Online-Journals.org

JFSE Journal for Future Society and Education

JFSE | eISSN: 3078-6010 | Vol. 2 No. 1 (2025) | OPEN ACCESS

https://doi.org/10.3991/jfse.v2i1.53439

SHORT PAPER

Application of Blockchain Technology in Medical Dispute Management

Xiaofeng Wang[1], Xiaoguang Yue[1](✉), Ahthasham Sajid[2,3], Noshina Tariq[4]

[1]College of Management, Shenzhen University, Shenzhen, China

[2]Multimedia University, Cyberjaya, Malaysia

[3]Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

[4]Department of Artificial Intelligence and Data Science, National University of Computer and Emerging Sciences, Islamabad, Pakistan

xgyue@whu.edu.cn

ABSTRACT

With the increasing complexity of global health challenges and the growing awareness of health among individuals, the importance of personal health management has become more prominent. In modern society, due to the frequent occurrence of medical disputes, it has had a significant impact on the protection of the rights and interests of hospitals and patients. How to obtain necessary data in medical disputes and store it safely is a problem that everyone is facing. Against this backdrop, blockchain technology, with its features of decentralization, immutability, and high transparency, offers a potential solution. By leveraging distributed ledgers, cryptographic algorithms, and smart contracts, blockchain technology can effectively enhance the security and privacy of health data, enabling trustworthy data sharing and interoperability. While the application prospects of blockchain technology in personal health management are broad, its development faces multiple challenges, including technological complexity, issues of standardization, and incomplete legal and regulatory frameworks. Therefore, this paper's in-depth research on the application and impact of blockchain technology in medical disputes, exploring specific implementation pathways to enhance data security, privacy protection, data sharing, and interoperability, holds significant theoretical and practical value for promoting its application in the field of health management.

KEYWORDS

blockchain technology, health management, medical dispute, privacy protection

1 INTRODUCTION

Currently, the challenges of "difficult access to medical care" and "expensive medical costs" are widespread in society. Problems such as the uneven distribution of medical resources, long waiting times, and high expenses are prevalent, and the increasing occurrence of medical disputes has become a focal point of public concern.

To address the pain points in traditional hospital visits, medical and health institutions across the country have launched "internet hospitals." Internet hospitals offer a series of smart medical services, including online appointment and registration,

Wang, X., Yue, X., Sajid, A., Tariq, N. (2025). Application of Blockchain Technology in Medical Dispute Management. *Journal for Future Society and Education (JFSE)*, 2(1), pp. 48–54. https://doi.org/10.3991/jfse.v2i1.53439

Article submitted 2024-10-22. Revision uploaded 2024-12-03. Final acceptance 2024-12-18.

access to electronic diagnostic results, and online payment. However, due to technical limitations and management constraints, the Internet has not fully realized its expected potential. For instance, in the event of medical accidents, the storage and management of electronic medical record data, typically controlled by hospitals, may be susceptible to tampering.

In this context, this study proposes the use of blockchain technology to develop a medical data governance system that ensures multi-point consensus and autonomous guarantees. This system will interface with the existing electronic medical record systems of internet hospitals, enabling algorithm-driven autonomous data verification (absolute authenticity) and data traceability (verification of operator identity and time of operation). If implemented and promoted, this approach could enhance the governance efficiency of Internet hospitals (optimizing and safeguarding the medical process), significantly improve doctor-patient relationships, and bolster the credibility of government regulatory authorities.

2 LITERATURE REVIEW

Currently, international applications of blockchain technology in the healthcare field include the following cases and studies:

In 2015, Philips Healthcare established a lab to explore the role of blockchain in healthcare, proposing a decentralized real-time monitoring solution to address security challenges inherent in previous centralized storage systems. In 2016, the Estonian government launched a blockchain-based healthcare record security project to ensure the authenticity of data and trace changes in records [1].

Kshetri proposed that traditional healthcare institutions adhere to three modes for healthcare data interoperation: push, pull, and query. Blockchain provides a fourth mode: recording and sharing patients' lifetime medical records while maintaining patient control over the data [2].

Ichikawa developed and evaluated a tamper-resistant mHealth system using blockchain technology. This system uses a distributed network with digital signatures and timestamps to ensure the security and reliability of health data, enabling medical decisions to be based on accurate patient information [3].

Blockchain integrates cryptographic techniques, peer-to-peer transmission, distributed storage, and consensus algorithms into a new programming framework. It enables distributed, cross-institutional data storage, trusted verification, and traceability through computer algorithms without human intervention. Due to its ability to address challenges in multi-party collaboration and trusted processing, blockchain has been widely recognized as the cornerstone of a "programmable trust society" [4].

Currently, blockchain technology is primarily applied in the financial sector, with limited cases available for reference in social governance. Since its inception, blockchain technology has evolved into three main architectures—private chains (centralized), public chains (decentralized), and consortium chains (multi-centered)—along with numerous complex open-source platforms [5]. To harness and implement blockchain in practice, it is necessary to systematically analyze intra- and inter-hospital regional health information workflows while delving deeply into blockchain's technical details, philosophical principles (Chen Chun, 2017), and social application scenarios [6].

3 PROJECT DESIGN

The project combines the characteristics of public and private blockchains, offering advantages such as fast operation speeds, low operational costs (without

the need for incentive mechanisms), and a certain degree of decentralization [7]. Therefore, this project plans to establish a blockchain network jointly developed by medical and administrative institutions. Servers (recommended at least four) will be deployed in this network to achieve distributed (decentralized) trusted storage of key information hash digests from medical institutions. In the event of a medical dispute, hashes can be retrieved and compared (comparing the "original fixed HASH" stored in the blockchain with the "real-time HASH" dynamically generated during dispute resolution), thereby enabling reliable evidence authentication and dispute resolution [8]. The entire business process is supported by the following systems.

A decentralized, tamper-proof storage system is formed using multiple nodes through blockchain technology (based on Fabric 1.1) to store the hash data of key content from various electronic medical records (EMRs) [9]. An EMR Information Collection System will extract key content from the EMRs after data entry and generate a unique hash value for each piece of critical information using HASH256. After assembling the block information, the data will be sent to the blockchain for storage.

The Data Query and Browsing Platform (B/S architecture) allows any individual or third-party institution to register and log in to query the hash information of the required EMRs (comparing the "original fixed HASH" stored on the blockchain with the "real-time HASH" dynamically generated within the hospital). A simple comparison of the two can determine whether the content of the EMR has been tampered with. Untampered records or medical files can serve as the basis for dispute resolution and legal evidence, and tampered fields can be pinpointed (tampering behavior can also contribute to the governance process).

The overall implementation plan of the project is shown in Figure 1. The aim is to establish a closed-loop simulated experimental environment for effective testing, with four blockchain node servers simulating different hospitals and administrative institutions.

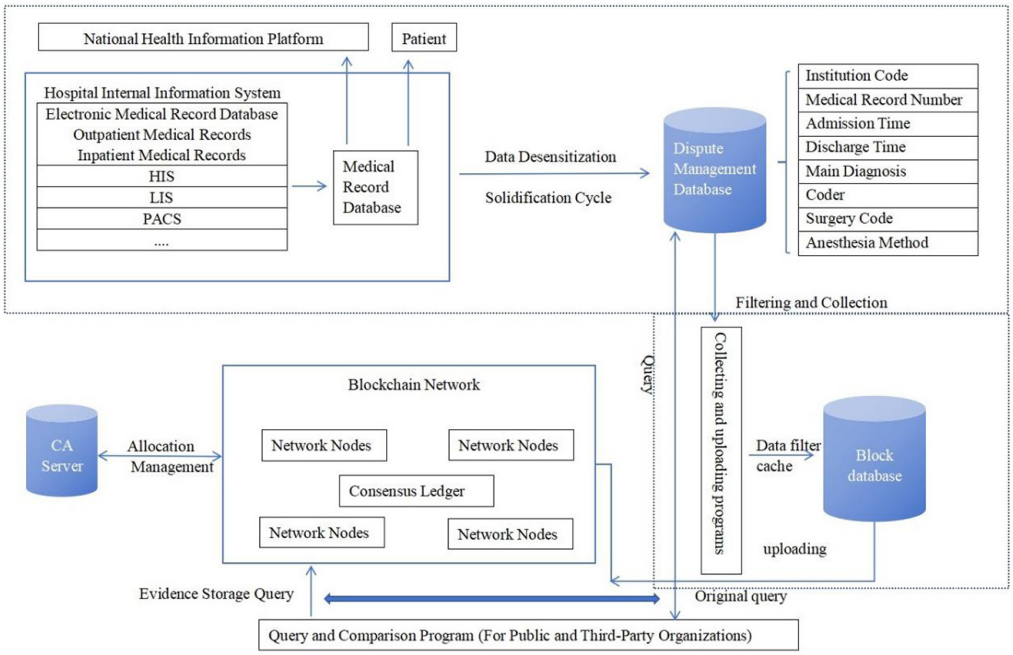

Fig. 1. Project design plan

4 SYSTEM DESIGN

Based on the hospital's internal information system, this study proposes a seamless integrated design for a medical dispute governance system. It focuses on detailing the functionalities and technical macro-implementation methods of each module, as well as the establishment and allocation of fundamental system resources (network, database, and system), as shown in Figure 2.

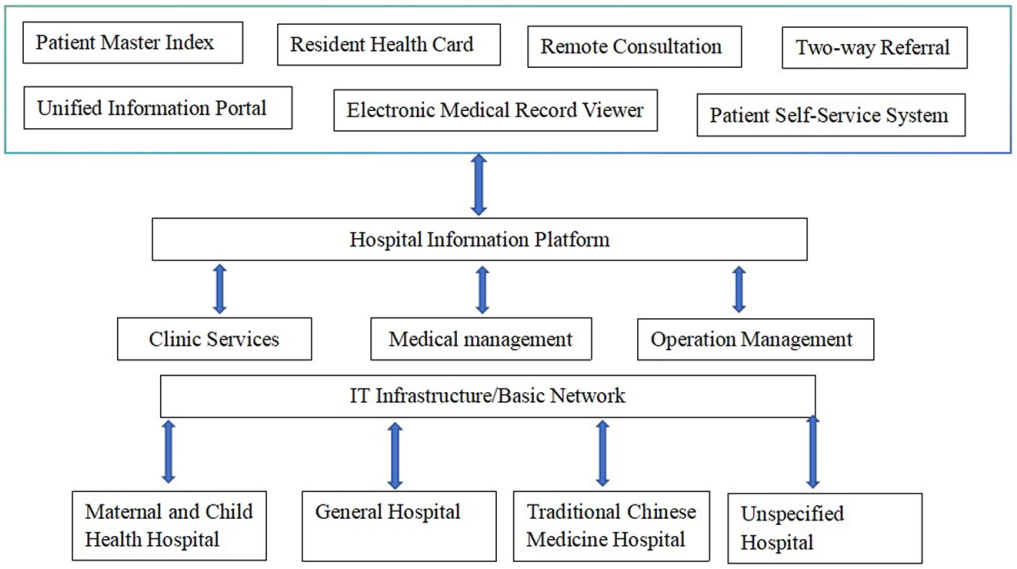

Fig. 2. Framework of hospital informatization construction

This project, based on blockchain technology, aims to establish a blockchain network with multiple nodes to achieve effective governance of medical disputes without altering the existing hospital workflows.

- After completing the EMR/medical record registration, generate hash values for critical information in medical activities (e.g., case number, admission date, diagnosis, ICD coding personnel, surgical codes, anesthesia methods, etc.).
- Upload these hash values to the blockchain to enable distributed storage (decentralization) and consensus-based tamper-proofing (data persistence and immutability).
- Print the blockchain address of these hash values (represented as QR codes of the hash-encrypted data fingerprints/digests on the blockchain, hereinafter referred to as QR codes) onto discharge documents (discharge summaries, diagnostic certificates, or inpatient records). If any modification is made to the critical contents of the EMR, the hash algorithm will generate a completely different hash value, which can be compared with the hash value stored on the blockchain to verify the data's authenticity and validity.
- In the event of a medical dispute (typically involving questioning the authenticity of the EMR), the real-time hash values of the critical contents of the EMR can be compared with the data characteristics stored on the blockchain. This provides the most effective means to verify data validity and consistency, ensuring the credibility and authority of medical data and actions through technical measures.

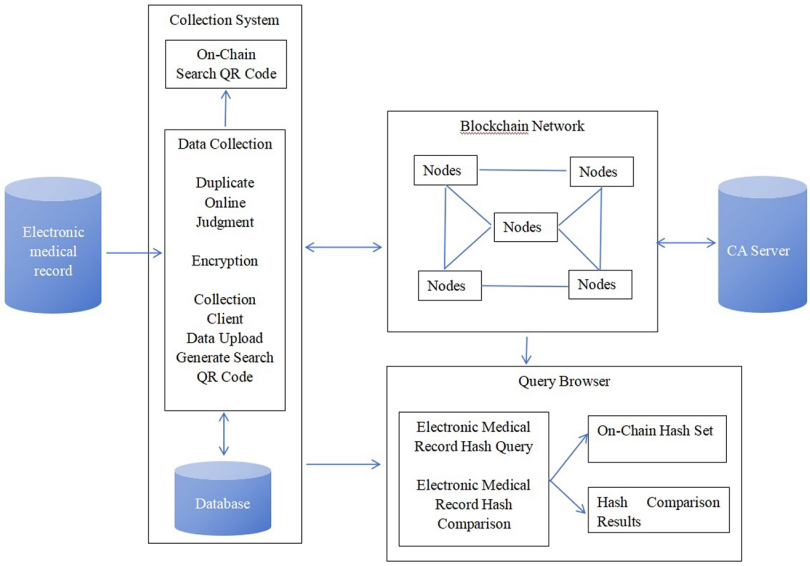

Fig. 3. Design Framework of medical dispute system

- Hospital Side: Approve blockchain nodes for EMRs, allowing them to join the blockchain network after verification. Through the EMR Information Collection System, encrypt the existing EMR information and upload the data to the blockchain. When data verification is required, the Data Query Browser will calculate the hash of locally stored EMR information and compare it with the data on the blockchain. If any changes are detected in the local data, a notification will be issued.
- Other Hospitals or Third-Party Institutions: Submit applications to hospitals to establish blockchain nodes for EMRs and join the blockchain network as member nodes. These nodes directly store, use, or monitor the entire network (including local and non-local EMRs). Each node retains the hash values of key EMR information from all hospitals, allowing it to access the hash values of key EMR information from any hospital at any time. Additionally, these nodes can encrypt key EMR information from their own systems using data encryption programs and upload it to the blockchain.
- Other Relevant Parties: Patients or their families, courts, or other third parties involved in disputes over EMRs can use the Data Query Browser to access the hash values of key EMR information. By comparing the retrieved hash values with the EMRs in the hospital, they can determine whether the content of the hospital's EMRs has been altered.

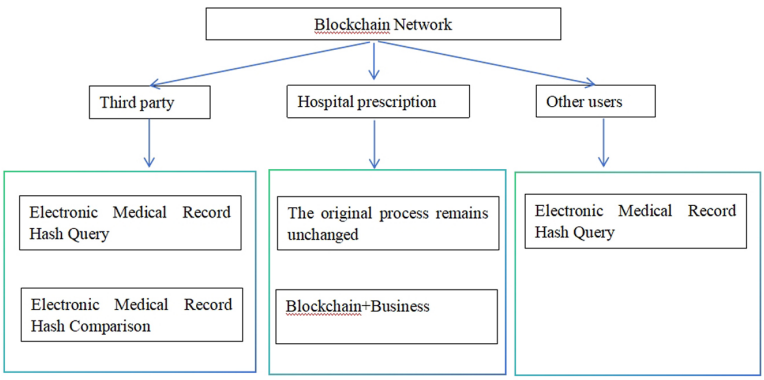

Fig. 4. Functional schematic diagram

5 CONCLUSION

Currently, Internet hospitals, both domestically and internationally, are still in their infancy. Although many hospitals are actively promoting and publicizing their services, they primarily offer basic functions such as appointment scheduling and online consultations, which fall far short of the original vision of Internet hospitals.

This project is the first attempt to apply blockchain to the governance of medical disputes in Internet hospitals, which is a major extension and breakthrough innovation of traditional Internet hospitals in terms of functions.

The methodology adopted in this project simultaneously creates and conveys trust: scientifically establishing a data collection window, pumping hash summaries of key data into the blockchain network, and achieving four primary functions—key data feature extraction, tamper-proof recording, reverse credit verification, and data traceability—while ensuring absolute protection against full-text data leakage [10].

This project employs a multi-centered architectural design, enabling the effective integration of technologies such as public key encryption, digital signatures, and timestamp certificates without requiring credit endorsement from third-party institutions. It stands as the best solution to balance individual data sovereignty with the trust and authority of management institutions.

Funding: This study is supported by the National Social Science Foundation of China (Grant No. 20BGL218).

6 REFERENCES

[1] Z. Ning and Z. Shan, "Blockchain-based personal privacy protection mechanism," *Computer Applications*, vol. 37, no. 10, pp. 2787–2793, 2017.

[2] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017. https://doi.org/10.1016/j.telpol.2017.09.003

[3] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR Mhealth & Uhealth*, vol. 5, no. 7, p. e111, 2017. https://doi.org/10.2196/mhealth.7938

[4] H. Yuki, "Illustrated cryptography techniques," *People's Posts and Telecommunications Publishing*, no. 6, pp. 229–251, 2016.

[5] G. Zyskind, Oz. Nathan, and Alex 'Sandy' Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180–184. https://doi.org/10.1109/SPW.2015.27

[6] H. Xiaoyan, "Blockchain creates trust—interview with academician Chen Chun of the Chinese academy of engineering," *High Technology and Industrialization*, no. 7, pp. 30–33, 2017.

[7] Janssen M. Ubacht, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," Government Information Quarterly, 2017.

[8] Z. Yan, G. Gan, and K. Riad, "BC-PDS: Protecting privacy and self-sovereignty through blockchains for OpenPDS," in *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, San Francisco, CA, USA, 2017, pp. 138–144. https://doi.org/10.1109/SOSE.2017.30

[9] D. Fu and L. Fang, "Blockchain-based trusted computing in social network," in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2016, pp. 19–22. https://doi.org/10.1109/CompComm.2016.7924656

[10] W. Reijers, F. O'Brolcháin, and P. Haynes, "Governance in blockchain technologies & social contract theories," *Ledger*, vol. 1, pp. 134–151, 2016. https://doi.org/10.5195/ledger.2016.62

7 AUTHORS

Xiaofeng Wang is with the College of Management, Shenzhen University, Shenzhen, China (E-mail: freewxf@szu.edu.cn).

Xiaoguang Yue is with the College of Management, Shenzhen University, Shenzhen, China (E-mail: xgyue@whu.edu.cn).

Ahthasham Sajid is with the Multimedia University, Cyberjaya, Malaysia; Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan (E-mail: ahthasham.sajid@riphah.edu.pk).

Noshina Tariq is with the Department of Artificial Intelligence and Data Science, National University of Computer and Emerging Sciences, Islamabad, Pakistan (E-mail: noshina.tariq@isb.nu.edu.pk).