Scholar Publishing Group
International Journal of Health and Pharmaceutical Medicine
https://doi.org/10.38007/IJHPM.2025.050104
ISSN 2789-8393 Vol. 5, Issue 1: 32-42

Research on the Application of Blockchain Technology in the Security of Digital Healthcare Data

Thanh-Huyen Truong

DIAB HEALTHCARE,Ho Chi Minh City,Vietnam,700000

lunababygiasi@gmail.com

Keywords: Blockchain; Electronic Health Records; Medical Data Interoperability; Privacy Protection Mechanism; Consortium Blockchain

Abstract: As digital healthcare continues to evolve, there is a growing concern about the secure sharing and privacy protection of healthcare data. Nowadays, although electronic health records (EHR) have become the main way for healthcare organisations to manage their data, most hospitals and clinics are still using their own centralised systems - in this way, not only is the data like 'an island' unconnected to each other, making it difficult for different organisations to collaborate with each other, but such systems are also vulnerable to hacking, leading to the leakage of patient information and compromising privacy rights. This not only makes the data like 'islands' that are not connected to each other, making it difficult for different organisations to collaborate with each other, but also makes such systems vulnerable to hacking, leading to the leakage of patient information and compromising everyone's privacy. Because of this, this paper explores the potential of blockchain technology in building a trustworthy medical data sharing mechanism, and also proposes a solution that protects privacy without affecting the operational effectiveness of the system. In this study, for the characteristics of medical scenarios, the coalition chain with access control is chosen as the underlying architecture, and the traditional consensus mechanism is improved directionally to design a hybrid consensus algorithm that fits the needs of the medical industry. This algorithm combines the proof-of-interest and probabilistic verification mechanisms, which can fairly distribute the node bookkeeping rights, significantly improve the system processing speed and enhance the anti-attack ability. For the possible node monopoly and voting imbalance in the consensus election, we introduce the multi-source random sequence generation method and ring signature technology, which makes the system more secure and stable in the complex network environment, and the election more transparent. Finally, considering the sensitivity of medical data, we have specially designed a dual protection mechanism of 'layered processing' and 'cryptographic hashing'. Specifically, the patient's identity information and medical treatment data are stored separately, and also use SHA-256, an irreversible algorithm, to generate a unique identity information 'identity fingerprint'. In this way, even if part of the data is accidentally leaked, it is difficult to restore the complete privacy information, thus making the system more secure in protecting the anonymity of the user and preventing the leakage of information by association. Comprehensive evaluation results demonstrate that the proposed blockchain-based medical data-sharing model achieves strong performance in efficiency, security, and privacy protection, thereby providing technical support for compliant, efficient, and trustworthy cross-institutional data

collaboration.

1. Introduction

The rapid advancement of medical informatics is reshaping traditional healthcare service models. Electronic Health Records (EHRs) are gradually replacing paper-based medical records, becoming a crucial data foundation for clinical treatment, medical insurance, scientific research, and public health management. However, the contradiction between the distributed generation of medical data and its centralized management has become increasingly prominent. Most medical institutions develop independent information systems that lack unified standards and interoperability mechanisms, leading to low efficiency in cross-institutional data sharing and the formation of typical data silos. In addition, although the cloud platform makes the storage and transmission of medical data faster and more convenient, it uses a centralised architecture, which still has obvious shortcomings in terms of privacy protection, security checks and system risk resistance.

Healthcare data breaches have been a frequent occurrence in recent years, exposing the weaknesses of traditional information systems in terms of identity confidentiality, access rights management, and data tracking and tracing. Statistics from a number of countries show that when medical data is compromised, the cost per unit of data lost is much higher than in other industries. Moreover, these data contain particularly sensitive information such as patients' identities, diagnostic results, past medical history, etc., which, if leaked, will bring irreversible and serious consequences to both individuals and healthcare organisations. This phenomenon has led people to think deeply about how medical data can be shared credibly while protecting privacy. Some existing research attempts to improve data security through encryption, access control, and cloud-based privilege management, but most of the solutions still rely on the assumption of ‘centralised and trusted organisations’, which makes it difficult to truly achieve equal and verifiable collaboration between multiple organisations. In recent years, blockchain technology has shown great potential for application in finance, justice, and IoT because of its decentralised, tamper-proof, and traceable features, and it has also brought new possibilities for the sharing of medical privacy data. However, if the existing blockchain architecture is directly transferred to the medical scenario, it will still encounter quite a few problems, such as the transaction processing speed is not fast enough, the consensus mechanism may be manipulated, and the data is prone to privacy leakage once it is uploaded to the chain.

In order to solve those previously mentioned difficulties, this paper designs a new blockchain medical data sharing approach based on the actual needs of medical scenarios. This approach can ensure that the system operates efficiently and protects the data privacy, as well as strictly controls the data access rights. It optimises the consensus algorithm and node management method on the basis of the federated chain architecture, and also adopts privacy protection strategies such as encrypted hash processing of identity information, sliced data storage, and off-chain preservation of some data. In this way, different healthcare organisations can safely cooperate with each other even if the trust level is very low, providing a solution that can be realised with technology and is compatible with the existing system for the trusted circulation of data in digital healthcare.

2. Related Research

The security and privacy protection of medical data are core challenges in the development of

digital healthcare and have become a hot topic of interdisciplinary research. Tertulino R[1], through a systematic literature review, pointed out that although electronic health record systems are gradually gaining popularity, ensuring data privacy without sacrificing system performance and interoperability remains a major dilemma. This conclusion resonates with the problems identified in the introduction, namely data silos and the risks of privacy leakage. Szarfman A[2] further reinforced this perspective and proposed a direction for fundamental reform, namely, the establishment of systems that incorporate standardized data formats, unified patient identifiers, and auditable infrastructures to break down data barriers and lay the foundation for secure and efficient data exchange.

At the technical application level, Yang X’s[4] work demonstrated the potential of artificial intelligence in unlocking the value of unstructured medical data. His large-scale clinical language models significantly improved the performance of natural language processing tasks in healthcare. However, as reviewed by Sivan R[5], when such computationally intensive tasks are deployed on cloud platforms, scalability and collaborative capabilities are gained at the cost of heightened security and privacy challenges, which necessitate careful evaluation and design of protection mechanisms. Together, these studies outline the future landscape of healthcare IT: while data applications increasingly depend on cloud-based computational power, their implementation must be grounded in a robust data security framework.

In terms of blockchain integration and empowerment, existing research has already begun to explore its potential in addressing these challenges. Tertulino R’s review revealed that blockchain, due to its immutability and traceability, has been widely investigated as a solution for safeguarding EHR data privacy. From a broader perspective, Ressi D[8] suggested that artificial intelligence can optimize blockchain technology itself—enhancing its efficiency, security, and reliability in key aspects such as consensus mechanisms, smart contracts, and data privacy. This theoretical foundation supports the possibility of deeply customizing blockchain through the integration of artificial intelligence and other technologies to better fit healthcare scenarios[6].

In summary, existing studies have clearly shown the inherent limitations of traditional centralized healthcare data management systems[7], while blockchain technology has been identified as a promising solution for constructing trusted medical data infrastructures[8]. However, most current research treats blockchain as a ready-made tool, with little effort devoted to deeply customizing or optimizing its underlying mechanisms to address the complex demands of the healthcare sector, such as high concurrency, strong privacy protection[9], and cross-institutional collaboration. This study fills this research gap by designing a blockchain solution tailored to healthcare scenarios that innovates on both consensus mechanisms and privacy-preserving architectures[10].

3. Technical Support of Blockchain for Medical Data Security

3.1 Decentralized Consensus Mechanism and System Robustness

In the security framework of medical data, the consensus mechanism serves as the core process for maintaining the stable operation of the blockchain. Since medical information systems must remain online over the long term and assume strict auditing responsibilities, consensus protocols are required not only to guarantee consistency of on-chain states but also to balance performance, scalability, and fault tolerance. Under conditions where the number of nodes is limited, institutional heterogeneity is significant, and regulatory requirements are stringent, healthcare scenarios place comprehensive demands on consensus mechanisms, including low resource consumption, predictable latency, and reasonable fault-tolerance thresholds.

To characterize consensus performance more intuitively, the overall system latency can be modeled, as shown in formula 1:

$$L_{total} = T_{prop} + \frac{f}{N-f} \cdot T_{vote} + T_{verify} \qquad \text{formula 1}$$

Here, T_{prop} denotes the transaction propagation time across the network, T_{vote} represents the average time required for nodes to complete voting and confirmation, and T_{verify} is the time for verifying a new block. N refers to the total number of nodes, and f indicates the number of tolerable faulty or malicious nodes. The formula shows that when the proportion of malicious nodes approaches the fault-tolerance threshold, system latency increases significantly. Therefore, in the parameter design of consortium blockchains, it is necessary to strike a balance among network scale, fault tolerance, and system latency.

To further validate the performance advantages of the improved consensus mechanism, this study conducts a comparative analysis of the average block generation time under different mechanisms. The results, as illustrated in Figure 1, demonstrate that the proposed hybrid consensus not only maintains low latency but also provides stronger stability, making it better suited to the real-time requirements of healthcare applications.

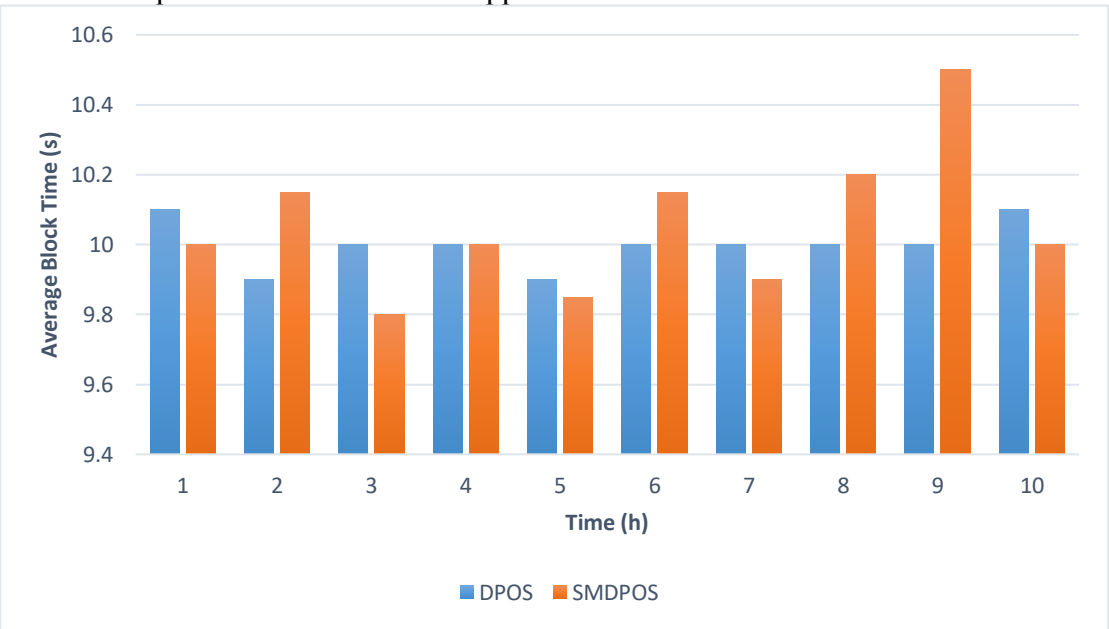

Figure 1: Comparison of average block generation time under different blockchain consensus mechanisms in healthcare scenarios

Compared with open public blockchains, medical data sharing is more suitable for operation under a consortium blockchain architecture. In this framework, medical institutions, regulatory authorities, and service providers jointly participate, and all nodes are certified legal entities. This design avoids the high costs associated with anonymous competition while overcoming the vulnerabilities of traditional centralized models. On this basis, an improved Delegated Proof-of-Stake (DPoS) mechanism is introduced. Through probabilistic elections and representative rotation, ledger rights are fairly allocated, ensuring decentralization and scalability while also achieving energy efficiency. Unlike traditional mechanisms, medical consortium blockchains place greater emphasis on robustness and continuous operation. Accordingly, the number of representative nodes, rotation cycles, and penalty mechanisms are designed with stronger attention to block generation stability and rapid system recovery.In the election session, in order to avoid bribery, lack of voting motivation and weak centralisation problems caused by node solidification,

the study proposes a design that combines random number generation and ring-signature anonymous voting. The former collaboratively generates unpredictable sequences for determining the block order and candidate list; the latter approach ensures verifiable voting results and hides the voter's identity, reducing the risk of benefit transfer and retaliatory manipulation. After the improvement, the security and stability of the system in the face of malicious nodes are significantly enhanced.

The robustness of the decentralised consensus mechanism is mainly reflected in several aspects: multiple nodes recording data together can effectively avoid the failure of a single node leading to the paralysis of the whole system, the improved mechanism improves the resistance to malicious and collusive behaviours by randomly replacing the participating nodes and anonymous voting, and supports normal operation of the system when some nodes are unavailable, and the coalition chain is no longer restricted by the high energy consumption of workload proof and can guarantee security while meeting the real-time requirements for data processing speed in medical scenarios. The coalition chain is no longer restricted by the problem of high energy consumption of proof of workload and can meet the real-time requirements of medical scenarios on data processing speed while guaranteeing security, and the consensus process on the chain, which cannot be modified and can be verified, also provides a transparent and reliable basis for auditing and accountability.

In the engineering landing process, the consensus process can be constructed as a closed loop, node identity unified management by the regulatory body, medical institutions participate in the voting to form a candidate collection according to the cycle, collaborative random number to determine the witness rotation and the order of the block, the system in the event of double signatures or long time offline immediately triggered penalties and record the evidence, and based on the volume of business and quality of service issued incentives. The mechanism achieves decentralised governance while taking into account centralised compliance, and maintains the long-term stable operation of the healthcare data platform under the premise of ensuring security.

When facing the data security requirements of digital healthcare scenarios, the decentralised consensus mechanism relies on the federation chain architecture, optimised DPoS consensus, and randomisation and anonymity mechanisms to achieve an effective balance between performance, security and compliance requirements, and lays a reliable technological foundation for the privacy protection and trusted data sharing of the upper-layer applications.

3.2 The Role of Cryptographic Tools in Privacy Protection

Cryptography tools, with their unique technical properties, build an impenetrable defence for healthcare data privacy protection.While blockchain itself can guarantee the trustworthiness of data storage and transmission through its distributed architecture and tamper-resistant features, the highly sensitive nature of medical data requires additional cryptographic methods to strengthen privacy protection. A common approach is the use of hybrid encryption: symmetric algorithms handle the efficient encryption of large-volume data such as medical images and text, while asymmetric encryption ensures the secure distribution of symmetric keys, thus preventing risks associated with plaintext key exposure. In practice, encryption schemes can be combined with national cryptographic standards to meet regulatory compliance, and the use of dynamic or fragmented keys can further reduce the impact of potential leaks. Meanwhile, digital signatures provide guarantees for data integrity and non-repudiation. However, the dual demand for privacy and auditability in cross-institutional collaboration drives the adoption of group signatures and ring signatures, which enable verifiability while concealing the identity of individual signers, and in certain cases, allow for accountability tracing. Additionally, de-identification techniques map real identities to hashed values, enabling on-chain verifiability without disclosing sensitive information,

thereby reducing the risk of re-identification.

In more complex cross-institutional scenarios, cryptographic tools also serve as enablers of fine-grained access control. Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS) can write the access policy into ciphertext or signature directly to achieve strict control of ‘who can access what kind of data under what conditions’, which is of great significance for multi-institutional joint scientific research and clinical diagnosis and treatment. Searchable encryption technology supports searching in a ciphertext environment, so that users can complete keyword searching without revealing the plaintext, which ensures the confidentiality of data and improves usability at the same time. Proxy re-encryption technology can securely transfer data access to other users without unlocking the ciphertext. This not only avoids the risk of original data leakage, but also reduces the security risks when transferring data across organisations. When used in conjunction with smart contracts, it can also automate rights management and policy enforcement, making the system more flexible and easier to audit.

Cryptographic tools act as the ‘glue’ that binds on-chain and off-chain systems. Due to the large volume of data, such as medical images and historical records, they are usually encrypted and stored in a decentralised file system off-chain, while only the index and access records of these data are kept on the blockchain. This reduces the storage pressure on the blockchain and ensures the traceability of all data operations. This ‘off-chain encrypted data storage, on-chain indexing and operation logging’ approach successfully achieves an effective balance between system performance, compliance requirements and user privacy protection.Overall, hybrid encryption, digital signatures, de-identification, attribute-based cryptographic systems, searchable encryption, and proxy re-encryption collectively form the core of privacy protection in blockchain-based medical data security frameworks. Together with consensus mechanisms and smart contracts, they enable the system to remain robust under the simultaneous demands of high concurrency, strict regulation, and strong privacy requirements.

To provide a more intuitive illustration of the hybrid encryption and on/off-chain collaboration process, this study presents the pseudocode of the encryption and submission workflow, as shown in Figure 2.

```
serial_number = Function <Hash> ([name, ID])
cipher_text = Function <AesEnc> ([M, k])
encrypted_key = Function <RsaEnc> ([k, public_key])
WHILE True (DO)
IF (cipher_text && encrypted_key) IS NOT NULL THEN
transaction = Function <Upload> ([serial_number, cipher_text, encrypted_key])
ELSE
Function <Sleep> ([t])
END IF
END WHILE
```

Figure 2：Encryption and submission workflow

4. Security Requirements of Digital Healthcare Data and Blockchain-Based Applications

4.1 Analysis of Medical Data Sensitivity and Privacy Risks

Electronic Health Records (EHRs) cover the entire life cycle of patients, containing essential information such as personal identity, clinical diagnoses, prescriptions, medical imaging, and test results. Once disclosed, these elements directly point to individuals and allow inferences about their health conditions and medical behaviors, making medical data inherently highly sensitive and difficult to anonymize. While the comprehensiveness and structured advantages of EHRs enhance healthcare quality and service efficiency, they also imply that any improper access may cause substantial harm to individual privacy and rights, raising higher security thresholds for data sharing and circulation.

In practice, medical institutions have long stored records in independent information systems with fragmented management strategies and data formats, hindering interoperability. As a result, patients often still need to carry paper materials for cross-institution consultations, while redundant copies and "data silos" proliferate within systems. Migration to cloud platforms by some institutions alleviates local storage pressure to a certain extent but introduces network dependency and centralized attack surfaces. Once central infrastructure is compromised, overall services may collapse due to single-point failure, which is naturally in conflict with the healthcare sector's demand for continuous availability.

The real risks of privacy breaches have been demonstrated by multiple incidents and cost assessments. Studies reveal that the average total cost of a data breach worldwide is measured in millions of dollars, with the healthcare sector bearing far higher per-record costs than other industries. Each breach results in unbearable direct expenditures and long-term trust erosion. At the same time, attack patterns are increasingly systematic and industrialized: from large-scale intrusions into national medical databases for identity information to scanning and exploiting weak configurations in PACS systems, enabling unrestricted downloads of millions of medical records and hundreds of millions of images. These incidents trigger secondary harms such as identity theft, extortion, and data tampering.

In this context, digital healthcare needs to meet three security requirements: first, confidentiality, which ensures that identity and treatment information is only visible to authorised parties when circulating across organisations; second, integrity, which ensures that data cannot be added, deleted or altered at will and can be traced back to the relevant responsible parties; and third, availability, which means that the system can continue to provide services and recover quickly from failures despite multi-party involvement and complex environments. Blockchain's decentralisation, non-tampering and traceability features provide a viable solution for the trusted sharing of medical data. Multiple organisations can maintain a unified ledger through a consensus mechanism, with on-chain records providing the basis for auditing and responsibility tracing, while reducing the risk of single point of failure and internal misuse at the architectural level, and also laying the foundation for subsequent strategies such as access control, encrypted retrieval and minimal disclosure.

4.2 Blockchain-Based Schemes for Sharing and Access Control

In cross-institutional and strong compliance medical data circulation scenarios, blockchain can be used as a 'trusted coordination layer' to fix the access control policy and data sharing process on the chain, so as to achieve auditable and traceable responsibility; while large-scale medical records and images are saved in the form of cipher text under the chain, so that performance and security can be taken into account by means of the method of 'on-chain index + off-chain cipher text'. The large-scale medical records and images are stored in the form of secret files under the chain, taking into account both performance and security by means of 'on-chain indexing + off-chain ciphering'. Under this architecture, Attribute Based Encryption (ABE) can bind access policies directly to ciphertexts or keys to achieve more granular authorisation control.

Attribute-Based Signatures (ABS) further ensure the authenticity of data sources while concealing the identity of signers, achieving both verifiability and de-identification. With the support of decentralized file systems such as IPFS, encrypted EHRs are stored off-chain, while the blockchain records immutable pointers and access traces, preventing single points of failure and preserving auditable evidence throughout the process.

In authorization and decryption workflows, a permissioned (consortium) blockchain is introduced to manage admission governance and audit logs. Patients and institutions receive policy-based keys according to their attributes, while the granting and revocation of access rights are executed atomically via on-chain transactions, avoiding uncertainties in offline coordination. To reduce terminal computing overhead, decryption can be outsourced to Self-Controlled Objects (SCOs) coordinated by smart contracts: permissions and billing are verified on-chain, while restricted ciphertext transformations are executed off-chain, ensuring that sensitive plaintext never leaves the secure domain. In addition, considering the frequent policy changes in healthcare business, the improved CP-ABE (e.g., SHDPCP-CP-ABE) is able to support semi-policy hiding and dynamic privilege updating, which enables fine-grained privilege adjustment without exposing sensitive policy details. In more complex collaborations, certificateless traceable ring signatures and distributed key generation can be integrated to enhance compatibility between anonymity and accountability.

To ensure ciphertext usability without revealing plaintext or query intentions, searchable encryption supports keyword retrieval in encrypted domains. By leveraging polynomial equations, keywords can be flexibly combined to support complex queries such as case retrieval and research screening. When authorization subjects or collaboration relationships change, proxy re-encryption enables secondary authorization without decrypting original data, reducing plaintext exposure during cross-institution circulation. Access can also be limited by time-conditioned smart contracts, ensuring that data remain readable only within predefined time windows and expire automatically afterward. To foster broader participation, reputation and incentive mechanisms can be introduced, mapping institutional compliance and resource contributions into on-chain metrics, thereby driving long-term collaborative trust.

At the system level, this study proposes a layered architecture: large-scale sensitive data such as medical records and imaging are stored off-chain, protected by symmetric or attribute-based encryption; meanwhile, blockchain records indexes, access permissions, and operation traces, with consortium blockchain consensus ensuring consistency and traceability. This design, as shown in Figure 3, enables encrypted protection and trustworthy sharing through coordinated "on-chain control + off-chain storage," avoiding the single-point failures and privacy risks of centralized systems while ensuring secure and efficient circulation in multi-institutional environments.

At the engineering implementation level, early Ethereum-based experiments such as MedRec revealed several practical limitations of public blockchains in healthcare scenarios, including high costs of on-chain storage and execution, significant transaction confirmation delays, and difficulties in adequately mitigating privacy risks within a purely on-chain architecture. These experiences suggest that real-world deployment of data-sharing and access-control solutions should adopt hybrid linkages and layered architectures. Specifically, permission management and auditing logic should be placed on permissioned blockchains or sidechains to ensure governance and traceability, while large-scale clinical data should be stored off-chain or in decentralized file systems in encrypted form. Immutable auditability can then be maintained through on-chain pointers and access records. At the same time, in order to make the system process data more efficiently and spend less cost when invoking it, it can be paired with such privacy-protecting technologies as off-chain trusted computing, zero-knowledge proof or multi-party secure computing at the application level. Specifically, the computation process that needs to be kept private is completed in

a controlled secure environment or in an encrypted area, and in the end, only the most streamlined ‘verification information’, that is, the key data that proves that the computation did not go wrong, is written back to the blockchain. This way, privacy can be preserved and the requirement of ‘verifiable results’ can be met.

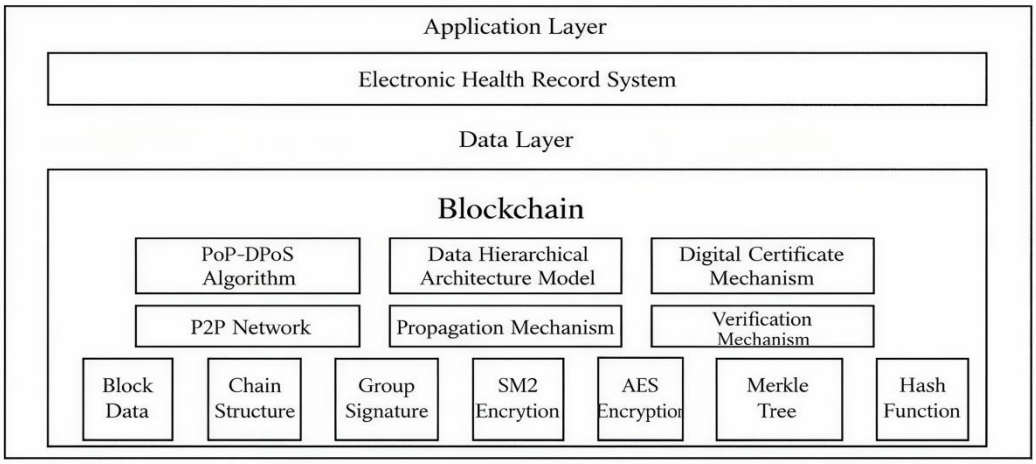

Figure 3： Overall framework of blockchain-driven medical data sharing

In the practical application of data governance and cross-system interoperability, a viable solution must strike a balance between standardisation, compliance requirements and the efficiency of multi-party collaboration. It is recommended to adopt metadata and index formats that comply with healthcare information interoperability standards (e.g., FHIR), so that data recorded on the chain and stored off the chain can be more easily recognised and recalled by various heterogeneous systems, thus reducing the cost of data integration in cross-institutional collaboration. In terms of access governance, an agency with regulatory functions or a certified industry organisation should be responsible for maintaining a node whitelist and a certificate revocation mechanism to ensure that participants are legitimate and trustworthy, and that their behaviour can be traced. When balancing privacy protection and auditing needs, a combination of policy-based authorisation mechanisms - such as attribute-based permission control or time limits - and auditable smart contracts can be used to achieve transparent management and historical traceability of the whole process from authorisation, access to revocation. In order to support scientific research and statistical application scenarios, techniques such as federated learning or differential privacy can be introduced under the premise of ensuring that individuals are not identifiable, so that multiple parties can work together to train models and analyse results without having to share the original data, thus promoting the effective use of medical data while fully protecting privacy.

Finally, deployment evaluation should be guided by quantifiable security and service metrics, covering not only traditional system performance indicators such as latency, throughput, and recovery time, but also security-related indicators such as privacy leakage probability, least-visibility achievement rate, audit traceability, and governance compliance. In practice, a gradual pilot approach is recommended: initial validation of permission models, ciphertext retrieval, and re-encryption processes can be carried out within a controlled consortium environment and limited business scenarios. Based on pilot results, adjustments can then be made to key management strategies, on-chain/off-chain task division, and incentive governance mechanisms, before scaling to broader cross-institutional collaborations. Through a combination of hybrid technical deployment and parallel institutional mechanisms for admission and auditing, blockchain-based sharing and access-control solutions can gradually enhance the trustworthy sharing capacity and governance

resilience of digital healthcare data while safeguarding individual privacy.

5. Conclusion and Outlook

This study explored the potential applications and suitable pathways of blockchain technology for secure sharing and privacy protection of digital healthcare data. The research highlights that traditional centralized architectures face inherent challenges in cross-institutional collaboration, including data silos, privacy breaches, and single points of failure. By contrast, blockchain’s decentralization, immutability, and traceability provide a new technical foundation for the trustworthy circulation of medical data. In this study, a hybrid consensus algorithm is designed based on the coalition chain architecture, which improves the fairness and tamper-proof capability of node governance by introducing random sequence generation and ring signature mechanism. In terms of privacy protection, a scheme combining hierarchical storage and identity hashing is proposed to achieve isolated protection of sensitive data with the help of irreversible encryption and off-chain storage. Experimental results show that the model achieves a good balance between performance, security and privacy protection, and provides effective support for compliant sharing of cross-institutional medical data.

However, several limitations still exist in the current research. The processing capacity of blockchain technology in high concurrency medical business scenarios is not yet sufficient to fully meet the actual demand, and how to further reduce the delay and improve the system throughput under the premise of guaranteeing security is a technical challenge that needs to be focused on in the future. Existing privacy mechanisms mostly rely on cryptographic tools and off-chain storage, how to achieve confidentiality while enhancing data availability and retrievability remains to be further explored. In addition, the promotion of blockchain in healthcare is not only about technical maturity, but also involves institutional factors such as regulatory policy, legal compliance and ethical review. Cross-institutional and cross-regional data circulation must be built on the basis of unified standards and collaborative governance before large-scale application can be realised.

Looking ahead, the application of blockchain in medical data security will show a trend of synergistic development of technological innovation and institutional construction.On the technological front, the incorporation of cutting-edge methods such as zero-knowledge proofs, secure multiparty computation, and differential privacy into consensus mechanisms and privacy-preserving algorithms can further strengthen verifiability and confidentiality. Meanwhile, approaches such as federated learning and edge computing can unlock the value of medical data without exposing plaintext, supporting the intelligent transformation of research and clinical practices. At the institutional level, the refinement of industry standards, the establishment of cross-institutional compliance frameworks, and the embedding of auditing and incentive mechanisms into smart contracts may yield replicable and scalable implementation models. With continuous technological advancements and the gradual improvement of governance systems, blockchain is poised to play an increasingly central role in safeguarding medical data security and promoting collaborative digital healthcare.

References

[1] Tertulino R, Antunes N, Morais H. Privacy in electronic health records: a systematic mapping study[J]. Journal of Public Health, 2024, 32(3): 435-454.

[2] Szarfman A, Levine J G, Tonning J M, et al. Recommendations for achieving interoperable and shareable medical data in the USA[J]. Communications medicine, 2022, 2(1): 86.

[3] Fan Y. Automatic Optimization of Trading Strategies Based on Reinforcement Learning[C]//2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT). IEEE, 2025: 59-64.

[4] Yang X, Chen A, PourNejatian N, et al. A large language model for electronic health records[J]. NPJ digital medicine, 2022, 5(1): 194.

[5] Sivan R, Zukarnain Z A. Security and privacy in cloud-based e-health system[J]. Symmetry, 2021, 13(5): 742.

[6] Wu X, Bao W. Research on the Design of a Blockchain Logistics Information Platform Based on Reputation Proof Consensus Algorithm[J]. Procedia Computer Science, 2025, 262: 973-981.

[7] Zhang M. Discussion on Using RNN Model to Optimize the Accuracy and Efficiency of Medical Image Recognition[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 66-72.

[8] Ressi D, Romanello R, Piazza C, et al. AI-enhanced blockchain technology: A review of advancements and opportunities[J]. Journal of Network and Computer Applications, 2024, 225: 103858.

[9] Hui X. Medical Entity Recognition Based on Bidirectional LSTM-CRF and Natural Language Processing Technology and Its Application in Intelligent Consultation[J]. 2025, 6(1),1-8

[10] Wu H. From Large Language Models to Innovative Applications of Blockchain AI in Web3[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 11-17.