Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.059359

REVIEW

Blockchain-Assisted Electronic Medical Data-Sharing: Developments, Approaches and Perspectives

Chenquan Gan[1,*], **Xinghai Xiao**[2], **Qingyi Zhu**[1], **Deepak Kumar Jain**[3,4] **and Akanksha Saini**[5]

[1]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China

[2]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China

[3]Key Laboratory of Intelligent Control and Optimization for Industrial Equipment of Ministry of Education, School of Artificial Intelligence, Dalian University of Technology, Dalian, 116024, China

[4]Symbiosis Institute of Technology, Symbiosis International University, Pune, 412115, India

[5]College of Business and Law, RMIT University, Melbourne, VIC 3000, Australia

*Corresponding Author: Chenquan Gan. Email: gancq@cqupt.edu.cn

Received: 04 June 2024 Accepted: 14 September 2024 Published: 19 December 2024

ABSTRACT

Medical blockchain data-sharing is a technique that employs blockchain technology to facilitate the sharing of electronic medical data. The blockchain is a decentralized digital ledger that ensures data-sharing security, transparency, and traceability through cryptographic technology and consensus algorithms. Consequently, medical blockchain data-sharing methods have garnered significant attention and research efforts. Nevertheless, current methods have different storage and transmission measures for original data in the medical blockchain, resulting in large differences in performance and privacy. Therefore, we divide the medical blockchain data-sharing method into on-chain sharing and off-chain sharing according to the original data storage location. Among them, off-chain sharing can be subdivided into on-cloud sharing and local sharing according to whether the data is moved. Subsequently, we provide a detailed analysis of basic processes and research content for each method. Finally, we summarize the challenges posed by the current methods and discuss future research directions.

KEYWORDS

Electronic medical data; data-sharing; medical blockchain; cloud; federated learning

1 Introduction

With the integration of cloud computing, big data, and the Internet of Things (IoT), digital medical technology is rapidly evolving. The use of IoT devices, such as wearable sensors, in the medical field has led to the generation of a substantial amount of electronic medical data [1]. After performing in-depth analysis using artificial intelligence technology, this data can be utilized for intelligent medical applications, including remote health monitoring and disease detection, empowering medical institutions to offer tailored treatment plans to patients [2–4]. Nonetheless, data collected by individual medical institutions may face issues, such as limited sample distribution or insufficient data volume, making it challenging to satisfy the requirements of intelligent medical applications. Sharing electronic medical data between multiple medical institutions can result in a more comprehensive dataset and improve services offered to patients [5]. However, due to the sensitivity of electronic medical data, any data leakage during the data-sharing process can severely compromise patient personal privacy [6]. Therefore, safeguarding the security and privacy of data remains a significant challenge in electronic medical data-sharing.

Privacy protection is crucial in electronic medical data-sharing. One of the traditional methods to ensure privacy is by encrypting the original electronic medical data and storing it in the cloud for sharing purposes [7–11]. Medical institutions can use private clouds internally to share data among patients and staff, or public clouds for sharing data with other institutions [12]. Cloud storage is advantageous for remote data-sharing and reducing local storage pressure. However, this method also entails a loss of direct control and ownership of data by medical institutions [13]. To address this, access control using encryption methods such as role-based or attribute-based access control can be implemented to restrict user access to data [14–16]. Nevertheless, this relies on centralized systems or trusted third parties for supervision and control. In addition, cloud environments suffer from insurmountable trust issues [17]. It is difficult for users to fully trust that cloud service providers can properly implement and comply with security measures to protect the privacy and integrity of data.

Blockchain technology can be viewed as a decentralized, transparent, and auditable digital ledger [18]. By applying blockchain to electronic medical data-sharing, access control, and trust issues can be effectively addressed [19–21]. First, a decentralized electronic medical data-sharing system can be built using blockchain, which allows electronic medical data to be shared directly without the need for third-party intermediaries [22]. This ensures the security and privacy of the data. Secondly, blockchain technology can design smart contracts to achieve more secure and automated data-sharing operations without relying on third-party trust institutions and set high-granularity access control for data access and sharing [23]. Finally, the transparency and tamper-resistance of blockchain enable all participants to verify and confirm the authenticity and integrity of data, thereby resolving trust issues [24].

With the development of medical blockchain, there have been many investigations analyzing medical blockchain from different perspectives. Jin et al. [25] divided medical blockchain into permission-based and non-permission-based methods, and scrutinized the advantages and disadvantages of each method respectively. Abu-Elezz et al. [26] analyzed the benefits of medical blockchain for patients and organizations, as well as the existence of organizational, social, and technological types of threats. Chukwu et al. [27] conducted a comprehensive technical and architectural analysis of privacy, security, cost, and performance for different medical blockchains. Attaran [28] analyzed the primary challenges that medical blockchain faces, including access control, interoperability, data integrity, and data sources, and discussed the processes they need to improve. Haleem et al. [29] investigated the advantages and workflow of medical blockchain and have discussed fourteen possible applications for the technology. Rahman et al. [30] scrutinized the application of medical blockchain in the Internet of Medical Things (IoMT) and analyzed the challenges faced by existing research concerning privacy leakage, energy consumption, and communication scalability.

Although the above studies have analyzed medical blockchain in detail, they fail to consider the differences in the specific implementation of medical blockchain. In the realm of medical blockchain data-sharing, diverse implementation methods exist based on the storage and transmission modalities of original data. The performance, security, and privacy aspects of these methods exhibit significant variations. Consequently, it becomes imperative to classify and analyze medical blockchain data-sharing methods to furnish insights for subsequent research endeavors. According to the storage location of the original electronic medical data in the medical blockchain, two primary forms emerge: on-chain sharing and off-chain sharing. The on-chain sharing method directly encrypts and saves original medical data on the blockchain and shares it through the blockchain [31]. Conversely, the off-chain sharing method entails storing the original electronic medical data outside the blockchain [32]. The off-chain sharing method further differentiates into the on-cloud sharing method and the local sharing method, depending on whether the original electronic medical data is transferred. The on-cloud sharing method preserves the original electronic medical data in the cloud, sharing the hash and address of the original data through the blockchain [33]. In contrast, the local sharing method does not transmit the original medical data saved locally, but only shares the model parameters through federated learning and blockchain [34]. The choice between on-chain, on-cloud, and local sharing methods depends on various factors, such as data size, privacy considerations, and collaboration requirements. Each method presents its unique advantages and challenges. Therefore, we delve into the analysis of the three implementations (on-chain, on-cloud, and local sharing) to discuss their contributions to medical data-sharing and the challenges they pose.

Our main contributions can be summarized as follows:

1) Utilizing blockchain and federated learning technologies to enable secure, transparent, and traceable electronic medical data-sharing.
2) Dividing medical blockchain data-sharing into on-chain and off-chain methods, with off-chain further categorized into on-cloud and local sharing according to the original data storage location.
3) Providing an in-depth analysis of each method and research content, summarizing current challenges and discussing potential future research areas.

The rest of the paper is distributed as follows: Section 2 introduces preliminary about blockchain and federated learning. Section 3 presents the current status of research on different healthcare blockchain data-sharing methods. Section 4 analyzes the challenges faced by the current research, and Section 5 discusses possible future research directions. Finally, the paper is summarized in Section 6.

2 Preliminary

This section mainly provides an overview of blockchain technology, federated learning, and their integrated applications.

2.1 Brief Introduction to Blockchain

Blockchain is an accounting technology that is jointly maintained by multiple parties, uses cryptography to ensure transmission and access security, and can achieve consistent storage of data, be difficult to tamper with and prevent denial. It is also known as distributed ledger technology. The block structure diagram of a blockchain is shown in Fig. 1. Tracing its origins, blockchain is closely linked to Bitcoin, first proposed by Satoshi Nakamoto in 2008 and emerging as the cornerstone technology of Bitcoin [18]. Since the birth of the Bitcoin network, blockchain has gradually evolved from a local technology to a globally recognized technological innovation due to its unique advantages of decentralization, immutability, and high transparency.

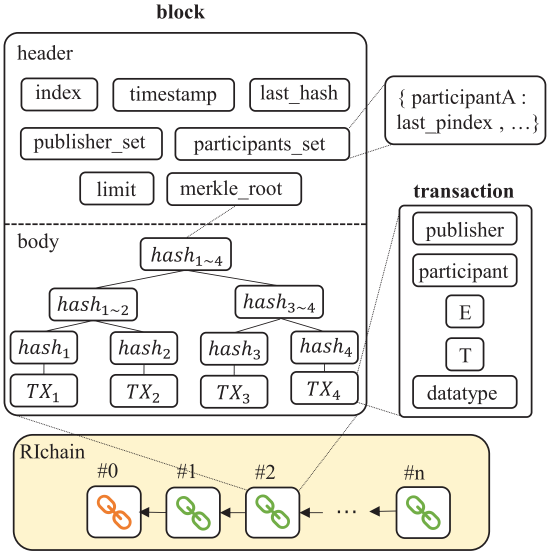

Figure 1: A block structure of a blockchain [39]

With the continuous evolution of technology, the development of blockchain has shown increasingly rich diversity, and various customized blockchain solutions have emerged, aiming to accurately meet the unique needs of different industries and fields. The various types of blockchain, including public chains, private chains, and consortium chains (the differences among them are shown in Table 1), each carry distinct technical characteristics and a wide range of application scenarios, laying a solid foundation for the widespread application of blockchain technology [35]. Blockchain technology is playing an increasingly important role in various fields such as finance, supply chain, healthcare, and real estate. It not only enhances the security and credibility of data, but also promotes transparency of information and simplification of processes, injecting new vitality into the digital transformation of various industries [36].

Table 1: Comparison of different types of blockchain

Type	Advantage	Disadvantage	Typical application
Public chains	Fully decentralized and high transparency	Slow processing of data	Bitcoin and Ethereum
Private chains	Fast transaction speed and good privacy protection	It does not have the characteristics of decentralization	Internal application
Consortium chains	Strict access control management and provide fast trading	Limited scope of application and lack of full transparency	Hyperledger Fabric

2.2 Brief Introduction to Federated Learning

Federated learning is an innovative distributed machine learning method that aims to unite training samples from multiple devices or machine learning models to collaboratively train a global model while ensuring strict protection of user data privacy. The federation learning flow chart is shown in Fig. 2. This concept was initially proposed by Google in 2016 to address data privacy and efficiency issues during local model updates on Android phones [37]. With the increasing emphasis on personal privacy and data security worldwide, federated learning, as a model of the integration of machine learning and privacy computing, provides a new solution to the problem of data silos.

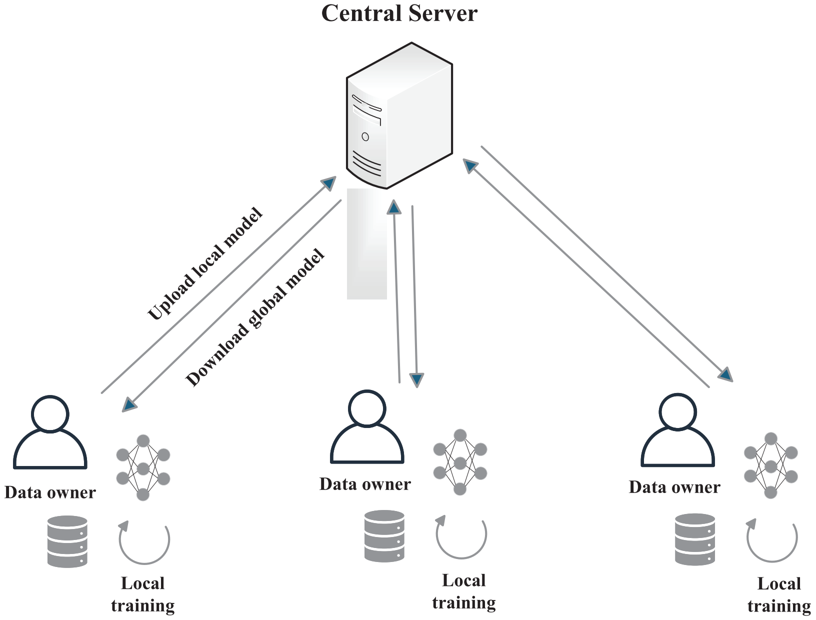

Figure 2: Federated learning framework

The federated learning system consists of three core elements: data sources, federated learning systems, and users. Under this framework, each data source is responsible for data preprocessing, jointly building a learning model, and providing timely feedback on the model's output results to users. According to the differences in the distribution of data sources among the participating parties, federated learning can be divided into three types: horizontal federated learning, vertical federated learning, and federated transfer learning. These classifications help to address data privacy protection and model training more accurately in different scenarios [38].

2.3 Brief Introduction to Blockchain-Enabled Federated Learning

Blockchain-enabled federated learning combines the advantages of blockchain technology and federated learning, aiming to improve data privacy protection, ensure the security and reliability of model training, and promote trusted collaboration among multiple parties. Looking ahead to the future, with the increasing popularity and deep application of IoT devices such as smartphones and smart homes, blockchain-enabled federated learning will demonstrate unprecedented broad application space in the field of cross device learning.

In this context, blockchain-enabled federated learning has given rise to several distinctive architectures: one is the decentralized federated learning architecture, which centers around blockchain and achieves distributed and decentralized management of the learning process; Another approach is synchronous federated learning architecture, which utilizes the characteristics of blockchain to ensure synchronous updates and consistency of learning data among multiple devices; There is also an asynchronous federated learning architecture that relies on blockchain technology to enable devices to autonomously and efficiently advance learning processes without relying on a global clock. The innovation and application of these architectures will further promote the in-depth development and widespread application of federated learning in the field of the Internet of Things [39].

3 Current Research on Medical Blockchain Data-Sharing Methods

This section aims to present an overview of the various implementations of medical blockchain data-sharing methods. To begin, we will outline the inclusion and exclusion criteria of these sharing methods. Next, we will compare relevant literature to analyze the research directions of current methods. Finally, we will provide a summary of these methods.

3.1 Inclusion and Exclusion Criteria

During the period from 2008 to 2024, we mainly conducted searches on reputable scientific databases, including IEEE Xplore, ScienceDirect, Springer, and ACM, employing keywords such as data-sharing, medical health, blockchain, and federated learning. Screen all searched literature according to the following inclusion and exclusion criteria.

1) Inclusion criterion 1: Belonging to the category of data-sharing methods. This review mainly summarizes the methods of medical data-sharing, and we will consider any literature related to data-sharing methods.
2) Inclusion criterion 2: Using blockchain and federated learning technologies. This review mainly explores the development, challenges, and solutions of blockchain and federated learning technologies in medical data-sharing.
3) Exclusion criterion 1: Not related to medical health. Under the first two inclusion criteria, remove literature unrelated to healthcare.

3.2 The Previous Survey

To have a comprehensive understanding of medical data-sharing methods, we first collected all the previous surveys related to blockchain technology applied to medical data and included a comparison table (see Table 2) to clearly highlight the advantages and improvements offered by the proposed study in relation to existing survey papers.

Table 2: Comparison of different review methods

Research work	Introduction to blockchain	Classification of data-sharing methods	Comprehensive analysis of data-sharing methods	Bibliographic comparison	Challenge discussion
Jin et al. [25]	✓	✓	×	✓	✓
Xi et al. [40]	✓	×	×	✓	✓
Młodawski et al. [41]	✓	×	×	×	✓
Dubovitskaya et al. [42]	✓	×	×	×	✓

(Continued)

Table 2 (continued)

Research work	Introduction to blockchain	Classification of data-sharing methods	Comprehensive analysis of data-sharing methods	Bibliographic comparison	Challenge discussion
Osamor et al. [43]	✓	×	×	✓	✓
Rahal et al. [44]	✓	×	×	✓	✓
Vinchurkar et al. [45]	✓	×	×	✓	✓
Deshmukh et al. [46]	✓	×	×	×	✓
Ours	✓	✓	✓	✓	✓

The analysis presented in Table 2 compares five key aspects. These methods all involve blockchain technology, but there are individual or several shortcomings, only our method is comprehensive and meets all requirements. The details of these methods are outlined as follows: Jin et al. [25] categorized medical data-sharing into two types: permissioned blockchain and permissionless blockchain approaches. Xi et al. [40] emphasized the tamper-proof and traceable characteristics of blockchain in managing medical data. Młodawski et al. [41] explored the application of blockchain in healthcare, along with its potential benefits and challenges. Dubovitskaya et al. [42] analyzed the motivations, advantages, and limitations of implementing blockchain technology in oncology. Osamor et al. [43] identified critical challenges related to scalability, regulatory considerations, and ethical implications that must be addressed for successful integration of healthcare blockchains. Rahal et al. [44] conducted a comparative study of various technologies developed from blockchain in the medical field. Vinchurkar et al. [45] discussed research directions and use cases for blockchain in healthcare, providing a comprehensive overview of data management and storage technologies in healthcare systems. Finally, Deshmukh et al. [46] delved into the decentralized storage framework for accessing medical information in smart applications.

In addition, for ease of description, according to the original medical data storage and transmission in the medical blockchain, we classify the current medical blockchain methods into three categories: on-chain sharing, cloud sharing, and local sharing. A comparison of these three medical blockchain implementation methods is shown in Table 3.

Table 3: Comparison of different implementation methods of medical blockchain

Method	Storage location	Metadata transfer	Size limit	Data security	Storage cost	Sharing performance
On-chain sharing	On-chain	Yes	Yes	High	High	Normal
On-cloud sharing	Off-chain	Yes	No	Normal	Normal	High
Local sharing	Off-chain	No	No	High	Normal	High

3.3 On-Chain Sharing

The method of on-chain sharing involves encrypting electronic medical data by smart contracts and storing it on the blockchain for sharing, which is then jointly maintained by the nodes that join the blockchain [47]. The blockchain's decentralization, anonymity, and tamper-resistance provide ample protection for the encrypted electronic medical data stored on the chain, ensuring the security of electronic medical data during sharing [48]. The operating process of this method is illustrated in Fig. 3. Data requesters use smart contracts to request data-sharing. Upon obtaining permission from the data owner, the smart contract searches for the corresponding data on the chain, decrypts it, and sends it to the data requester. The blockchain can achieve distributed storage of chain data, thereby avoiding single-point failures [49]. Furthermore, the decentralized nature of the blockchain ensures that data-sharing only requires consensus among nodes on the blockchain without third-party endorsement, thus resolving trust issues [50]. Additionally, the process of encrypting electronic medical data on the chain via smart contracts can also specify the format of sharing data from different sources, reducing data heterogeneity [51].

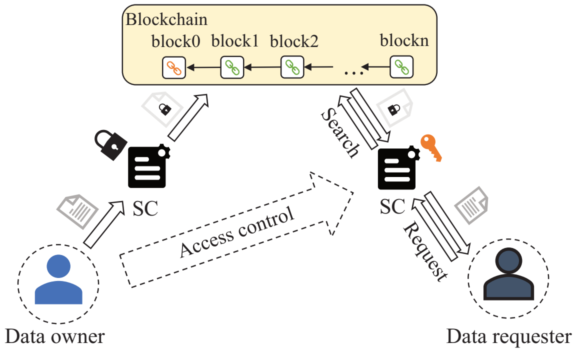

Figure 3: Operation process of the original electronic medical data on-chain sharing methods

Table 4 compares current studies on on-chain sharing methods. It can be observed that these studies are typically implemented on blockchain platforms such as Ethereum and Hyperledger. This is because these platforms have mature consensus mechanisms and can facilitate the deployment of smart contracts to achieve authentication of data requesters, thus providing data owners with access control to data on the chain [24,50,52]. Additionally, due to block size limitations, electronic medical data in the on-chain sharing method is dominated by data with highly compressed features, such as Electronic Medical Records (EMR). To enhance the privacy, efficiency, and security of the on-chain sharing methods, these studies have actively explored searchable encryption, matching mechanism, and security optimization mechanism.

Table 4: Comparison of on-chain sharing methods

Category	Research work	Platform	Medical data from	Access control	Searchable encryption	Matching mechanism	Security optimization	Consensus algorithm
Access control mechanism	Sharma et al. [52]	Ethereum	Medical certificate	✓	×	×	×	PoW
	Garcia et al. [24]	Hyperledger Besu; CosmWasm	Electronic prescription	✓	×	×	×	IBFT2; Tendermint

(Continued)

Table 4 (continued)

Category	Research work	Platform	Medical data from	Access control	Searchable encryption	Matching mechanism	Security optimization	Consensus algorithm
	Al-Sumaidaee et al. [50]	Hyperledger Fabric	Uncertain	✓	×	×	×	RAFT
Searchable encryption	Zhang et al. [49]	JUICE	PHI	✓	✓	×	×	PoC
	Xu et al. [53]	Ethereum	IoMT data	✓	✓	×	×	Uncertain
	Shamshad et al. [54]	Self-Building	EHR	✓	✓	×	✓	Uncertain
	Rahman et al. [55]	Self-Building	IoMT data	✓	✓	×	×	Uncertain
Matching mechanism	Liu et al. [56]	Uncertain	EHR	✓	×	✓	×	Improved DPoS
	Wu et al. [57]	Chainsql	EMR	✓	×	✓	✓	PoP
	Abdellatif et al. [58]	Uncertain	IoMT data	×	×	✓	×	DPoS
	Wu et al. [59]	Chainsql	EMR	✓	×	✓	×	PoP
Security optimization mechanism	Lee et al. [48]	Self-Building	EHR	✓	×	×	✓	Uncertain
	Qu et al. [60]	Uncertain	QEMR	×	×	×	✓	Uncertain
	Cao et al. [61]	Ethereum	EHR	✓	×	×	✓	PoW
	Guo et al. [62]	Uncertain	EHR	✓	×	×	✓	Uncertain
	Zou et al. [63]	Self-Building	EMR	✓	×	×	✓	BFT-SMaRt

Searchable encryption. As the amount of electronic medical data stored on the blockchain increases, the on-chain sharing method needs to ensure data privacy while achieving accurate data searchability. To address this issue, many studies use searchable encryption to encrypt electronic medical data [49]. Xu et al. [53] employed attribute-based encryption (ABE) to encrypt patients' data and generate an index after encryption. Authorized hospital doctors can generate search traps, and zero-knowledge proofs are used to match doctors with patients to achieve secure data-sharing. An authorization and revocation mechanism was also implemented to ensure that patients can implement access control. Shamshad et al. [54] utilized public encryption with keyword search (PEKS) technology with keyword search to encrypt electronic health record data and save the encrypted data on a private blockchain. The security index consisting of encrypted keywords was stored on the alliance blockchain. The system administrator used proxy re-encryption (PRE) to enable third-party users to securely access data. Rahman et al. [55] proposed a secure symmetric order-preserving encryption (OPE) technology based on the characteristics of IoMT data to achieve privacy protection for accurate and range searches. They also introduced an efficient search result verification mechanism based on multi-signatures, allowing blockchain nodes and data users to authenticate and verify search results.

Matching mechanism. As the number of data owners and requesters participating in electronic medical data-sharing increases, these entities have different sharing purposes, as well as varying degrees of urgency and needs. Therefore, a matching mechanism is needed to establish matching relationships between these entities, in order to improve the efficiency of electronic medical data-sharing [59]. Liu et al. [56] proposed a symptom matching mechanism for patients with the same disease symptoms. Once mutual authentication is completed, patients can establish a session key to convey disease information. They also improved traditional delegation proof-of-stake to enhance data-sharing efficiency. Wu et al. [57] used a hierarchical purpose tree to classify and relate different data-sharing purposes and developed a matching mechanism that enables mutual anonymous evaluation. The mechanism provides secure and privacy-preserving access control decisions for different purposes. To ensure the privacy of evaluation, local differential privacy protection technology is also used to protect its sensitive attributes before the data is put on the chain. Abdellatif et al. [58] designed a multi-channel blockchain architecture that assigns different priorities to share tasks based on their urgency and importance. The architecture matches the tasks to appropriate channels and optimizes the blockchain channel configuration to fit the characteristics and types of electronic medical data, thereby enhancing sharing efficiency and reducing computational costs.

Security optimization mechanism. Although blockchain can permanently store encrypted electronic medical data on the chain and protect them from tampering, the privacy and security of on-chain data are still inevitably threatened when facing attacks against the blockchain. Therefore, corresponding security optimization measures need to be designed to resist possible attacks [48,61]. Guo et al. [62] proposed a Multiple Authority Attribute-Based Signature (MA-ABS) scheme based on monotonic predicates to safeguard patients' privacy and maintain the integrity of electronic health record data. They also employed a shared pseudorandom function seed between every two medical institutions to resist conspiracy attacks from N-1 corrupt institutions. Zou et al. [63] reconstructed the block structure by using a chameleon hash function and changed the structure of the chain, dividing the blocks into key blocks and micro blocks. The key block stores the blockchain public key of the current leader, and the micro blocks link to the key block to save specific sharing transactions. A reputation proof consensus was designed to select the leader responsible for mining. Through changes in blockchain structure and consensus can effectively resist 51% attacks, Sybil attacks, and reputation fraud attacks from the blockchain. Qu et al. [60] designed a quantum blockchain network to implement electronic medical data-sharing and a new distributed quantum electronic medical record (QEMR) protocol. By introducing a quantum authentication program to track on-chain data and ensure its safety and privacy, it can effectively resist external attacks, Intercept-Measure-Repeat (IMR) attacks, and Entanglement-Measure (EM) attacks.

The on-chain sharing method offers a decentralized storage solution for encrypted medical records. Even if a node in the blockchain fails, data can still be obtained by accessing other nodes. In addition, benefiting from the tamper-proof characteristic of the blockchain, the security and privacy of encrypted electronic medical data stored on the chain can be well protected. While searchable encryption, matching mechanisms, and anti-attack methods can address some challenges faced by this method, there are still some outstanding issues. The limited block capacity of the blockchain currently impedes the sharing of large medical files such as images. Additionally, electronic medical data is time-sensitive and does not require permanent storage on the blockchain, which can pose significant storage challenges as the blockchain grows in size.

3.4 On-Cloud Sharing

The method of on-cloud sharing entails encryption of the electronic medical data and storing it on a storage server in the cloud. Subsequently, the blockchain is utilized to store the hash, index, and storage address of the encrypted electronic medical data for data-sharing [64]. The blockchain can check whether the electronic medical data has been tampered with by checking the information stored on the blockchain and helping users understand the flow of data during data-sharing [65]. Fig. 4 illustrates the operating process of the method of on-cloud sharing. Once the data requester undergoes blockchain identity verification, they can search for the required electronic medical data by using the critical information saved on the blockchain. The data requester then sends a sharing request to the data owner and, upon receiving the owner's consent, obtains the decryption key to complete the data-sharing. This method of data-sharing ensures efficient storage of electronic medical data with a large capacity and prevents cloud service providers from tampering with data by verifying the information stored on the blockchain [66]. Furthermore, the anonymity of the blockchain enables verification of the authenticity of the data source without revealing the identity of the data owner [67].

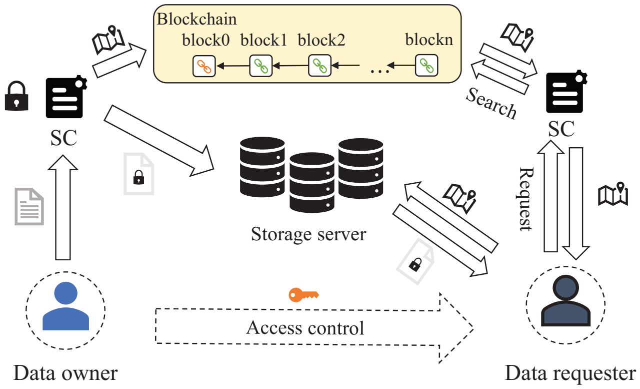

Figure 4: Operation process of the original electronic medical data on-cloud sharing methods

Access control based on ABE and smart contracts. We conducted a comparative analysis of various on-cloud sharing methods in the relevant research, and the results are presented in Table 5. Most of the existing research uses attribute-based encryption and smart contracts to achieve fine-grained access control [68,69]. Wang et al. [70] proposed a constant-size attribute-based encryption scheme and a privacy-preserving on-chain boolean search scheme, which embeds the attribute access policy into the search results on the blockchain. Yang et al. [71] reduced the computation burden on users by allowing them to specify specific access policies and authorizing doctors to use attribute-based encryption schemes to encrypt electronic medical data. They also used an attribute-based signature scheme to sign the data, which protects the identity of the signatory while verifying the authenticity of the electronic medical data source. Tan et al. [72] utilized attribute-based encryption for electronic medical data and saved a tracking list and a revocation list of the data on the blockchain. This method allows only users who meet the required attributes and are not on the revocation list to access the data, thus preventing malicious users from destroying data-sharing. Dai et al. [73] proposed a decentralized attribute-based encryption (DABE) scheme to encrypt data and used an attribute-hiding zero-knowledge proof to protect the attribute privacy of users during the access control process. In methods of on-cloud sharing, searchable encryption technology can achieve privacy protection and retrieval of data on untrusted cloud storage servers. Additionally, combining attribute-based encryption and smart contracts provides secure and reliable access control [74]. Chen et al. [75] employed K-anonymity to preprocess electronic medical data before encrypting it with searchable encryption technology. They utilized smart contracts to enable keyword search and attribute-based access control, thereby restricting data access to users who meet the corresponding attributes. Zhang et al. [76] developed an attribute-based searchable encryption method based on blockchain to provide fine-grained access control and efficient retrieval of encrypted electronic medical data. They also periodically update the key to prevent key leakage and ensure the forward security of the encrypted electronic medical data. Li et al. [77] proposed a secure keyword searchable attribute-based encryption scheme based on lattice cryptography. This scheme not only provides secure and fine-grained access control, but also reduces communication costs and key size. It can effectively resist adaptive keyword attacks and adaptive selection policy attacks in a quantum computing environment.

Table 5: Comparison of on-cloud sharing methods

Category	Research work	Platform	Medical data from	Access control	Searchable encryption	Security optimization	Consensus algorithm	Storage method
Access control based on ABE and smart contracts	Xia et al. [68]	Self-Building	EMR	✓	×	×	Uncertain	Cloud
	Cheng et al. [69]	Uncertain	Uncertain	✓	×	×	Uncertain	Cloud
	Yang et al. [71]	Uncertain	Uncertain	✓	×	×	Uncertain	Cloud
	Wang et al. [70]	Ethereum	EHR	✓	×	×	Uncertain	Cloud
	Chen et al. [75]	Hyperledger Fabric	PHI	✓	✓	×	Uncertain	Cloud
	Dai et al. [73]	Ethereum	Uncertain	✓	×	✓	Uncertain	Cloud
	Zhang et al. [76]	Ethereum	PHR	✓	✓	✓	PoA	Cloud
	Li et al. [77]	Uncertain	EMR	✓	✓	✓	Uncertain	Cloud
Security optimization	Nguyen et al. [67]	Ethereum	EMR	✓	×	✓	Uncertain	IPFS
	De Aguiar et al. [78]	Hyperledger Fabric	Medical images	✓	×	✓	PBFT	Cloud
	Azbeg et al. [79]	Ethereum	IoMT data	✓	×	✓	PoA	IPFS
	Egala et al. [80]	Ethereum	EHR	✓	×	✓	Uncertain	IPFS
	Jayabalan et al. [81]	Uncertain	EHR	✓	×	✓	PoW	IPFS
Consensus mechanism platform construction	Du et al. [82]	Self-Building	EMR	✓	×	✓	MBFT	Cloud
	Pang et al. [74]	Self-Building	EHR	✓	✓	×	sc-PBFT	Cloud
	Fan et al. [64]	Uncertain	EMR	✓	×	×	Hybrid-consensus	Cloud

Security optimization. Remote access to encrypted electronic medical data stored on cloud servers requires security optimization to prevent various security threats. To address this issue, De Aguiar et al. [78] inserted a unique identifier token into electronic medical data to prevent data leakage. This token is stored on the blockchain, which not only enables data owners to control data access, but also quickly identifies and holds accountable those responsible for data leakage. In addition, to mitigate the threat of DoS attacks faced by centralized cloud storage servers, using a decentralized InterPlanetary File System (IPFS) to store encrypted electronic medical data has become a commonly used security optimization method [67,79]. Egala et al. [80] implemented a hybrid on-chain/off-chain storage and computing architecture using blockchain and IPFS, which reduces storage costs and latency while introducing selective ring-based access control, patient anonymity, and device authentication algorithms to provide data privacy, security, traceability, and availability. Jayabalan et al. [81] encrypted original electronic medical data with symmetric keys and stored them on IPFS, used asymmetric encryption to generate digital envelopes to transmit symmetric keys to authorized entities, and finally used digital signatures to ensure the validity of transactions and verify them from authorized nodes. To prevent Sybil attacks, two-factor authentication is also employed to verify the identities of doctors and patients. Shuaib et al. [83] used the Istanbul Byzantine Fault Tolerance (IBFT) consensus algorithm to reduce delay, throughput, success rate, and other issues caused by IPFS, and used a threshold signature scheme to record index data on the blockchain to protect users' privacy from link attacks caused by associating patients with every provider they have accessed.

Consensus mechanism platform construction. Currently, most research on on-cloud data-sharing methods relies on existing blockchain platforms such as Ethereum and Hyperledger. However, the consensus mechanisms utilized by these platforms are not scalable enough to cater to electronic medical data-sharing requirements of various scales. Therefore, constructing a blockchain platform based on actual needs and improving the consensus mechanism is crucial. Fan et al. [64] have designed a hybrid consensus mechanism that selects an endorsement node for transaction submission in each region. By allowing endorsement nodes to take turns submitting transactions, network congestion caused by data flooding can be avoided, and consensus can be reached with minimal resources. To improve the efficiency of data-sharing, Du et al. [82] have designed a Mixed Byzantine Fault Tolerance (MBFT) algorithm that periodically selects verification nodes using verifiable random functions to form a consensus committee. The consensus committee audits the electronic medical data-sharing records during its tenure and anonymizes the shared records on the chain to prevent irrelevant third parties from observing the sharing records. Moreover, Pang et al. [74] have designed a Practical Byzantine Fault Tolerance (PBFT) consensus algorithm with node-state-checkable functionality that checks the status of the main node based on the completion status of the pre-prepare, prepare, and commit phases. Any malicious behavior exhibited by the main node will be marked and isolated to prevent malicious nodes from interfering with data-sharing.

The on-cloud sharing method can provide a solution for sharing large amounts of electronic medical data, but the choice of storage server also puts on-cloud sharing in a dilemma. Sharing encrypted original electronic medical data via cloud storage servers can effectively address security concerns in electronic medical data-sharing, and has the added benefits of flexibility and scalability [26]. However, cloud storage servers pose centralization issues and make it difficult to recover lost or tampered data. Using IPFS to encrypt and store raw data in a distributed manner can solve the centralization problem of cloud storage, allowing data to be accessed from multiple locations, and also has advantages such as decentralization and anonymous access [84]. Nevertheless, the distributed storage method and P2P network structure may result in reduced efficiency of data-sharing and higher storage costs compared to cloud storage servers. Moreover, both on-chain and on-cloud sharing methods require the transmission and movement of original electronic medical data, which increases the risk of privacy breaches during transmission.

3.5 Local Sharing

To address the security risks associated with the transmission and sharing of the original electronic medical data, the method of local sharing which is combined with federated learning has emerged [85]. With this method, federated learning can be used to train local electronic medical data, and a new global model can be obtained by sharing and aggregating the model parameters trained locally by data owners through a central aggregator, without limiting the size of the original data [86–88]. Blockchain can provide a decentralized implementation and incentive mechanism for federated learning [89–91]. Compared to on-chain and on-cloud sharing methods, the local sharing method can better safeguard the privacy of original electronic medical data. Currently, there are two main implementations for the local sharing methods.

The first implementation is to implement federated learning on the chain, as shown in Fig. 5. The blockchain is used to store the global model parameters as well as the local model parameters for federated learning, and the model parameters are aggregated through smart contracts [92,93]. The data requester of federal learning publishes the initial global model to the blockchain, and other data owners get the global model by accessing the latest block, and then use the local data for training to get the local model parameters. The local model parameters will be sent to the blockchain as transactions and then aggregated through smart contracts to get the new global model. Then a mining node is selected by blockchain consensus to generate a new block containing the global model parameters. Data owners access the new blocks for the next round of training, and so on until the global model converges. This implementation utilizes a decentralized blockchain instead of a central aggregator, thus avoiding a single point of failure and also giving incentives to the data owners using the mining mechanism of the blockchain [94].

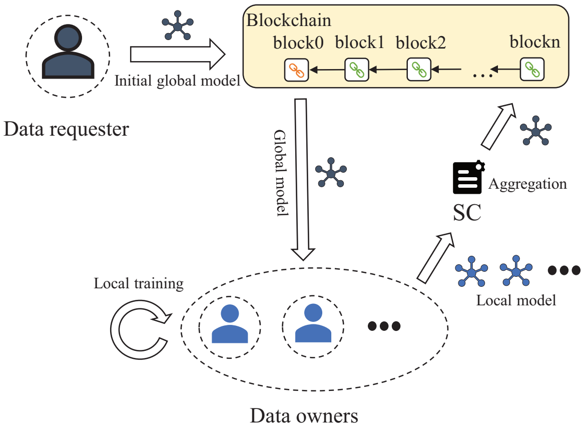

Figure 5: Operation process of the original electronic medical data local sharing methods implemented on-chain

Another implementation is to implement federated learning under the chain, as shown in Fig. 6. The blockchain is used to store information about the index, reputation, and incentive of the nodes, and then the information on the chain is used to select nodes for federated learning [95,96]. In the federated learning process, the first step is for data owners to register on the blockchain and save relevant node information. When a data requester submits a shared task request, the system selects suitable data owners in the node selection phase based on the node information saved on the blockchain before starting federated learning. After completion of the federated learning process, the system updates the nodes' information on the blockchain based on their performance during training. This method improves efficiency and enables the evaluation of node parameters to prevent low-quality and malicious nodes from participating, thus enhancing the training effectiveness of federated learning [97]. In addition, the incentive of the nodes is given by their overall performance, which can motivate the data owners to maintain the stability of each training round.

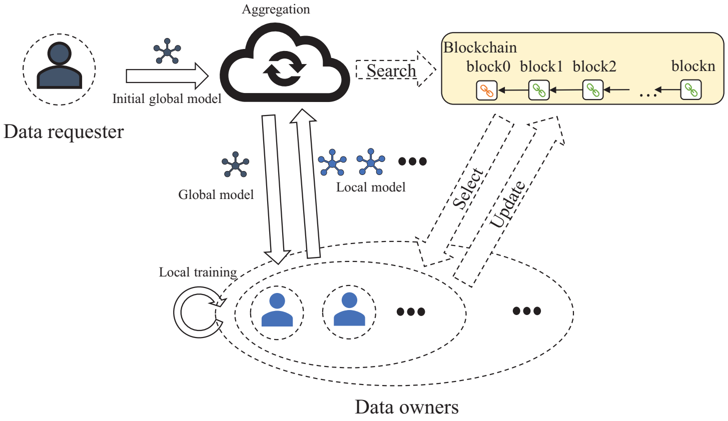

Figure 6: Operation process of the original electronic medical data local sharing methods implemented off-chain

We compared the current research for the local sharing methods, and the results are shown in Table 6. Similar to the method for on-cloud sharing, the method for local sharing does not limit the size of original electronic medical data and mostly performs image task sharing. In addition, to improve the sharing efficiency of federated learning, there are several studies to improve the consensus algorithm by constructing blockchain by themselves. Samuel et al. [98] designed a consensus algorithm based on two rounds of the reinforced additive games to select the mining nodes by the scores of each node after participating in the game. It can reduce the energy consumption of consensus while guaranteeing fairness. Chen et al. [99] proposed a Proof-of-Contribution (PoC) algorithm that can select the node with the largest contribution as the mining node based on the node's contribution to the global model accuracy at each training round by giving a corresponding incentive. Jin et al. [100] proposed a Delayed Consensus (DefCon) that can periodically select a cluster representative for aggregation to achieve single-chain consensus and cross-chain consensus, thus reducing the frequency of consensus communication and improving system efficiency.

Table 6: Comparison of local sharing methods

Category	Research work	Platform	Medical data from	Preprocessing optimization	Model optimization	Security optimization	Incentive mechanism	Consensus algorithm	FL Position
Data preprocessing	Sun et al. [97]	Uncertain	INCART	✓	×	×	×	Uncertain	Off-chain
	Samuel et al. [98]	Self-Building	IoMT data	✓	×	×	✓	Two rounds reinforcing addition game	On-chain
	Połap et al. [101]	Self-Building	MNIST	✓	×	×	×	Uncertain	Off-chain
	Wang et al. [102]	Uncertain	GAMETES	✓	✓	✓	×	Uncertain	Off-chain
	Kumar et al. [103]	Uncertain	Medical images	✓	✓	×	×	PoW	On-chain
Model optimization	Noman et al. [85]	Self-Building	Medical images	×	✓	×	✓	PoW	On-chain
	Chen et al. [99]	Hyperledger Fabric	Medical images	×	✓	×	✓	PoC	On-chain
	Hai et al. [104]	Hyperledger	EHR	×	✓	×	×	Uncertain	Off-chain
	Houda et al. [105]	Ethereum	PHR	×	✓	×	×	PoW	On-chain
Security optimization mechanism	Singh et al. [93]	Uncertain	Uncertain	×	×	✓	✓	Uncertain	On-chain
	Rehman et al. [106]	Uncertain	IoMT data	✓	×	✓	×	Uncertain	On-chain
	Wang et al. [107]	Hyperledger Fabric	Uncertain	×	×	✓	×	Uncertain	On-chain
	Alzubi et al. [108]	Uncertain	EHR	×	×	✓	×	Uncertain	On-chain
	Lakhan et al. [109]	Uncertain	IoMT data	×	×	✓	×	PoW	On-chain
	Rahman et al. [110]	Uncertain	IoMT data	×	×	✓	×	Uncertain	On-chain
Other	Jin et al. [100]	Self-Building	IoMT data	×	×	✓	✓	DefCon	On-chain
	El Rifai et al. [94]	Ethereum	Pima Indians Diabetes	×	×	×	×	Uncertain	On-chain
	Das et al. [92]	Ethereum	Uncertain	×	×	✓	×	PoW	On-chain

Data preprocessing. Since the size, quality, type, time, and other factors of training data vary among medical institutions when performing local model training, the differences in these training parameters will affect the effect of model training and data-sharing. Therefore, there are many studies to optimize the data preprocessing before federated learning [98,106]. Kumar et al. [103] used the Lanczos interpolation algorithm to adjust CT images with different resolutions in the data preprocessing stage, and then normalized the signal intensity of each voxel in the CT images.

Wang et al. [102] have designed an automatic quality control method that can screen the data quality of nodes participating in federated learning. The quality control information is then stored on the blockchain to help exclude low-quality nodes from participating and improve the modeling efficiency of federated learning. Połap et al. [101] set up a data management agent to classify and manage different types of electronic medical data, and then store information such as the index and type of the data on the blockchain, so that the classified electronic medical data can be quickly used for federated learning train. Sun et al. [97] used a micro-classifier based on Kullback-Leibler divergence to achieve the high-precision dynamic classification of electronic medical data of different types and seasons, thereby improving the generalization ability of the model.

Model optimization. To obtain better medical detection results, it is necessary to optimize the federated learning model. Model optimization is mainly divided into two aspects. On the one hand, it is to design more complex models and deploy them in federated learning; on the other hand, it is to improve the aggregation algorithm of the global model in federated learning. Most of the current federated learning combined with blockchain scenarios is based on Convolutional Neural Networks (CNN) [89,92]. These shallow neural network models perform poorly in the face of complex disease detection tasks. Kumar et al. [103] proposed a permissioned blockchain-based federated learning framework and designed a capsule network to generate a high-precision classification model for COVID-19 detection. Hai et al. [104] used blockchain to store electronic medical data indexes, and then used federated learning to train LightGBM and N-Gram models to provide patients with personalized treatment plans. In addition, the aggregation algorithm of original federated learning can only determine the weight according to the data volume of the data owners, and needs to wait for all nodes to upload updates before aggregation. This makes the inference and classification performance of the model limited by the quality of the data owners, thereby degrading the effectiveness of electronic medical data-sharing. Therefore, Houda et al. [105] designed a new secure aggregation algorithm for local learning models based on Secure Multiparty Computation (SMPC), which improves the aggregated global model quality. Chen et al. [99] designed a contribution-weighted aggregation algorithm, which takes the contribution of data owners to the global model accuracy and the amount of data together as the weight for aggregation. Noman et al. [85] directly combined the local model test accuracy and data volume of data owners into a weight matrix, thereby reducing the time cost caused by repeated testing of node contributions.

Security optimization mechanism. Although the local sharing methods based on federated learning have good security performance, they will also face security threats from both blockchain and federated learning. On the one hand, the blockchain itself has security issues such as 51% attacks, replay attacks, and Sybil attacks. On the other hand, federated learning is also vulnerable to damage such as poisoning attacks and reasoning attacks. Therefore, how to design an additional security optimization mechanism is also the focus of current research. Singh et al. [93] leveraged permissioned blockchains to design additional security protocols via differential privacy and homomorphic encryption to achieve perfect forward secrecy and prevent replay attacks. Rahman et al. [110] used Intel Software Guard Extension (SGX) to provide security protection for model parameter aggregation on hardware, and then used homomorphic encryption and differential privacy of multi-party computing to reduce the possibility of inference attacks. Wang et al. [107] utilized smart contracts to verify the identities of data owners, and then detect the quality of each data owner's local model parameters, thereby preventing Sybil attacks and poisoning attacks. Rehman et al. [106] used blockchain to connect data owners in the medical system, and then designed an intrusion detection system (IDS) to detect malicious behavior of data owners through smart contracts, so as to prevent the model aggregation of federated learning from being destroyed. Alzubi et al. [108] designed a CNN-based security classification model to classify normal and abnormal users by using available data sets, and then select reliable nodes to participate in federated learning combined with blockchain. Lakhan et al. [109] saved a detection list on the blockchain, and screened out abnormal data through the detection list after the training of each data owner was completed, so as to ensure the training effect of federated learning.

The method of local sharing of original electronic medical data is a new development trend in medical blockchain data-sharing. Federated learning can solve the "data island" problem existing in electronic medical data, enabling multiple medical institutions to obtain more accurate medical models by sharing model parameters. Blockchain can provide a decentralized, secure, and transparent shared environment for federated learning, and it can also solve the problem of the lack of incentives for federated learning. Although the current implementations of the local sharing methods have their advantages, they also have shortcomings. When federated learning is implemented on the chain, the efficiency of federated learning is limited by the efficiency of blockchain consensus, which makes it difficult to meet large-scale shared tasks, and lacks the management of data owners. When federated learning is implemented off-chain, since the blockchain is only used to manage node information, federated learning needs to rely on the central aggregator for parameter aggregation, and still faces problems such as single point of failure and DoS attacks.

These three blockchain medical data-sharing methods have their own advantages and disadvantages and are applicable in different scenarios. On-chain sharing is suitable for sensitive data-sharing such as small medical records or identity authentication that require high security, but when the data is large, it cannot be efficiently expanded, and privacy protection needs to be strengthened. On-cloud sharing is suitable for large medical image data analysis and rapid processing of non-sensitive data, but data security depends on third parties and requires improved encryption and access control. Local sharing is suitable for cross-institutional collaborative research and distributed data analytics that requires data privacy, such as federated learning, but federated learning requires efficient model synchronization mechanisms and reliable participant management. The specific advantages and disadvantages of each method are shown in Table 7.

Table 7: Comparison of advantages and disadvantages

Method	Advantage	Disadvantage
On-chain sharing	High security Data immutable Strong transparency	Limited storage capacity High cost High latency
On-cloud sharing	Large storage capacity Fast processing speed Lower cost	Inadequate privacy protection Rely on cloud service providers
Local sharing	Data privacy is well protected Distributed processing Applicable federated learning	Complex coordination mechanism High computing resource requirements

4 Current Challenges

Through the above content, this paper analyzes the research content of the three methods of the current medical blockchain data-sharing. In this section, we will analyze some common challenges faced by existing methods.

4.1 Consensus Algorithm Limitations

The new block containing the shared results needs to be approved by most nodes on the blockchain through the consensus algorithm before it can be uploaded to the chain. Therefore, the operating efficiency of the medical blockchain data-sharing method is greatly limited by the consensus algorithm of the blockchain.

Most of the current research relies on the consensus algorithm in the existing blockchain platform to build a medical blockchain, such as the Proof of Work (PoW) algorithm [18], the Proof of Stack (PoS) algorithm [111], Practical Byzantine Fault Tolerance (PBFT) algorithm [112], etc. Although the PoW algorithm can provide better security and fairness, it has disadvantages such as low throughput and high energy consumption. These shortcomings will make it difficult for the medical blockchain composed of PoW algorithms to achieve real-time sharing and difficult to deploy in IoMT. For example, when there are a large number of healthcare organizations that need to share and access healthcare data in real-time, PoW algorithms may not provide sufficient transaction throughput, resulting in data synchronization delays or network congestion. Compared with the PoW algorithm, the PoS algorithm reduces energy consumption and improves throughput. However, this algorithm sacrifices some security and fairness, which may cause some nodes to be controlled by larger currency holders. Although the medical blockchain composed of a PoS algorithm can improve the efficiency of data-sharing, it also brings huge security risks. The PBFT algorithm also improves throughput and reduces energy consumption, and has stronger network security. However, it is necessary to select highly trusted nodes to participate in the consensus process, which is not conducive to decentralization. At the same time, when the number of nodes is too large, it will lead to performance degradation. In medical blockchain data-sharing, the medical blockchain composed of the PBFT algorithm has the characteristics of fast transaction confirmation and strong fault tolerance, which can improve the efficiency and security of data-sharing. However, the PBFT algorithm needs to communicate with each other among all nodes, so there may be performance bottlenecks in large-scale electronic medical data-sharing. These consensus algorithms either focus on solving the problems of security and energy consumption, or focus on solving the problems of communication and processing time constraints, which are difficult to perfectly adapt to electronic medical data-sharing. Therefore, how to balance the relationship between the two and design a new consensus algorithm based on the actual electronic medical data-sharing scenario still needs research [56,82]. The limitations of consensus algorithms can lead to medical data not being synchronized to the blockchain network in real-time, thus affecting doctors' timely diagnosis and treatment of patients' conditions. As the amount of medical data continues to increase, the limitations of consensus algorithms will be further highlighted, limiting the scalability of blockchain networks and the inability to meet the needs of future medical data-sharing. To overcome these limitations, new consensus algorithms for medical data-sharing need to be investigated. These algorithms should take into account the efficiency, security and degree of decentralization, while considering the particularity and real-time requirements of medical data. For example, consensus algorithms based on credit scores can be explored, or a combination of multiple consensus mechanisms can dynamically adjust consensus strategies based on network state and transaction demand.

In addition, the existing consensus algorithm cannot be combined with the federated learning process, which leads to the need for additional consensus calculations to generate blocks containing new global model parameters after the medical blockchain collects the local training parameters uploaded by the nodes [35]. This not only leads to increased energy consumption in the data-sharing process, but also makes the sharing efficiency greatly limited by the block production speed of the consensus algorithm.

4.2 Lack of Reputation Management Mechanisms

To maintain the security and reliability of medical blockchain data-sharing, it is necessary to ensure that the behavior of participants is legal and prevent the malicious behavior of nodes from destroying the sharing. Current research mainly focuses on trust management mechanisms such as identity authentication [56], authority management [53], and access control [71] in medical blockchains, and there is a lack of discussion on reputation management mechanisms.

The reputation management mechanism is used to evaluate and record the behavior, contribution, and reliability of the participants, so as to determine their rights and benefits in the network according to the reputation value, which is a dynamic management method [85]. In the medical blockchain data-sharing method, by designing the reputation management mechanism to evaluate the reputation value of the participants, the appropriate participants can be selected for data transmission and sharing, thereby improving the security and reliability of data-sharing. Specifically, the reputation management mechanism can assign an initial reputation value to each participant in electronic medical data-sharing. The reputation value will be updated as the participant's historical behavior, transaction records, data contribution, and other factors change. Participation with high reputation value Participants will be given priority in data-sharing. In addition, the reputation of nodes can be evaluated by introducing indicators such as credit scoring systems, historical behavior records, and data quality evaluations. At the same time, the incentive mechanism and punishment measures are combined to reward high-reputation nodes and punish low-reputation or malicious nodes, to maintain the stability and trust of the network.

The lack of a reputation management mechanism in the medical blockchain may hinder effective supervision of participating nodes' behavior, thereby exposing the system to potential threats from malicious nodes engaging in malicious activities. Furthermore, the lack of a reputation management mechanism poses challenges in ensuring the quality of data contributed by participating nodes, subsequently impacting the overall credibility and availability of the data. For example, some medical organizations may provide false or incomplete medical data to obtain additional benefits or avoid liability. The lack of a reputation management mechanism will cause the credibility of medical data to be questioned, affecting doctors' judgment of patients' conditions and the formulation of treatment plans. If medical data providers frequently provide false data, it will lead to a crisis of trust in the blockchain medical data-sharing platform, which will in turn affect the healthy development of the entire medical industry.

4.3 Insufficient Incentive Mechanisms

Medical blockchain data-sharing methods typically require incentive mechanisms to encourage participants to actively share data and ensure their cooperation and honest behavior [113]. However, the incentive mechanism in the current research lacks the distinction of participant types, contributions, and other factors, resulting in insufficient incentives for active participants.

In incentive mechanisms for on-chain sharing and on-cloud sharing methods, participants are usually incentivized through encrypted currencies or tokens on the blockchain [59,72]. After contributing electronic medical data and uploading it to the blockchain, participants can receive a certain amount of encrypted currency or tokens as a reward. In local sharing methods, incentive mechanisms can also be designed based on the size or quality evaluation indicators of the data shared by data owners, thus encouraging them to contribute more and better data [85,98]. However, these incentive mechanisms lack consideration of the cooperation and competition relationships among data owners, data requesters, and blockchain miners, resulting in a lack of fairness and difficulty in maximizing benefits for all parties involved. In order to stimulate the initiative of nodes, it is necessary to design a more reasonable and fair incentive mechanism. It can be considered to reward nodes according to their contribution, data quality, activity, and other factors while introducing competition and cooperation mechanisms to promote positive interaction between nodes. In addition, diversified incentive methods can also be explored, such as providing medical service concessions, point exchange, etc., to increase nodes' willingness to participate and loyalty.

The medical blockchain data-sharing method lacks an effective incentive mechanism, which will reduce the enthusiasm of data-sharing participants, make cooperation more difficult, and is not conducive to maintaining the long-term stability of the system [114]. For example, some healthcare organizations may be reluctant to share data for fear of data breach or privacy protection issues; Patients, on the other hand, may be reluctant to provide their medical data because they lack sufficient incentives. Inadequate incentives will lead to a decrease in the willingness of healthcare organizations and patients to share data, which will affect the richness and diversity of healthcare data. If medical data cannot be fully shared and utilized, it will limit doctors' comprehensive understanding of patients' conditions and optimization of treatment plans, which will affect the improvement of medical level.

4.4 Insufficient Security Optimization

To ensure the security, integrity, and reliability of data in medical blockchain data-sharing, it is very important to resist various types of attacks. However, current research still has deficiencies in safety optimization measures. If the security optimization is insufficient, it may face risks such as data leakage and privacy violation. For example, hackers could exploit vulnerabilities in blockchain networks to attack data nodes and steal or tamper with medical data; Or some malicious organization may gain access to sensitive patient information through improper means. Inadequate security optimization will expose medical data to a higher risk of leakage, seriously threatening the privacy of patients and the reputation of medical institutions. If a data breach or privacy violation occurs, it may lead to legal disputes and compensation liabilities, bringing unnecessary economic losses and legal risks to medical institutions and patients.

Since the medical blockchain data-sharing method mainly relies on the blockchain for sharing, most current medical blockchain data-sharing methods have discussed blockchain attacks, such as 51% attacks, bifurcation attacks, and collusion attacks [20]. However, most of the current resistance to block attacks relies on mature consensus algorithms to resist, and does not consider small-scale medical blockchain networks. Therefore, when it is necessary to build a new consensus algorithm according to the needs of actual electronic medical data-sharing, it is necessary to re-evaluate the threat of blockchain attacks.

In the context of electronic medical data transmission, security threats such as eavesdropping, tampering, or man-in-the-middle attacks are common. To address these threats, encryption [54], digital signatures [71], and identity authentication [108] technologies are typically employed to ensure that only authorized users can access and share electronic medical data. However, these technologies may also have shortcomings and face challenges. For instance, encryption algorithms may be susceptible to quantum computing, which could compromise the security of the data. Digital signatures and identity authentication may be vulnerable to identity forgery and replay attacks, which may undermine the integrity and reliability of the data. Man-in-the-middle attacks may also be used to steal or tamper with data by hijacking communications and altering data packets.

Compared with on-chain and on-cloud sharing methods, the method of local sharing not only needs to consider blockchain attacks and data transmission attacks, but also needs to consider attacks against federated learning. Poisoning attack is an attack method against machine learning models, which inserts malicious samples or noise data into the training data to change the learning results of the model [115]. However, the current research on the local data-sharing method does not consider the problem of attack resistance in the initial data sparse state of the system, and lacks immediate resistance to poisoning attacks. This leads to some hidden malicious nodes being selected to participate in federated learning, and then conducting poisoning attacks in the middle round of federated learning. Even if the hidden malicious nodes are exposed after the attack is completed, the damage it causes is irreversible. Inference attack is an attack method that infers the data information of data owners by observing the model parameters transmitted in federated learning [116]. Existing research usually uses differential privacy protection technology to resist, which will lead to a decrease in the accuracy of the model. Although the support vector machine can be added to reduce the impact on model accuracy, it will reduce the operating efficiency and increase the storage pressure of the blockchain.

5 Future Research Directions

In the previous section, we summarized the challenges faced by existing methods. This section proposes some future research directions regarding these challenges.

5.1 Optimize Consensus Algorithm

Combining the process of data-sharing to build a consensus algorithm is a development trend of future medical blockchain data-sharing methods. There are many directions for optimizing consensus algorithms.

The consensus algorithm can be optimized by improving the reliability of data-sharing. For example, Zhang et al. [49] designed a Proof of Conformance consensus algorithm that requires participants to provide proof of the consistency of medical data and indexes before new blocks can be added to the chain. At the same time, optimizing the consensus algorithm from the perspective of reducing data-sharing energy consumption and network congestion is also a feasible solution. For example, Fan et al. [64] designed a hybrid consensus mechanism that can select endorsement nodes and submit transactions in turn to improve the efficiency of data-sharing.

Furthermore, based on the training and aggregation process of federated learning, it is necessary to design a consensus algorithm that is low in energy consumption and can be combined with the federated learning process. For example, the trust degree and data quality of the data owners in federated learning can also be considered proof of the consensus algorithm [99]. Mining nodes are selected by evaluating local updates of data owners to determine their quality and contribution to federated learning. After the mining node generates a new block, other nodes reach a consensus by verifying the evaluation results of the mining node, and then uploading the new block to the chain. In this context, we can further combine the ideas of mature consensus algorithms such as PoW, PoS, and PBFT to develop new low-energy, efficient, and safe consensus algorithms.

5.2 Design Reputation Management Mechanisms

The design and implementation of the reputation management mechanism need to fully consider the privacy and security protection requirements of electronic medical data to ensure that the privacy of participants is protected and avoid potential data leakage and abuse risks.

Therefore, Zou et al. [63] used the Chameleon hash function to construct key blocks and micro-blocks, and designed a reputation mechanism based on this to prevent reputation fraud attacks. Furthermore, encryption technology can be used to protect the participant's reputation score and transaction records, ensuring the confidentiality and integrity of the data. Digital signatures can be used to verify the identity of participants and the authenticity of data, preventing the forgery of reputation scores or tampering with transaction records. Smart contracts can be used to automatically enforce reputation management rules [117], ensuring fair and transparent reputation evaluation and management.

Combining reputation management mechanisms with other mechanisms in the medical blockchain is also a feasible research direction in the future. For example, Lian et al. [118] selected mining nodes for consensus based on reputation, thereby eliminating potential risks. Besides, reputation management mechanisms can be integrated with consensus algorithms or federated learning aggregation algorithms, and the reputation value of participants can be utilized as a weight for their involvement in the consensus process or federated learning aggregation process. At the same time, reputation management mechanisms can also be combined with trust management mechanisms to encourage participants to follow rules and maintain a good reputation. Participants with reputation values higher than the initial value can be given priority access rights, data usage rights, or the right to participate in shared decision-making. Participants with reputation values lower than the initial value should be punished by limiting their participation in sharing.

5.3 Improve Incentive Mechanism

The development of incentive mechanisms is a dynamic process that necessitates continuous adjustment and optimization based on participant performance and the data-sharing environment.

To enhance incentive mechanisms in medical blockchain data-sharing, game theory can be utilized to create cooperative game models among participants that allocate incentives fairly. Such as Shen et al. [119] used Shapley values to build a dynamic and fair incentive scheme for data-sharing in multi-cloud, and built a revenue distribution model. Cooperative game models can take into account aspects such as participant cooperation and contribution, as well as data quality and quantity to equitably distribute incentives and encourage active data-sharing. Furthermore, since participants in medical blockchain data-sharing may be competitive and self-interested, non-cooperative game models like Stackelberg games or Nash games can also be employed to improve incentive mechanisms [120]. These models can offer optimal strategies based on the interests and goals of each participant, guiding them to make more informed decisions when sharing data.

Integrating a reputation mechanism with the incentive mechanism can improve the latter by regularly distributing incentives based on reputation values [119]. This can help to maintain participants' enthusiasm and cooperative behavior over the long term, with high-reputation participants receiving proportionally higher incentives. And those participants who provide false data will receive incentive penalties. Implementing this method can enhance the efficiency of data-sharing, and maintain the security and reliability of medical blockchains.

5.4 Improve Security Optimization

The existing medical blockchain data-sharing methods encounter security threats on three fronts: blockchain, data transmission, and federated learning. The following outlines potential security optimization methods to address these threats in the future:

Security threats in the blockchain, such as collusion attacks, can be resisted by regularly checking the security of the consensus algorithm and introducing external verification mechanisms. For example, Guo et al. [62] can resist $N-1$ collusion attacks by sharing the secret pseudorandom function seeds among authorities. Furthermore, a strict participant verification and authorization mechanism can be established to limit the permissions of participants and monitor their behavior to prevent collusion attacks from occurring.

To bolster the security of data transmission, privacy protection technologies such as anonymization, de-identification, and differential privacy can be leveraged to safeguard the data slated for sharing. For instance, Chen et al. [75] employed K-anonymity technology to preprocess shared data, while Wang et al. [102] proposed a periodic aggregation method coupled with a differential privacy mechanism to fortify the privacy of shared model parameters. Furthermore, establishing a legal and compliant data use authorization mechanism is recommended, encompassing explicit data use purposes, access control, and data use auditing.

Local sharing methods in medical blockchain need to take into account both data security and sharing efficiency when resisting attacks against federated learning, such as poisoning attacks and inference attacks. For example, Rehman et al. [106] built an intrusion detection system to detect attacks before sharing. Wang et al. [107] designed a smart contract that can evaluate the performance of model parameters to automatically detect attacks and punish malicious nodes. In addition, the current research on the local data-sharing method lacks the prevention of cheating data owners. These cheating data owners will copy the updates of other nodes, thus affecting the training efficiency of federated learning. It can be considered to combine zero-knowledge proof and encryption technology to prevent cheating data owners from interfering with federated learning training while ensuring the privacy of parameter updates.

6 Conclusions

The use of medical blockchain for data-sharing has garnered significant attention and is rapidly evolving. However, the implementation methods of medical blockchain are diverse and complex, lacking systematic organization. This paper classifies current medical blockchain data-sharing methods into three categories based on the storage location of the original electronic medical data during data-sharing: on-chain sharing, on-cloud sharing, and local sharing. The paper then provides a detailed introduction to the operation processes of these three medical blockchain data-sharing methods, as well as a summary of the current research characteristics of each implementation. Finally, the paper analyzes the challenges faced by current medical blockchain data-sharing methods and identifies future research directions. This paper provides a comprehensive analysis of medical blockchain data-sharing methods from a novel perspective, not only discussing the well-established on-chain and on-cloud sharing but also exploring the hot topic of local sharing based on federated learning. Through a comprehensive review and analysis of these existing medical blockchain data-sharing methods, valuable references and guidance can be provided for future electronic medical data-sharing research.

Acknowledgement: The authors are grateful to the anonymous reviewers and the editor for their valuable comments and suggestions.

Funding Statement: This work was supported by the Guangxi Science and Technology Project (No. AB24010317).

Author Contributions: The authors confirm contribution to the paper as follows: Chenquan Gan: Conceptualization, Methodology, Validation, Writing—original draft; Xinghai Xiao: Writing—original draft, Formal analysis; Qingyi Zhu, Deepak Kumar Jain, and Akanksha Saini: Supervision, Writing—review & editing. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa and A. H. Gandomi, "Insights into internet of medical things (IoMT): Data fusion, security issues and potential solutions," *Inf. Fusion*, vol. 102, no. 4, 2024, Art. no. 102060. doi: 10.1016/j.inffus.2023.102060.

[2] J. Wiens and E. S. Shenoy, "Machine learning for healthcare: On the verge of a major shift in healthcare epidemiology," *Clin. Infect. Dis.*, vol. 66, no. 1, pp. 149–153, 2018. doi: 10.1093/cid/cix731.

[3] N. H. Shah, A. Milstein, and S. C. Bagley, "Making machine learning models clinically useful," *JAMA*, vol. 322, no. 14, pp. 1351–1352, 2019. doi: 10.1001/jama.2019.10306.

[4] B. Shickel, P. J. Tighe, A. Bihorac, and P. Rashidi, "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record (EHR) analysis," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 5, pp. 1589–1604, 2017. doi: 10.1109/JBHI.2017.2767063.

[5] A. Rauniyar *et al.*, "Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7374–7398, 2024. doi: 10.1109/JIOT.2023.3329061.

[6] Y. Sun, J. Liu, K. Yu, M. Alazab, and K. Lin, "PMRSS: Privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 1981–1990, 2021. doi: 10.1109/TII.2021.3070544.

[7] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 9, pp. 2499–2505, 2020. doi: 10.1109/JBHI.2020.2973467.

[8] M. Alhanahnah, P. Bertok, and Z. Tari, "Trusting cloud service providers: Trust phases and a taxonomy of trust factors," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 44–54, 2017. doi: 10.1109/MCC.2017.20.

[9] L. Yang, Q. Zheng, and X. Fan, "RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks," in *IEEE INFOCOM 2017-IEEE Conf. Comput. Commun.*, 2017, pp. 1–9.

[10] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2062–2074, 2018. doi: 10.1109/TIFS.2018.2809679.

[11] H. Li, Y. Yang, Y. Dai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," *IEEE Trans. Cloud Comput.*, vol. 8, no. 2, pp. 484–494, 2017. doi: 10.1109/TCC.2017.2769645.

[12] M. Chiregi and N. J. Navimipour, "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms," *J. Electr. Sys. Inform. Technol.*, vol. 5, no. 3, pp. 608–622, 2018. doi: 10.1016/j.jesit.2017.09.001.

[13] M. Chen, Y. Qian, J. Chen, K. Hwang, S. Mao and L. Hu, "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing," *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1274–1283, 2016. doi: 10.1109/TCC.2016.2617382.

[14] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," *Future Gener. Comput. Syst.*, vol. 78, no. 3, pp. 1020–1026, 2018. doi: 10.1016/j.future.2016.12.027.

[15] A. Pugazhenthi and D. Chitra, "Data access control and secured data sharing approach for health care data in cloud environment," *J. Med. Syst.*, vol. 43, no. 8, p. 258, 2019. doi: 10.1007/s10916-019-1381-7.

[16] S. Chandrasekhar, A. Ibrahim, and M. Singhal, "A novel access control protocol using proxy signatures for cloud-based health information exchange," *Comput. Secur.*, vol. 67, no. 4, pp. 73–88, 2017. doi: 10.1016/j.cose.2017.02.008.

[17] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health cloud: Opportunities and challenges," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012. doi: 10.3390/fi4030621.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, vol. 4, 2008, Art. no. 21260.

[19] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, 2018, Art. no. 470. doi: 10.3390/sym10100470.

[20] A. Alsunbul, W. Elmedany, and H. Al-Ammal, "Blockchain application in healthcare industry: Attacks and countermeasures," in *2021 Int. Conf. Data Anal. Bus. Ind. (ICDABI)*, 2021, pp. 621–629.

[21] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017. doi: 10.1109/ACCESS.2017.2730843.

[22] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–27, 2020.

[23] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, 2020, Art. no. 94. doi: 10.3390/electronics9010094.

[24] R. D. Garcia, G. Ramachandran, and J. Ueyama, "Exploiting smart contracts in PBFT-based blockchains: A case study in medical prescription system," *Comput. Netw.*, vol. 211, no. 2, 2022, Art. no. 109003. doi: 10.1016/j.comnet.2022.109003.

[25] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019. doi: 10.1109/ACCESS.2019.2916503.

[26] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Inform.*, vol. 142, 2020, Art. no. 104246. doi: 10.1016/j.ijmedinf.2020.104246.

[27] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020. doi: 10.1109/ACCESS.2020.2969881.

[28] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *Int. J. Healthc. Manag.*, vol. 15, no. 1, pp. 70–83, 2022. doi: 10.1080/20479700.2020.1843887.

[29] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Netw.*, vol. 2, no. 9, pp. 130–139, 2021. doi: 10.1016/j.ijin.2021.09.005.

[30] M. S. Rahman, M. A. Islam, M. A. Uddin, and G. Stea, "A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges," *Internet Things*, vol. 19, no. 8, 2022, Art. no. 100551. doi: 10.1016/j.iot.2022.100551.

[31] A. Zakzouk, A. El-Sayed, and E. E. -D. Hemdan, "A blockchain-based electronic medical records management framework in smart healthcare infrastructure," *Multimed. Tools Appl.*, vol. 82, no. 23, pp. 1–19, 2023. doi: 10.1007/s11042-023-15152-z.

[32] B. S. Egala, A. K. Pradhan, P. Dey, V. Badarla, and S. P. Mohanty, "Fortified-Chain 2.0: Intelligent blockchain for decentralized smart healthcare system," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12308–12321, 2023. doi: 10.1109/JIOT.2023.3247452.

[33] T. Benil and J. Jasper, "Blockchain based secure medical data outsourcing with data deduplication in cloud environment," *Comput. Commun.*, vol. 209, no. 5, pp. 1–13, 2023. doi: 10.1016/j.comcom.2023.06.013.

[34] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. Alabdulatif, "A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data," *Comput. Biol. Med.*, vol. 167, no. 3, 2023, Art. no. 107630. doi: 10.1016/j.compbiomed.2023.107630.

[35] Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao and J. Yearwood, "Blockchain-enabled federated learning: A survey," *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–35, 2022.

[36] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–34, 2019.

[37] J. Konečný, H. B. McMahan, F. Yu, P. Richtarik, A. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," in *Proc. 29th Conf. Neural Inf. Process. Syst. (NIPS)*, Barcelona, Spain, 2016, pp. 5–10.

[38] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for internet of things: Recent advances and future challenges," *Comput. Secur.*, vol. 108, no. 5, 2021, Art. no. 102355. doi: 10.1016/j.cose.2021.102355.

[39] C. Gan, X. Xiao, Q. Zhu, D. K. Jain, A. Saini and A. Hussain, "Federated learning-driven dual blockchain for data sharing and reputation management in internet of medical things," *Expert. Syst.*, vol. 21260, 2024, Art. no. e13714. doi: 10.1111/exsy.13714.

[40] P. Xi, X. Zhang, L. Wang, W. Liu, and S. Peng, "A review of blockchain-based secure sharing of healthcare data," *Appl. Sci.*, vol. 12, no. 15, 2022, Art. no. 7912. doi: 10.3390/app12157912.

[41] J. Młodawski, M. Mlodawska, M. Sikorski, and G. Swiercz, "The use of blockchain technology in medicine. Literature review and future perspectives," *Med. Stud.*, vol. 39, no. 3, pp. 304–309, 2023. doi: 10.5114/ms.2023.131676.

[42] A. Dubovitskaya, P. Novotny, Z. Xu, and F. Wang, "Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review," *Oncology*, vol. 98, no. 6, pp. 403–411, 2020. doi: 10.1159/000504325.

[43] V. C. Osamor, I. B. Edosomwan, and O. O. Damilola, "Application of blockchain technology for data privacy and secured sharing in electronic medical records: A systematic literature review," in *2024 Int. Conf. Sci., Eng. Bus. Driving Sustain. Dev. Goals (SEB4SDG)*, IEEE, 2024, pp. 1–12.

[44] H. R. Rahal, S. Slatnia, O. Kazar, and E. Barka, "Blockchain for medical security data: A review and perspectives," in *2023 Int. Conf. Adv. Electron., Control Commun. Syst. (ICAECCS)*, IEEE, 2023, pp. 1–6.

[45] S. Vinchurkar, S. Kediya, T. Somnathe, Y. Sure, A. Agrawal and K. Ingole, "Revolutionizing healthcare data management: A comprehensive review of blockchain application," in *2023 Int. Conf. Commun. Secur. Artif. Intell. (ICCSAI)*, IEEE, 2023, pp. 506–510.

[46] S. A. Deshmukh, S. L. Kasar, and Y. Chichani, "Analysis of challenges in decentralized storage framework for sharing medical data," in *2023 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, IEEE, 2023, pp. 1–10.

[47] R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," *IEEE Trans. Serv. Comput.*, vol. 15, no. 6, pp. 3668–3686, 2021. doi: 10.1109/TSC.2021.3085913.

[48] J. -S. Lee, C. -J. Chew, J. -Y. Liu, Y. -C. Chen, and K. -Y. Tsai, "Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract," *J. Inf. Secur. Appl.*, vol. 65, no. 1, 2022, Art. no. 103117. doi: 10.1016/j.jisa.2022.103117.

[49] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, 2018. doi: 10.1007/s10916-018-0995-5.

[50] G. Al-Sumaidaee, R. Alkhudary, Z. Zilic, and A. Swidan, "Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare," *Inf. Process. Manag.*, vol. 60, no. 2, 2023, Art. no. 103160. doi: 10.1016/j.ipm.2022.103160.

[51] R. Johari, V. Kumar, K. Gupta, and D. P. Vidyarthi, "BLOSOM: BLOckchain technology for Security Of Medical records," *ICT Express*, vol. 8, no. 1, pp. 56–60, 2022. doi: 10.1016/j.icte.2021.06.002.

[52] P. Sharma, S. Namasudra, R. G. Crespo, J. Parra-Fuente, and M. C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Inf. Sci.*, vol. 629, no. 3s, pp. 703–718, 2023. doi: 10.1016/j.ins.2023.01.148.

[53] G. Xu *et al.*, "A privacy-preserving medical data sharing scheme based on blockchain," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 698–709, 2023. doi: 10.1109/JBHI.2022.3203577.

[54] S. Shamshad, K. Mahmood, S. Kumari, and C. -M. Chen, "A secure blockchain-based e-health records storage and sharing scheme," *J. Inf. Secur. Appl.*, vol. 55, no. 10, 2020, Art. no. 102590. doi: 10.1016/j.jisa.2020.102590.

[55] M. S. Rahman, A. Alabdulatif, and I. Khalil, "Privacy aware internet of medical things data certification framework on healthcare blockchain of 5G edge," *Comput. Commun.*, vol. 192, no. 4, pp. 373–381, 2022. doi: 10.1016/j.comcom.2022.06.013.

[56] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019. doi: 10.1109/ACCESS.2019.2937685.

[57] G. Wu, S. Wang, and Z. Ning, "Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8091–8104, 2021. doi: 10.1109/JIOT.2021.3138104.

[58] A. A. Abdellatif *et al.*, "Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15762–15775, 2021. doi: 10.1109/JIOT.2021.3052910.

[59] G. Wu, S. Wang, Z. Ning, and B. Zhu, "Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system," *IEEE J. Biomed. Health Inform.*, vol. 26, no. 5, pp. 1917–1927, 2021. doi: 10.1109/JBHI.2021.3123643.

[60] Z. Qu, Z. Zhang, and M. Zheng, "A quantum blockchain-enabled framework for secure private electronic medical records in internet of medical things," *Inf. Sci.*, vol. 612, no. 3, pp. 942–958, 2022. doi: 10.1016/j.ins.2022.09.028.

[61] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf. Sci.*, vol. 485, no. 3, pp. 427–440, 2019. doi: 10.1016/j.ins.2019.02.038.

[62] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018. doi: 10.1109/ACCESS.2018.2801266.

[63] R. Zou, X. Lv, and J. Zhao, "SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system," *Inf. Process. Manag.*, vol. 58, no. 4, 2021, Art. no. 102604. doi: 10.1016/j.ipm.2021.102604.

[64] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–11, 2018. doi: 10.1007/s10916-018-0993-7.

[65] C. Gan, H. Yang, Q. Zhu, Y. Zhang, and A. Saini, "An encrypted medical blockchain data search method with access control mechanism," *Inf. Process. Manag.*, vol. 60, no. 6, 2023, Art. no. 103499. doi: 10.1016/j.ipm.2023.103499.

[66] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, 2020. doi: 10.1109/JIOT.2020.3032997.

[67] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019. doi: 10.1109/ACCESS.2019.2917555.

[68] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, 2017, Art. no. 44. doi: 10.3390/info8020044.

[69] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *J. Med. Syst.*, vol. 44, no. 2, 2020, Art. no. 52. doi: 10.1007/s10916-019-1468-1.

[70] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang and X. Jia, "MedShare: A privacy-preserving medical data sharing system by using blockchain," *IEEE Trans. Serv. Comput.*, vol. 16, no. 1, pp. 438–451, 2023.

[71] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020. doi: 10.1109/ACCESS.2020.2976894.

[72] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei and H. Lu, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 271–281, 2021. doi: 10.1109/TNSE.2021.3101842.

[73] W. Dai, S. Tuo, L. Yu, K. -K. R. Choo, D. Zou and H. Jin, "HAPPS: A hidden attribute and privilege-protection data-sharing scheme with verifiability," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25538–25550, 2022. doi: 10.1109/JIOT.2022.3197708.

[74] Z. Pang, Y. Yao, Q. Li, X. Zhang, and J. Zhang, "Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm," *IEEE Access*, vol. 10, no. 9, pp. 87803–87815, 2022. doi: 10.1109/ACCESS.2022.3186682.

[75] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 5, pp. 1–12, 2021. doi: 10.1016/j.comcom.2021.04.028.

[76] J. Zhang, Y. Yang, X. Liu, and J. Ma, "An efficient blockchain-based hierarchical data sharing for healthcare internet of things," *IEEE Trans. Ind. Inform.*, vol. 18, no. 10, pp. 7139–7150, 2022. doi: 10.1109/TII.2022.3145851.

[77] C. Li *et al.*, "Efficient medical big data management with keyword-searchable encryption in healthchain," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5521–5532, 2022. doi: 10.1109/JSYST.2022.3173538.

[78] E. J. De Aguiar, A. J. Dos Santos, R. I. Meneguette, E. Robson, and J. Ueyama, "A blockchain-based protocol for tracking user access to shared medical imaging," *Future Gener. Comput. Syst.*, vol. 134, no. 2, pp. 348–360, 2022. doi: 10.1016/j.future.2022.04.017.

[79] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," *Egypt. Inform. J.*, vol. 23, no. 2, pp. 329–343, 2022. doi: 10.1016/j.eij.2022.02.004.

[80] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021. doi: 10.1109/JIOT.2021.3058946.

[81] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distr. Comput.*, vol. 164, no. 8, pp. 152–167, 2022. doi: 10.1016/j.jpdc.2022.03.009.

[82] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," *IEEE Trans. Eng. Manag.*, vol. 68, no. 6, pp. 1677–1689, 2020. doi: 10.1109/TEM.2020.2966832.

[83] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, "Secure decentralized electronic health records sharing system based on blockchains," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5045–5058, 2022. doi: 10.1016/j.jksuci.2021.05.002.

[84] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions," *Secur. Priv.*, vol. 4, no. 5, 2021, Art. no. e162. doi: 10.1002/spy2.162.

[85] A. A. Noman, M. Rahaman, T. H. Pranto, and R. M. Rahman, "Blockchain for medical collaboration: A federated learning-based approach for multi-class respiratory disease classification," *Healthcare Anal.*, vol. 3, no. 5, 2023, Art. no. 100135. doi: 10.1016/j.health.2023.100135.

[86] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Stat.*, 2017, pp. 1273–1282.

[87] L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng and D. Liu, "Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records," *J. Biomed. Inform.*, vol. 99, no. 9, 2019, Art. no. 103291. doi: 10.1016/j.jbi.2019.103291.

[88] N. Rieke *et al.*, "The future of digital health with federated learning," *npj Digit. Med.*, vol. 3, no. 1, 2020, Art. no. 119. doi: 10.1038/s41746-020-00323-1.

[89] J. Passerat-Palmbach *et al.*, "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data," in *2020 IEEE Int. Conf. Blockchain (Blockchain)*, 2020, pp. 550–555.

[90] D. C. Nguyen *et al.*, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, 2021. doi: 10.1109/JIOT.2021.3072611.

[91] H. Kim, J. Park, M. Bennis, and S. -L. Kim, "Blockchained on-device federated learning," *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, 2019. doi: 10.1109/LCOMM.2019.2921755.

[92] P. Das, M. Singh, and D. G. Roy, "A secure softwarized blockchain-based federated health alliance for next generation iot networks," in *2021 IEEE Globecom Workshops (GC Wkshps)*, 2021, pp. 1–6.

[93] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology," *Future Gener. Comput. Syst.*, vol. 129, no. 2, pp. 380–388, 2022. doi: 10.1016/j.future.2021.11.028.

[94] O. El Rifai, M. Biotteau, X. de Boissezon, I. Megdiche, F. Ravat and O. Teste, "Blockchain-based federated learning in medicine," in *Artif. Intell. Med.: 18th Int. Conf. Artif. Intell. Med., AIME 2020*, Minneapolis, MN, USA, 2020, pp. 214–224.

[95] X. Chen, T. Wang, and S. Zhang, "The design of reputation system for blockchain-based federated learning," in *2021 Int. Conf. Artif. Intell. Blockchain Technol. (AIBT)*, 2021, pp. 114–120.

[96] X. Wang, Y. Zhao, C. Qiu, Z. Liu, J. Nie and V. C. Leung, "InFEDge: A blockchain-based incentive mechanism in hierarchical federated learning for end-edge-cloud communications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3325–3342, 2022. doi: 10.1109/JSAC.2022.3213323.

[97] L. Sun, J. Wu, Y. Xu, and Y. Zhang, "A federated learning and blockchain framework for physiological signal classification based on continual learning," *Inf. Sci.*, vol. 630, pp. 586–598, 2023. doi: 10.1016/j.ins.2023.02.003.

[98] O. Samuel *et al.*, "IoMT: A COVID-19 healthcare system driven by federated learning and blockchain," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 823–834, 2023. doi: 10.1109/JBHI.2022.3143576.

[99] Y. Chen, F. Lin, Z. Chen, C. Tang, R. Jia and M. Li, "Blockchain-based federated learning with contribution-weighted aggregation for medical data modeling," in *2022 IEEE 19th Int. Conf. Mobile Ad Hoc Smart Syst. (MASS)*, 2022, pp. 606–612.

[100] H. Jin, X. Dai, J. Xiao, B. Li, H. Li and Y. Zhang, "Cross-cluster federated learning and blockchain for internet of medical things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15776–15784, 2021. doi: 10.1109/JIOT.2021.3081578.

[101] D. Połap, G. Srivastava, and K. Yu, "Agent architecture of an intelligent medical system based on federated learning and blockchain technology," *J. Inf. Secur. Appl.*, vol. 58, no. 11, 2021, Art. no. 102748. doi: 10.1016/j.jisa.2021.102748.

[102] H. Wang, X. Zhang, Y. Xia, and X. Wu, "An intelligent blockchain-based access control framework with federated learning for genome-wide association studies," *Comput. Stand. Interfaces*, vol. 84, no. 3, 2023, Art. no. 103694. doi: 10.1016/j.csi.2022.103694.

[103] R. Kumar *et al.*, "Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging," *IEEE Sens. J.*, vol. 21, no. 14, pp. 16301–16314, 2021. doi: 10.1109/JSEN.2021.3076767.

[104] T. Hai, J. Zhou, S. R. Srividhya, S. K. Jain, P. Young and S. Agrawal, "BVFLEMR: An integrated federated learning and blockchain technology for cloud-based medical records recommendation system," *J. Cloud Comput.*, vol. 11, no. 1, p. 22, 2022. doi: 10.1186/s13677-022-00294-6.

[105] Z. A. E. Houda, A. S. Hafid, L. Khoukhi, and B. Brik, "When collaborative federated learning meets blockchain to preserve privacy in healthcare," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2455–2465, 2023. doi: 10.1109/TNSE.2022.3211192.

[106] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, 2022, Art. no. 106019. doi: 10.1016/j.compbiomed.2022.106019.

[107] Z. Wang, B. Yan, and Y. Yao, "Blockchain empowered federated learning for medical data sharing model," in *Wirel. Algorithms, Syst. Appl.: 16th Int. Conf., WASA 2021*, Nanjing, China, 2021, pp. 537–544.

[108] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 1080–1087, 2022. doi: 10.1109/TII.2022.3189170.

[109] A. Lakhan *et al.*, "Federated-learning based privacy preservation and fraud-enabled blockchain iomt system for healthcare," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 664–672, 2023. doi: 10.1109/JBHI.2022.3165945.

[110] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020. doi: 10.1109/ACCESS.2020.3037474.

[111] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," in *Self-Published Paper*, 2012, vol. 19, no. 1, pp. 1–6.

[112] E. Androulaki *et al.*, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. Thirteenth EuroSys Conf.*, 2018, pp. 1–15.

[113] C. Gan, A. Saini, Q. Zhu, Y. Xiang, and Z. Zhang, "Blockchain-based access control scheme with incentive mechanism for ehealth systems: Patient as supervisor," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 30605–30621, 2021. doi: 10.1007/s11042-020-09322-6.

[114] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? A survey," *ACM Comput. Surv.*, vol. 55, no. 7, pp. 1–38, 2022. doi: 10.1145/3594869.

[115] R. S. Antunes, C. André da Costa, A. Küderle, I. A. Yari, and B. Eskofier, "Federated learning for healthcare: Systematic review and architecture proposal," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, pp. 1–23, 2022. doi: 10.1145/3501813.

[116] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *2019 IEEE Symp. Secur. Priv. (SP)*, 2019, pp. 691–706.

[117] A. Jamal, M. U. Javed, N. Alrajeh, S. H. Bouk, and N. Javaid, "Blockchain based reputation management, data storage and distributed revocation in vehicular energy networks in smart health care systems," *Cluster Comput.*, vol. 27, no. 2, pp. 2151–2163, 2024.

[118] Z. Lian, W. Wang, Z. Han, and C. Su, "Blockchain-based personalized federated learning for internet of medical things," *IEEE Trans. Sustain. Comput.*, vol. 8, no. 4, pp. 694–702, 2023. doi: 10.1109/TSUSC.2023.3279111.

[119] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1229–1241, 2020. doi: 10.1109/JSAC.2020.2986619.

[120] W. Liu, B. Cao, L. Zhang, M. Peng, and M. Daneshmand, "A distributed game theoretic approach for blockchain-based offloading strategy," in *ICC 2020-2020 IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6.