaiswal, S., Sunderkrishnan, S., & Katre, N. (2017). HealthSense: A medical use case of Internet of Things and blockchain [Paper presentation]. *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, India

Ekblaw, A., Azaria, A., Halamka, J. D., et al. (2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data [Paper presentation]. *IEEE Open & Big Data Conference*, Cambridge, Massachusetts.

Fan, K., Wang, S., Ren, Y., Hui, L., & Yang, Y. (2018). Medblock: efficient and secure medical data sharing via blockchain. *Journal of Medical Systems, 42*(8), 136.

Fu, D. & Fang, Liri. (2016). Blockchain-based trusted computing in social network [Paper presentation]. *2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China.*

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). *Attribute-based encryption for fine-grained access control of encrypted data* [Paper presentation]. The 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems, 42*(7), 130.

Hao, K., Xin, J., Huang, D., et al. (2017). Decentralized distributed storage model. *Computer Engineering and Applications, 53*(24), 1-7.

He, B., & Wang, G. (2018). Application analysis of medical management informatization based on blockchain technology. *Journal of Sichuan University, 55*(6), 6.

Hua, J., Shi, G., Zhu, H., Wang, F., Liu, X., & Li, H. (2020). CAMPS: Efficient and privacy-preserving medical primary diagnosis over outsourced cloud. *Information Sciences, 527*, 560-575.

He, B., Wang, G. (2018). Analysis of medical management informatization application based on blockchain technology. *Journal of Sichuan University, 55*(6), 1219-1224.

He, P., Yu, G., Zhang, Y., et al. (2017). Review of Blockchain Technology and Application Prospects. *Computer Science, 44*(4), 1-7.

Huang, J., Fan, Q. (2019). Discussion on the application of blockchain technology in the construction of medical consortium. *Journal of Medical Informatics, 40*(10), 30-34.

Huang, G. Q., Qin, Z., Qu, T., & Dai, Q. (2010, June). *RFID-enabled pharmaceutical regulatory traceability system* [Paper presentation]. *IEEE International Conference on RFID-Technology and Applications*, Guangzhou, China.

Jiang, S., Cao, J., Wu,H., Yang,Y., Ma, M., & He, J. (2018). BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange [Paper presentation]. *IEEE International Conference on Smart Computing (SMARTCOMP)*, Taormina, Italy.

Ji, Y., Zhang, J., Ma, J., Yang, C., & Yao, X. (2018). BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. *Journal of Medical Systems, 42*(8), 147.

Li, L., Wu, Y., Yang, Z., et al. (2022). Sharing scheme of medical electronic medical records based on partitioned blockchain. *Computer Applications, 42*(1), 183-190.

Li, M., Yu, P. (2022). Research on the application of blockchain in drug traceability. *Information Technology and Network Security, 41*(4), 97-101.

Li, Y., Yang, X. (2020). Embedding blockchain technology into the information construction of medical consortium: internal logic and realistic challenges. *Journal of Xihua University, 39*(5), 78-87.

Li, X. (2019). Research on block-based electronic medical record sharing and privacy protection. Xi'an, China: Xidian University.

Li, M., Wang, D., Zeng, X., et al. (2019). Design of food safety traceability system based on blockchai. *Food Science, 40*(3), 279-285.

Liu, A., Du, X., Wang, N., Li, S. (2019). Big Data Access Control Mechanism Based on Blockchain. *Journal of Software, 30*(9), 2636-2654.

Ma X.F. (2020). The principle and practice of blockchain technology. *Machinery Industry Press. 1*.

Pang, Z., Yao, Y., Zhang, X. (2021). A scheme for secure storage and sharing of medical data based on blockchain. *Information Network Security*, (1), 5.

Park, Y. R., Lee, E., Na, W., et al. (2019). Is Blockchain Technology Suitable for Managing Personal Health Records? Mixed Methods Study to Test Feasibility. *Journal of Medical Internet Research,* 21 (2), e12533.

Peter, B. N. (2019). *Blockchain applications for health care*. Retrieved February 10, 2022, from http://www.cio.com/article/3042603/blockchain-applications-for healthcare.html

Ren, Y. (2018). Medical information privacy protection and sharing scheme based on blockchain. Xi'an, China: Xidian University.

Sun S. (2016). *Research on information sharing of medical files in public hospitals in Liaoning*. Shenyang, China: Northeastern University.

Shrier, D., Wu, W., Pentland, A. (2016). Blockchain & infrastructure (identity, data security ）. *Massachusetts Institute of Technology-Connection Science,1* (3),8-11.

Shae, Z. & Tsai, J. J. P. (2017). On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine [Paper presentation]. *IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, USA.

Song, B., Liu, Z., Feng, Y. (2020). Research on the architecture of the medical alliance system based on blockchain technology. *Computer Measurement and Control, 28*(9), 196-201.

Tang, Y., Song, S., Jiang, C. (2020). Construction of medical and health information platform under blockchain technology. *China Health Service Management, 37*(11), 4.

Tang, Y. L., Xiang, W. U., Qing, Y. E., Yan, X. X., & Jin-Xia, Y. U. (2017). Proxy re-encryption with keyword search scheme in cloud computing. *Journal of Chinese Computer Systems*, (10), 73-78.

Tan, M., Yang, J., Ding, L., Li, X., Xia, S. (2019). Overview of Blockchain Consensus Mechanism. *Computer Engineering, 26*(12): 1-11.

Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access, 6*, 32700-32726.

Wang Wei. (2019). Research on the privacy protection scheme of medical service data based on blockchain. *Information Technology and network security*, (8), 32-36.

Wang, T., Wu, M., Zhou, Y. (2022). A blockchain-based medical health data flow and security sharing scheme. *Information Systems Engineering*, (5), 4.

Wang, J., Li, S. (2021). Electronic prescription sharing and circulation model based on blockchain technology. *China Digital Medicine, 16*(10), 52-55.

Wang, Y., Zhang, A., Zhang, P., Wang, H. (2019). Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access, 7*, 136704-136719.

Wang T.Y., Zhang K.X. (2022). Research on regional medical and health data security sharing based on alliance chain. *Journal of Medical Informatics*. *43* (2): 57-61.

Wei, A., & Chen, M. (2019). Discussion on the application of blockchain technology in healthcare. *China Hospital Management,* (3):2.

Wright, C., S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved March 30, 2022, from https://ssrn.com/abstract=3440802.

Xiao, L., Tan, X., Xie, P., et al. (2017). Research on the traceability system of traditional Chinese medicine based on blockchain technolog. *Shizhen Chinese Medicine and Chinese Medicine, 28*(11), 2762-2764.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE Internet of Things Journal, 6*(5), 8770-8781.

Xue, T., Fu, Q., Wang, J., et al. (2017). Research on the medical data sharing model based on blockchain. *Chinese Journal of Automation, 43*(9): 1555-1562.

Yang, Y., Liu, X., Deng, R. H., & Li, Y. (2020). Lightweight Sharable and Traceable Secure Mobile Health System. *IEEE Transactions on Dependable and Secure Computing, 17*(1), 78-91.

Yang M., Ding L., Xu Y. (2019). Cloud storage and sharing scheme of medical and health data based on blockchain. *Journal of Nanjing University of Information Technology (Natural Science Edition), 11*(5):590-595.

Yu, Z., Guo, C., Xie, Y., et al. (2020). Research on medical anti-counterfeiting traceability system based on blockchain. *Computer Engineering and Applications, 56*(3), 35-41.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, *16*, 267-278

Zhou, T., Li, X., & Zhao, H. (2019). Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique Monitoring and Scientific Exercise Guiding. *Journal of Medical Systems*, *43*(9), 305.

Zhang, L., Zhang, Y., Tang, S., & Luo, H. (2018). Privacy Protection for E-Health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement. *IEEE Transactions on Industrial Electronics*, *65*(3), 2795-2805.

Zhang, A., & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *Journal of Medical Systems, 42*(8), 140.

Zhang, C., Zhu, L., Xu, C., & Lu, R. (2018). PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system. *Future Generation Computer Systems*, *79*, 16-25.

Zhao, J., Ma, J. (2019). The application of blockchain technology in residents' electronic health records. *Modern Hospital*, (2), 227-229.

Zhong, L., Chen, C., Song, J., et al. (2018). Research on the application of remote hierarchical diagnosis and treatment based on blockchain. *China Digital Medicine*, *15*(01), 4-7.