Medical Management Advances 2025 1(1):27-34
https://www.auberpublishing.com/index.php/MMA/index
E-mail: editorialoffice@auberpublishing.com

Review

Research on blockchain-based medical data storage and sharing

Qiuxia Wu*

School of Economics and Management, Nanchang Institute of Technology, Nanchang 330013, China.

Abstract

With its unique advantages of ensuring data integrity, preventing tampering, and enabling traceability, blockchain technology demonstrates immense potential in the field of medical data storage and sharing. Current challenges in medical data sharing include low cross-institutional efficiency and incomplete error correction mechanisms. Through core components such as distributed ledgers and smart contracts, blockchain technology provides new solutions for the secure storage and sharing of medical data. This paper explores the basic principles and related technologies of blockchain, discusses the current status and challenges of medical data storage and sharing, and focuses on the application of blockchain technology in secure storage and sharing systems for medical data. Furthermore, it analyzes future trends in blockchain applications for medical data storage and sharing, aiming to provide references for the further development of medical informatics and to promote the comprehensive improvement of healthcare service efficiency and quality.

Keywords: Blockchain technology; medical data; storage and sharing; privacy

1 Introduction

The rapid development of information technologies such as the industrial internet and big data has driven the digitization, personalization, and informatization of healthcare services, signifying a significant trend for the future. In this transformation process, the problem of "data silos" in the healthcare sector is expected to be gradually resolved, enabling the interconnection of medical data across regions, organizations, and institutions. This, in turn, allows information technology to be more effectively integrated into healthcare services, improving the utilization of medical data and the integration of healthcare resources.

The General Office of the State Council of China issued the "Opinions on Promoting the Development of Internet+ Healthcare," emphasizing the importance of strengthening information resource allocation and promoting the deep integration and sharing of information technology in the health and medical field. However, healthcare institutions in China still face significant challenges in data sharing and utilization, particularly in terms of cross-institutional medical data sharing, which remains inefficient, and error correction and fault tolerance mechanisms that are still underdeveloped [1].

Among the various available information technologies, blockchain is recognized as a critical breakthrough for integrating with healthcare informatics due to its advantages in ensuring data integrity, preventing tampering, enabling traceability, and scalability. Blockchain has the potential to address the shortcomings of healthcare institutions in terms of informatization, facilitating precise sharing and effective utilization of medical data across regions, organizations, and institutions.

However, blockchain's transparency and decentralized features could also pose potential risks to the security and privacy of medical data, potentially exacerbating data leakage risks. Therefore, a pressing challenge in the healthcare informatics domain is how to maximize data sharing and utilization while ensuring data security, thereby enhancing the efficiency of healthcare services.

***Correspondence**
Qiuxia Wu
School of Economics and Management, Nanchang Institute of Technology, Nanchang 330013, China.
E-mail: 1305215276@qq.com

2 Overview of Blockchain Technology

Blockchain is an advanced distributed database architecture, with its core components comprising blocks (used to record transaction information and other data units), chain structures (a sequence of blocks linked in chronological order to form a tamper-proof record), distributed ledger technology (which enables data storage across multiple nodes), and a decentralized design concept (eliminating a single controlling center and instead relying on the collaborative maintenance of all network members) [2].

This architecture employs a chain-based data structure combined with encryption methods such as hash algorithms and public-key cryptography to enhance data protection. It also relies on consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) to ensure that all nodes in the network agree on the state of the data, thereby guaranteeing data accuracy and integrity.

The main characteristics of blockchain are summarized as follows:

2.1 Decentralization

Blockchain employs a fully distributed data storage solution without central nodes. All participating nodes hold a complete and consistent set of block data, ensuring openness, transparency, high security, and trustworthiness. It also achieves data immutability.

2.2 Immutability

Each transaction record on the blockchain is assigned a unique hash value. To modify a single record, theoretically, the hash values of that block and all subsequent blocks would need to be altered simultaneously. This is highly impractical in reality, as it would require control over most of the blocks in the network. Thus, any attempt to modify a single block would be deemed invalid, ensuring data immutability.

2.3 Trustless

The operation of blockchain systems relies entirely on transparent rules and algorithms, eliminating the need for traditional trust relationships between nodes. Within the framework of the system, all nodes follow the same rules, making fraudulent behavior difficult and establishing a new trustless system based on algorithms [3].

2.4 Anonymity

Interactions between blockchain nodes depend on predefined algorithmic logic rather than identity trust between the nodes. Consequently, during transactions, parties can build trust without disclosing personal identities, offering anonymity protection for both parties involved.

3 Fundamental Principles and Related Technologies of Blockchain

3.1 Fundamental Principles of Blockchain

Blockchain is a database system that integrates features of sharing, decentralization, and distribution. It cleverly combines essential computational technologies such as timestamping, Merkle tree architecture, and consensus algorithms, while leveraging cryptographic principles like hash functions, asymmetric encryption, and digital signatures to create an innovative distributed infrastructure. In this architecture, nodes in the blockchain network consolidate information to be recorded into blocks, which are added to the chain through competitive consensus mechanisms. Each newly created block embeds the hash value of the previous block, creating a sequentially extended chain structure.

Blockchain manifests in three core forms: (1) Public Blockchain: A fully open blockchain platform that allows unrestricted participation by anyone. It achieves complete decentralization, enabling users to create and add blocks without prior authorization [4]. (2) Private Blockchain: Designed for specific organizations, this type of blockchain restricts participation to authorized nodes, resulting in limited decentralization. (3) Consortium Blockchain: Positioned between public and private blockchains, consortium blockchains enable limited decentralization. In healthcare applications, the consortium model is more suitable as it incorporates relevant medical institutions and regulatory bodies as nodes within the blockchain network while maintaining appropriate access thresholds.

3.2 Related Technologies in Blockchain

3.2.1 Distributed Ledger Technology

Distributed ledger technology (DLT) is a core component of blockchain. It ensures data integrity and security through the replication and distributed storage of data across multiple nodes in the network. In medical data sharing scenarios, DLT employs advanced encryption algorithms, such as SHA-256, to generate a unique hash identifier for every transaction, guaranteeing im-

mutability. Once data is written into a block, it cannot be altered by a single or a small group of nodes.

3.2.2 Asymmetric Encryption Algorithms

In 1985, Koblitz and Miller independently proposed the theory of elliptic curve cryptography (ECC), which marked a major breakthrough in asymmetric key encryption [5]. ECC functions, combined with hash algorithms, generate a pair of interrelated public and private keys. These keys are logically connected but cannot be deduced from one another.In this system, the public keys are used for data encryption, while the private keys are used exclusively for data decryption.

Hash algorithms play a crucial role in verifying data integrity, ensuring that data has not been tampered with during transmission. In a blockchain network, public keys are accessible to all nodes, while private keys are securely held by individual users. This design ensures high levels of security for data transmission and reliable authentication of the sender's identity.

3.2.3 Consensus Mechanisms

In the context of healthcare data management, consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) not only provide a tamper-proof security barrier for the data but also implement a decentralized process for transaction validation and record-keeping through algorithmic logic, thus avoiding direct intervention by central authorities. Specifically, in the PoW algorithm, nodes must solve complex computational problems to verify the authenticity of transactions. This process relies on the collaborative efforts of all nodes in the network, collectively ensuring the consistency and security of transaction data. Healthcare data sharing platforms that use the PoW mechanism can effectively control the risk of malicious transactions at a very low level (below 0.001%) [6]. Moreover, this algorithm promotes energy efficiency while encouraging broader network participation, thereby enhancing the network's decentralization and overall security. As a result, the application of consensus algorithms continues to expand its boundaries and gain wider adoption.

3.2.4 Smart Contracts

Smart contracts are automated execution programs deployed on blockchain networks. They trigger and execute contract terms automatically when preset conditions are met, without the need for third-party intervention. While traditional digital contracts can achieve automated execution, they are often vulnerable to tampering and attacks. Blockchain technology provides a secure environment for smart contracts, addressing trust issues during execution.

By leveraging blockchain's distributed storage:

• Patients can securely access and authorize their medical data without intermediaries using smart contract algorithms.

• Blockchain's immutability ensures the authenticity of contract terms.

• Decentralized storage enables all network nodes to back up data, collectively verifying and supervising contract execution.

Ethereum, as the most widely used and mature blockchain platform for smart contracts, continues to drive innovation and development in this field.

4 Current State and Challenges of Medical Data Storage and Sharing

4.1 Current State of Medical Data Storage and Sharing

Medical data storage and sharing are critical components of the digital transformation in the healthcare industry. To date, China has successfully established a range of hierarchical and categorized medical health data platforms tailored to different application needs. These platforms are built upon a system of healthcare information standards, which have been instrumental in advancing the informatization and digitization of medical and health data sharing. With continuous improvements in the health information standards management system, these platforms have significantly enhanced the interconnectivity and interoperability of medical and health data.

In terms of infrastructure, China has laid the groundwork for a foundational environment supporting the sharing of health and medical data. Stakeholders, including government agencies, medical institutions, research institutes, and various health data platforms, have demonstrated tremendous potential and vitality in data sharing activities. Through the construction of data centers, data warehouses, and cloud computing platforms, these stakeholders provide robust support for the storage, processing, and analysis of medical data [7].

Medical institutions, as primary sources of medical data, possess large volumes of patient health information. This data encompasses a wide range of content, including patients' basic information, medical records, diagnostic results, treatment plans, and imaging data, serving as a crucial foundation for medical deci-

sion-making, research, and treatment. Additionally, as medical technologies evolve and equipment advances, the volume and complexity of medical data continue to grow, enriching resources for data storage and sharing.

Moreover, the rapid development of "Internet+ Healthcare" has expanded the sources of health data. Beyond the data held by medical institutions, resources such as residents' electronic health records, electronic medical records, and electronic prescriptions serve as core institutional databases. Additionally, databases from third-party entities, such as public health agencies and diagnostic centers, contribute valuable resources for medical data storage and sharing. Integrating and sharing this data can not only improve the efficiency and quality of medical services but also provide more comprehensive and accurate support for medical research and treatment.

4.2 Challenges in Medical Data Storage and Sharing

4.2.1 Technical Challenges

(1) Data Format and Standards Diversity: Medical data formats and standards vary significantly, not only between institutions and systems but also within different departments of the same institution. This diversity complicates the integration and analysis of shared data. The lack of unified data standards and interfaces leads to inefficiencies and complexities in data exchange [8].

(2) Massive Data Growth: The rapid growth of medical data, especially imaging data and genomic sequencing information, places unprecedented demands on storage capacity and processing capabilities. Efficiently storing, managing, and analyzing these massive datasets remains a pressing technical challenge.

(3) Data Accuracy and Completeness: Ensuring data accuracy and completeness is vital for clinical decision-making. Errors during data entry, system upgrades that cause data loss or conversion issues, and incomplete patient histories can severely undermine data quality and lead to diagnostic mistakes.

(4) Data Security Risks: Medical data contains sensitive personal information. Any data breach poses significant threats to individuals' privacy and safety, making data protection a critical concern.

4.2.2 Legal and Ethical Challenges

(1) Diverse Privacy Regulations: Different countries and regions have varying laws for personal data protection, such as the European Union's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA). These discrepancies make cross-border data sharing particularly complex, requiring strict compliance with multiple legal frameworks.

(2) Ownership Disputes: The ownership of medical data is a contentious issue, with patients, medical institutions, and research organizations often having conflicting claims over data usage rights. Balancing these interests to ensure fair and reasonable data utilization is a significant legal and ethical challenge [9].

(3) Informed Consent and Ethical Use: Medical data is often shared for purposes such as research and education. Ensuring that all data usage undergoes rigorous ethical review and obtains informed consent from patients is central to safeguarding patients' rights and maintaining ethical standards in medical data usage.

4.2.3 Standardization and Interoperability Challenges

(1) Although international medical data standards like HL7 and DICOM exist, their adoption and compatibility remain limited in practice. The lack of unified data standards reduces the efficiency of data sharing, hindering the effective use of medical data on a larger scale.

(2) Poor interoperability between different medical information systems leads to issues such as mismatched formats and information loss during data exchange. This significantly hampers data integration and restricts the depth and breadth of data sharing.

4.2.4 Trust and Collaboration Challenges

(1) Concerns over data security and privacy often lead to a lack of trust between medical institutions, reducing their willingness to share data.

(2) Effective data sharing frequently requires coordination across multiple sectors, such as health, technology, and education. However, unclear responsibilities and uneven benefit distribution among these sectors create barriers to collaboration, further complicating data sharing efforts.

5 Applications of Blockchain Technology in Secure Medical Data Storage and Sharing Systems

5.1 Decentralized Data Storage

One key application of blockchain technology in secure medical data sharing is decentralized data storage. By distributing medical data across multiple nodes in a network, blockchain enhances data immutability and

reliability. Each node holds a complete copy of the data, and any updates require verification through consensus mechanisms among the majority of nodes to ensure consistency and integrity.

Compared to traditional centralized storage systems, decentralized storage is more resistant to single points of failure, improving system stability [10]. Additionally, since attackers must compromise multiple nodes simultaneously to affect the data, this storage method greatly reduces the risk of data breaches. It not only strengthens data security during storage and transmission but also enhances accessibility and the utility of the data.

5.2 Data Access Control and Privacy Protection

Strengthening access control and ensuring privacy protection are critical in building secure medical data sharing systems. Blockchain's smart contract capabilities provide a robust foundation for implementing complex and precise access control strategies. These strategies ensure that only authorized users can access specific medical information.

Smart contracts' autonomous execution eliminates the need for centralized management, significantly enhancing data security and privacy. Blockchain has demonstrated its ability to minimize unauthorized data access and reduce the risk of data breaches. Furthermore, blockchain can generate immutable audit logs for every data access event, increasing system traceability and transparency. This helps monitor and manage access behaviors, enhancing overall security and patient trust in privacy protection [11].

5.3 Optimizing Data Sharing Mechanisms and Enhancing Cross-System Interoperability

Blockchain provides a new pathway for inter-institutional data sharing that ensures data integrity and security. Its decentralized architecture allows the system to operate smoothly without a central server, ensuring that all participating nodes verify and maintain data consistency.

In real-world scenarios, blockchain has been successfully integrated into emergency response workflows, improving the efficiency of critical information sharing and increasing the success rate of emergency treatments [12]. Furthermore, the blockchain-powered data sharing framework can seamlessly connect disparate information systems with varying technical architectures, significantly enhancing interoperability between service providers. This improves resource utilization efficiency and delivers a smoother, more convenient service experience for users.

6 Practical Applications of Blockchain in Medical Data Storage and Sharing

The following are examples of how blockchain technology is being applied in medical data storage and sharing, showcasing its effectiveness in the healthcare domain:

6.1 Electronic Medical Records (EMRs)

Using blockchain technology to store medical records not only protects patient privacy but also ensures that healthcare providers can access and update medical records in real-time. This significantly enhances the accuracy of medical decisions and response times. For example, the Medical Blockchain BaaS Platform developed by Beijing University of Posts and Telecommunications has demonstrated top-tier capabilities in areas such as strengthening data security and privacy, promoting the sharing and traceability of medical information, optimizing medical service workflows, and improving insurance claim settlements and cost management. This platform has earned trust and praise from multiple hospitals, providing substantial value-added benefits.

6.2 Drug Traceability and Anti-Counterfeiting

By recording drug information on the blockchain, it becomes possible to trace and verify the entire lifecycle of a drug, from production to distribution. Consumers can easily access detailed production and supply chain information by scanning a QR code on the product. This measure effectively curbs the circulation of counterfeit drugs and greatly improves the quality and safety of pharmaceuticals. Some pharmaceutical companies have already adopted blockchain technology for drug traceability and anti-counterfeiting, ensuring the safety and efficacy of medications used by patients.

6.3 Medical Equipment Management

Blockchain technology also holds great promise in managing and maintaining medical equipment. It can provide detailed records of the origins, distribution paths, and usage of medical devices, offering robust assurances of their quality and safety. Additionally, by recording the maintenance history of equipment, blockchain enables

healthcare institutions to manage and maintain devices more efficiently. For instance, some medical institutions are already leveraging blockchain technology to track and manage medical equipment, improving utilization rates and ensuring safety during medical procedures [13].

6.4 Research Data Sharing Platforms

Blockchain provides strong technical support for the creation of decentralized research data-sharing platforms. By deploying smart contracts, these platforms can ensure the security and credibility of research data, fostering closer collaboration and data exchange among research institutions. Some organizations have already begun using blockchain to build such platforms, enabling cross-institutional data sharing and collaborative research, injecting new momentum into the advancement of medical research.

7 Future Trends of Blockchain in Medical Data Storage and Sharing

7.1 Technological Innovation

Blockchain technology will undergo significant improvements and optimizations. Core components, such as consensus mechanisms and encryption algorithms, will continue to be upgraded to enhance system scalability and overall performance. Innovations in consensus mechanisms will reduce transaction confirmation times and increase network throughput, enabling blockchain to handle large-scale data processing challenges. Advances in encryption algorithms will further strengthen data security, ensuring absolute privacy during data transmission and storage. Moreover, blockchain technology will no longer develop in isolation but will integrate deeply with emerging technologies like artificial intelligence (AI) and the Internet of Things (IoT), driving the digital and intelligent transformation of the healthcare sector. This cross-disciplinary collaboration will create new application scenarios and solutions, such as AI-based smart contract auditing and secure IoT device integration, bringing unprecedented changes and opportunities to the industry [14].

7.2 Expanding Applications

As blockchain technology matures, its applications in healthcare will continue to expand, becoming deeply integrated into various medical scenarios and workflows. In telemedicine, blockchain will ensure the integrity and privacy of patient data, enabling secure and efficient remote consultations. In supply chain management for healthcare, blockchain will allow full traceability of drugs and medical devices, effectively combating counterfeiting and improving transparency and safety. Additionally, blockchain will seamlessly integrate with healthcare IT systems, such as electronic medical records (EMR) and medical imaging storage and transmission systems, facilitating efficient data exchange and streamlined workflows. These cross-system collaborations will lay a solid foundation for the comprehensive digitalization and intelligent transformation of healthcare, improving service quality and operational efficiency.

7.3 Policy and Regulatory Improvements

The widespread application of blockchain in medical data storage and sharing has highlighted both its transformative potential and accompanying challenges, prompting governments and regulatory bodies to strengthen oversight and establish clear guidelines. In the future, we may see the introduction of specialized policies and regulations aimed at blockchain applications in healthcare. These measures will create a lawful and compliant environment for the technology's use while ensuring robust protection of patient privacy and data security [15].

Specifically, such regulations may address the entire lifecycle of data storage, transmission, use, and sharing, outlining precise requirements and operational standards. Blockchain technology providers and healthcare institutions will likely face stringent accreditation criteria to ensure their competence in areas like technical performance, data security, and privacy protection. Additionally, regulations will clarify liability in cases of data breaches or misuse, enabling swift identification of responsible parties and effective remediation. Governments will also promote the establishment of standardized frameworks for blockchain applications in healthcare, covering technical architecture, data formats, and interface protocols to ensure interoperability between different platforms and facilitate data exchange.

7.4 Protecting Patient Rights

Protecting patient rights will become a core focus of blockchain applications in medical data storage and sharing. Governments and regulatory agencies will prioritize the safeguarding of patient privacy and data security through enhanced oversight and a comprehensive

legal framework.

To achieve this, stricter data protection and privacy regulations will be implemented, specifying detailed requirements and responsibilities for data collection, storage, use, and sharing. Regulators will increase scrutiny of healthcare institutions and blockchain technology providers through routine and random inspections to ensure compliance with legal and privacy standards. Furthermore, mechanisms to protect patient rights will be developed, including complaint channels and dispute resolution systems, ensuring patients can quickly receive assistance and support in cases of data breaches or misuse [16].

7.5 International Cooperation and Exchange

The rapid global development and application of blockchain in medical data storage and sharing are driving a profound industry transformation. Against this backdrop, international collaboration and exchange will become increasingly important, serving as critical drivers of blockchain adoption.

In the future, more international conferences, high-level forums, and diverse exchange activities will focus on blockchain applications in healthcare. These events will provide platforms for showcasing technological achievements and exchanging innovative ideas, facilitating global technological collaboration. Through these interactions, countries can share valuable experiences and lessons learned from blockchain implementation. Whether analyzing successful case studies or addressing challenges, these insights will offer meaningful references for all parties. Additionally, international cooperation in data protection and privacy regulations will be crucial. As cross-border medical data flows become more frequent, ensuring legal and compliant data transfer and use will be a pressing challenge. Strengthening international coordination and establishing globally recognized standards for data protection and privacy will provide clear legal guidance and security for cross-border medical data exchange.

8 Conclusion

This article explores the application of blockchain technology in medical data storage and sharing, highlighting its potential to address data silos and enhance data security and reliability. As blockchain continues to develop and mature, its applications in healthcare are poised to expand significantly. In the future, blockchain will integrate deeply with other emerging technologies, such as artificial intelligence and IoT, driving the digital and intelligent transformation of the healthcare sector. At the same time, governments and regulatory bodies must strengthen oversight and establish clear guidelines to ensure robust protection of patient privacy and data security. With these measures in place, blockchain is expected to play an even greater role in improving healthcare service efficiency and quality, advancing medical research, and supporting innovative treatments.

Acknowledgments

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

The author contributed solely to the article.

Ethics Approval and Consent to Participate

No ethical approval was required for this review article.

Funding

This research received no external funding.

Availability of Data and Materials

TThe data presented in this study are available on request from the corresponding author.

Supplementary Materials

Not applicable.

References

[1] Xue TF, Fu QC, Wang C, *et al.* A Medical Data Sharing Model via Blockchain [J]. *Acta Automatica Sinica*, 2017, 43(9):1555-1562.

[2] Liu W, Peng YF, Tian Z, *et al.* A survey on Medical Information Privacy Protection Based on Blockchain [J]. *Journal of Zhengzhou University(Natural Science Edition)*, 2021, 53(2):1-18.

[3] Zhang C, Li Q, Chen ZH, *et al.* Medical Chain: Alliance Medical Blockchain System [J]. *Acta Automatica Sinica*, 2019, 45(8):1495-1510.

[4] Zhou Z, Chen L, Zhao Y, *et al.* Retrieval Integrity Verification and Multi-System Data Interoperability Mechanism of a Blockchain Oracle for Smart Healthcare with Internet of Things (IoT) Integration [J]. *Sensors*, 2024,

24(23):7487-7487.
[5] Huang JF and Liu J. Survey on Blockchain Research [J]. *Journal of Beijing University of Posts and Telecommunications*, 2018, 41(2):1-8.
[6] Luo WJ, Wen SL and Cheng Y. Blockchain-based electronic health record sharing scheme[J]. *Journal of Computer Applications*, 2020, 40(1):157-161.
[7] Liu YS, Xia Q, Li Z, *et al.* Research on secure data sharing system based on blockchain [J]. *Big Data Research*, 2020, 6(5):92-105.
[8] Zhu JM, Zhang QN and Gao S. Research Progress of Blockchain Key Technologies and Their Application [J]. *Journal of Taiyuan University of Technology*, 2020, 51(3):321-330.
[9] Punitha S and Preetha KS. A novel integration of Web 3.0 with hybrid chaotic-hippo-optimized Blockchain framework for healthcare 4.0 [J]. *Results in Engineering*, 2024, 24103528-103528.
[10] Ma L and Chu DL. Research on application technology of blockchain in medical field [J]. *Intelligent Computer and Applications*, 2019, 9(4):286-287.
[11] Mishra KD and Mehra SP. Diabetic Chain: a novel blockchain approach for patient-centric diabetic data management [J]. *The Journal of Supercomputing*, 2024, 81(1):166-166.
[12] OUYANG LW, Yuan Y, Zheng XH, *et al.* A novel blockchain-based surveillance and early-warning technology for infectious diseases[J]. *Chinese Journal of Intelligent Science and Technology*, 2020, 2(2):135-143.
[13] Zhang L, Zheng ZY and Yuan Y. A Controllable Sharing Model for Electronic Health Records Based on Blockchain [J]. *Acta Automatica Sinica*, 2021, 47(9):2143-2153.
[14] Zhou S, Fan J, Yuan K, *et al.* Efficient privacy-preserving online medical pre-diagnosis based on blockchain [J]. *The Journal of Supercomputing*, 2024, 81(1):111-111.
[15] Wang ML. Discussion on the Application of Blockchain Technology in the Field of Medical Health [J]. *Chinese Journal of Medicinal Guide*, 2021, 23(1):68-73.
[16] Zhang LH, Lan F, Jiang PP, *et al.* A secure medical record storage and sharing scheme based on dual-blockchain [J]. *Computer Engineering & Science*, 2019, 41(9):1581-1587.