cryptography

MDPI

Review

The Role of Blockchain in Medical Data Sharing

Hamed Taherdoost [1,2,3]

[1] Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6Z 0E5, Canada; hamed.taherdoost@gmail.com or hamed@hamta.org; Tel.: +1-236-889-5359

[2] Research and Development Department, Hamta Group, Hamta Business Corporation, Vancouver, BC V5Z 2C4, Canada

[3] College of Technology and Engineering, Westcliff University, Irvine, CA 92614, USA

Abstract: As medical technology advances, there is an increasing need for healthcare providers all over the world to securely share a growing volume of data. Blockchain is a powerful technology that allows multiple parties to securely access and share data. Given the enormous challenge that healthcare systems face in digitizing and sharing health records, it is not unexpected that many are attempting to improve healthcare processes by utilizing blockchain technology. By systematically examining articles published from 2017 to 2022, this review addresses the existing gap by methodically discussing the state, research trends, and challenges of blockchain in medical data exchange. The number of articles on this issue has increased, reflecting the growing importance and interest in blockchain research for medical data exchange. Recent blockchain-based medical data sharing advances include safe healthcare management systems, health data architectures, smart contract frameworks, and encryption approaches. The evaluation examines medical data encryption, blockchain networks, and how the Internet of Things (IoT) improves hospital workflows. The findings show that blockchain can improve patient care and healthcare services by securely sharing data.

Keywords: healthcare; data sharing; blockchain; encryption

check for updates

Citation: Taherdoost, H. The Role of Blockchain in Medical Data Sharing. *Cryptography* **2023**, *7*, 36. https://doi.org/10.3390/cryptography7030036

Academic Editor: William Puech

Received: 6 June 2023
Revised: 6 July 2023
Accepted: 10 July 2023
Published: 12 July 2023

1. Introduction

Everyone may benefit from healthcare data. It maintains a record of our bodily characteristics. It is essential for the treatment and diagnosis of disorders [1]. With the fast growth of artificial intelligence (AI), health records have become a tremendous advantage. It may assist in the development of AI diagnostic models and aid in the diagnosing process. Even while the recording of medical data has moved from paper data to electronic medical records (EMRs), which are more convenient for data storage and access, more attention needs to be placed on data privacy [2]. Several institutions and hospitals have curtailed data transmission and exchange to prevent data privacy breaches, which has resulted in the establishment of data silos as medical information is dispersed among numerous healthcare institutions [3].

The sharing of medical data provides numerous benefits to diverse stakeholders. Sharing data among clinical organizations, hospitals, and healthcare providers, for example, improves patient care coordination by providing comprehensive medical histories, allowing for more informed decisions and preventing unnecessary testing [4]. In emergencies, data sharing between hospitals and emergency medical services can expedite care, as immediate access to vital patient information enables responders to administer appropriate treatment, thereby reducing delays and enhancing patient outcomes [5]. The integration of medical data sharing with smart homes and Internet of Things (IoT) devices enables remote patient monitoring, which is advantageous for patients with chronic conditions and enables proactive healthcare delivery [6]. In addition, collaborative data sharing between institutions promotes medical research and scientific discoveries, facilitating the identification of patterns, risk factors, and the development of new treatments.

Today's data storage is accessible on the cloud rather than on paper in the era of digitalization. At hospitals and medical institutes, information is stored using computerized private databases [7]. As patients shift hospitals for personal reasons, these data disperse among the many hospitals, and when a patient wants these data for investigations, they lose all of their data and are unable to provide their medical history for the studies. Owing to the absence of consistent data exchange and administration, interoperability across hospitals becomes a challenge. The second difficulty comes when physicians are unable to access prior-treatment records for patients to plan future diagnoses since the records are held on the previous hospital's proprietary database to protect hospital and patient privacy. Consequently, data searching and sharing have become critical concerns [8,9].

Thus, more specialists and academics are beginning to investigate the issue of the secure exchange of medical data. In the past, with the advent of cloud service [10], the majority of medical institutions have selected a third-party cloud server as a data-sharing platform [11,12]. Nonetheless, these cloud-based apps are often vulnerable to a variety of assaults, such as identity theft, eavesdropping, and data tampering. Even though several firms provide unmonitored cloud servers to safeguard the privacy of data sharing, this centralized storage model is susceptible to single-point assaults.

Healthcare organizations, innovation trendsetters, and people from the healthcare field as a whole are focusing on how to find what is now possible with blockchain and what blockchain may enhance and moderate in the future [13]. Blockchain has the potential to produce a monumental accomplishment in the medical biological system since it can easily acquire explicit adjustments to the healthcare executives of the patient. With the assistance of this invention, the power will return to the people, thereby indicating that individuals will be responsible for maintaining their records, and thus acquiring control over their information [14].

Several surveys, like those by Fang et al. [15], Westphal and Seitz [16], and Kuo et al. [17], have explored the potential applications and benefits of blockchain in healthcare. They cover topics like preserving patient data integrity, privacy, and interoperability, use cases in healthcare management systems, and integrating blockchain with other technologies. Many studies have summarized blockchain-based model implementations. Soltanisehat et al. [18] evaluated many articles published from 2016 to 2020. This article focuses on healthcare sector scenarios rather than merely comparing and summarizing models. Abu-Elezz et al. [19] undertook a model study from a novel angle, examining both the advantages and hazards that technology presents to patients. Saha et al. [20] discuss many blockchain-based healthcare options; however, they do not compare their techniques. The published publications were subjected to a statistical analysis by Hasselgren et al. [21]. Unfortunately, the strategies were not summarized in this study. Jin et al. [22] examined the privacy-preserving exchange of medical data using the blockchain model. The evaluation classifies blockchains as either permissionless or permissioned. The authors then examined the merits and downsides of each blockchain model. Dubovitskaya et al. [23] studied primarily the use of blockchain in cancer medical data, including oncology data exchange and medication traceability. Their research has limitations since it solely analyzes oncology data.

Concerning the existing gap, this review discusses the current state, research trends, and challenges of blockchain in systematic medical data sharing. It examines a variety of blockchain-based healthcare scenarios, compared various techniques, and assesses the potential advantages and disadvantages. This work contributes to the current state of the art in blockchain-based medical data sharing and provides insights for researchers and practitioners in the field by providing a comprehensive overview.

2. Blockchain in Healthcare Overview

A blockchain may be seen as a distributed ledger that allows peers to exchange data [24,25]. It was launched with Bitcoin and resolved a persistent issue: the double-spend problem. With Bitcoin, this is accomplished by a majority consensus of so-called mining nodes and the addition of legitimate transactions to the blockchain. Bitcoin was the first to use blockchain technology. Therefore, introducing a coin is not required to utilize blockchain and develop decentralized apps [26]. This section explains the principles of blockchain technology to facilitate a comprehension of the remainder of this article. To aid the reader in comprehending the blockchain idea, its fundamental properties and building blocks and also their subsequent importance in healthcare will be detailed in the following sections.

2.1. Blockchain

A blockchain may be described as a sequence of time-stamped and cryptographically connected blocks. These blocks are permanently and securely sealed [27]. Each new block added to the end of the chain contains a reference to the content of the preceding block [28]. The shareholders, known as the blockchain's nodes, are arranged in a peer-to-peer (P2P) network. Each node in the network has two keys [29]: a private key used for decrypting messages and allowing the node to read them, and a public key used for encrypting messages transmitted to the node. Hence, the public key encryption process is employed to assure the non-repudiation, irreversibility, and consistency of a blockchain [25]. Messages encrypted with the accompanying public key can only be decrypted with the matching private key. The term for this idea is asymmetric cryptography. While a comprehensive explanation is beyond the scope of this study, more information may be obtained in [29]. The so-called hash, which is created using a cryptographic one-way hash function, is used to connect every block on the blockchain. It also assures the block's compactness, anonymity, and immutability [30].

This leads us to the significance of network nodes. Because the blockchain system is a P2P network, a node may be considered a peer when it begins to connect and interact with other nodes in the network; hence, peer node is the correct term. A full node is, in layman's words, any computer that has the main blockchain client installed and runs a complete copy of the whole blockchain ledger [25]. A user who wishes to interact with the blockchain connects to the network through a node [31]. Miners are a subset of nodes since each miner needs to also run a fully functional node. Each miner is thus a node, but not every node is also a miner. This situation is known from a certain sort of public blockchain using the proof-of-work (PoW) consensus algorithm. Some forms of blockchain networks using different distributed consensus mechanisms, such as proof-of-stake (PoS), do not need mining [32].

Depending on the level of involvement [33], blockchain may be classified into the consortium, private, and public chain. As its name suggests, a public chain is entirely public and open to anybody. Due to the immutability of the data on the chain, public chains are regarded to be entirely decentralized. Participation in the consortium chain is restricted to authorized members, and the write/read rights and participation accounting permissions on the blockchain are constructed by the alliance's norms. The private chain is exclusive to private organizations, and the write and read rights on the blockchain, as well as the permissions to participate in accounting, are constructed by the norms of the private organization. Participating nodes are restricted in reference [34].

2.2. Smart Contracts

Computer protocols known as "smart contracts" allow for the informational distribution, validation, and enforcement of contracts [35]. Smart contracts do not need the verification of a third party, and successful transactions are irrevocable and traceable. Computer software is used to create a legally binding contract that can be automatically executed. A smart contract is a program placed on the blockchain that guarantees the safety and security of transactions in the absence of third-party monitoring [36]. The process of smart contracts is shown in Figure 1. In the smart contract code, predefined response rules and trigger situations are encoded, triggering specific actions automatically when predetermined conditions are met. This eliminates the need for intermediaries and improves the contract execution process's transparency, security, and efficiency. When trigger situations, such as specific dates, events, or conditions, occur, the smart contract implements predefined actions, such as transferring ownership, releasing funds, and updating records. By incorporating blockchain technology into smart contracts, participants gain an increased trust, lower costs, and reduced fraud risks. Combining blockchain technology and smart-contract streamline processes optimizes contract administration and provides a secure and transparent solution for a variety of industries. Table 1 displays the highlights of blockchain-enabled smart contracts.

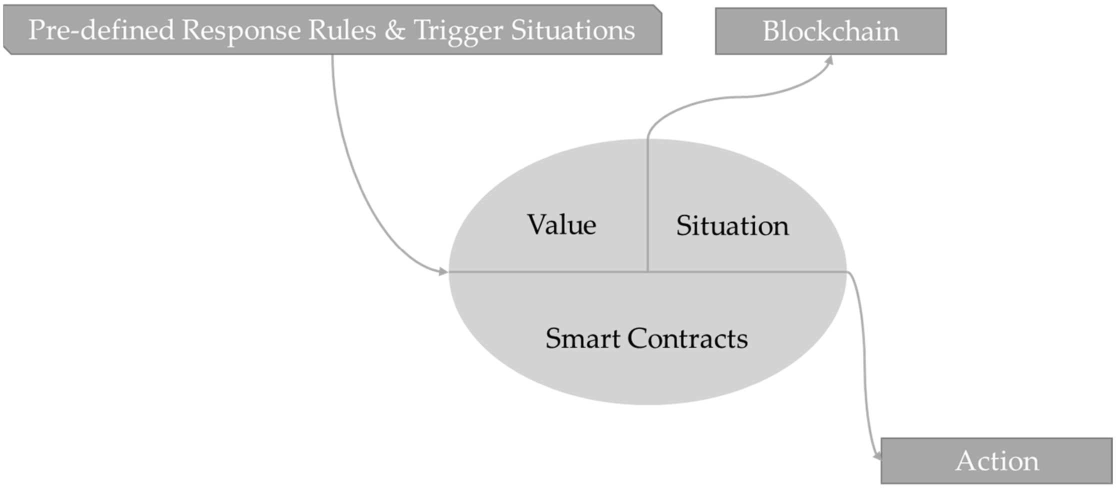

Figure 1. Blockchain in a smart contract process.

Table 1. Features of blockchain-enabled smart contracts.

Features	Description
Untamperable	Smart contracts cannot be changed after deployment. Like a contract, this cannot be changed once signed.
Low cost	Smart contracts do not need a third party to enforce the code after a violation; thus, they are cheaper than regular contracts.
Open and transparent	A smart contract will execute according to the design code and be transparent once deployed.
Decentralized	Computers supervise and arbitrate smart contracts without third-party involvement.

2.3. *Importance of Blockchain in Healthcare*

Blockchain may provide an effective, efficient, safe, and transparent method of data and information communication for all stakeholders involved in the healthcare business [37]. With tokenization and smart contracts, it is possible to decrease or eliminate the pre-authorization procedure in the healthcare industry [38]. While connecting with multiple parties, blockchain-based systems for health documentation protect the security of an individual's data via the use of secure encryption methods [39]. Using the encryption methods, smart contracts, and tokenization used in blockchain network transactions, the pre-authorization method will be drastically streamlined, allowing patients to obtain essential and informed treatment more quickly. This is a consequence of the healthcare provider's ability to immediately obtain pertinent information, whereas previously, they had to rely on the patient or on files physically delivered or emailed from many sources, such as local doctors, laboratories, etc. Not only may tokenization promote a more efficient contact and communication between insurance companies and healthcare practitioners, but it can also support and enhance patient–provider dialogue.

The expansion of the worldwide healthcare business may be aided by blockchain technology, which can also save money and stimulate additional investment in vital resources. With so much at risk, it is inconceivable that the current inefficient, excessively bureaucratic, and failing healthcare business can continue [40]. It is time for executives, practitioners, and patients to embrace the available technological and system-based innovations.

The misuse of available information prevents healthcare organizations from providing appropriate patient care and remarkably improved services. Even though these organizations are economically competent, they are unable to meet the needs of patients. Here are a few facts from Supporting Materials that illustrate this reality. Nowadays, healthcare data breaches in organizations are estimated to cost around USD 380 per compromised record. This amount is anticipated to increase with time. Several healthcare offices still use antiquated frameworks for maintaining patient records. These frameworks are beneficial for keeping patient information records close at hand. This might make it difficult for the professional to analyze, which can be tiresome for both the specialist and the patients. As a result, the cost of maintaining a patient-centered business increases substantially [41,42]. The majority of the present healthcare data infrastructure relies on reputable third parties. In numerous instances, however, they cannot be relied upon. A potential answer to this issue is the blockchain, which depends on consensus and does not need a central authority.

3. Methodology

This study continues by defining the used approach. The systematic study is confined to the subject of medical data sharing.

3.1. Research Questions

The purpose of the study was to address the following research questions (RQs):

- RQ1: How established is blockchain in medical data sharing, and how has this evolved?
- RQ2: What are the latest developments in blockchain-based medical data-sharing research?
- RQ3: What are the issues of using blockchain to share medical data?

3.2. Databases

Included in the systematic review were the following databases:

- Scopus;
- Google Scholar;
- ScienceDirect.

Using the query string(s) listed below, a search for related articles was conducted. Based on the study domain and the established RQs, the search strings were developed. These keywords have been used in the search:

- “Blockchain” AND “Medical data sharing”;

  OR
- “Blockchain” AND “Medical record sharing”;

  OR
- “Blockchain” AND “Healthcare data sharing”;

  OR
- “Blockchain” AND “Health data sharing”;

  OR
- “Blockchain” AND “Health record sharing”;

  OR
- “Blockchain” AND Medical data sharing;

  OR
- “Blockchain” AND Medical record sharing;

  OR

- "Blockchain" AND Healthcare data sharing;

  OR
- "Blockchain" AND Health data sharing;

  OR
- "Blockchain" AND Health record sharing.

The online digital library search was performed on 14 March 2023. The search query was purposely designed to be as comprehensive as feasible to evaluate as many results as possible that were relevant to the research topics given in this systematic review. By searching in the title of the articles, 284 total items were discovered via the main search. Figure 2 shows a summary of the search and selection technique used to choose the articles.

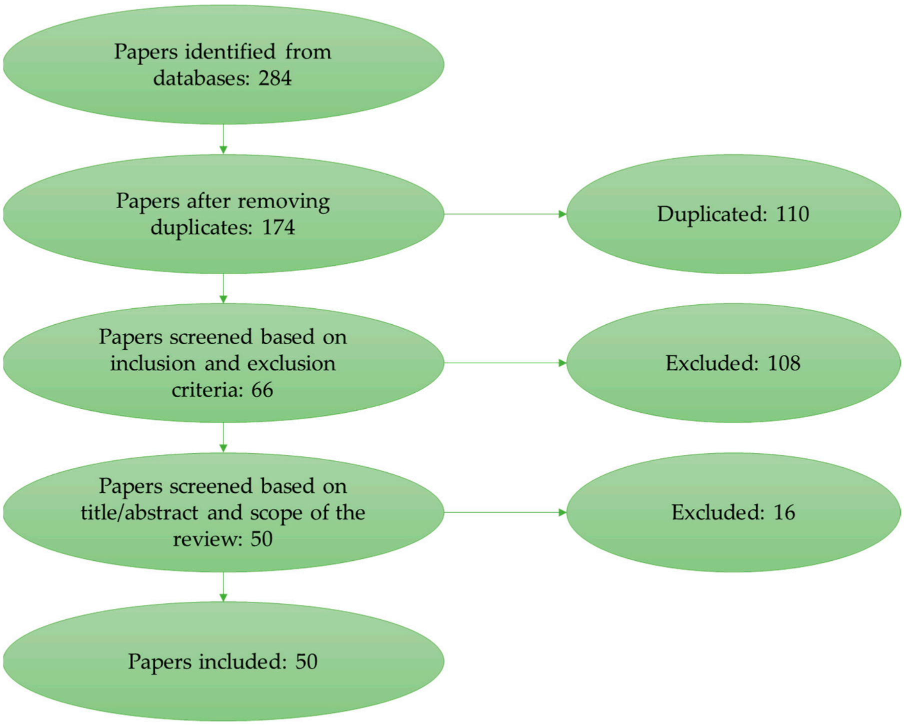
Papers identified from databases: 284
Papers after removing duplicates: 174
Duplicated: 110
Papers screened based on inclusion and exclusion criteria: 66
Excluded: 108
Papers screened based on title/abstract and scope of the review: 50
Excluded: 16
Papers included: 50

Figure 2. Process of study selection.

3.3. Selection of Studies

Depending on the criteria, articles were either included or excluded from the systematic review (Table 2). Fifty papers were ultimately included in the systematic review. To ensure that only high-quality and relevant research was examined, the approach was rigorous.

Table 2. Standards of inclusion and exclusion.

Inclusion Criteria	Exclusion Criteria
1. Publication stage: Final	1. Publication year: Out of the period 2017–2022
2. Document type: Article	2. Language: Not in English
3. Source type: Journal	3. Not focused on blockchain in medical data sharing
4. Article should contain and clearly outline research objectives	4. System design must not be defined properly

3.4. Limitations

One issue is due to the scope of attention; as systematic reviews have a confined focus. Another restriction concerns the study selection, information loss on critical outcomes, incorrect subgroup analysis, and inconsistency with the unique experimental results [43].

Limited databases and the title search query are other limitations of this review. The decision to use only article titles as the search query for this systematic review was motivated by the need to conduct a preliminary investigation of the topic within the limitations of time and resources. This method has several limitations, including the possibility of omitting relevant studies, a reduced precision in the study selection, and the risk of bias.

4. Discussion

RQ1: How established is blockchain in medical data sharing, and how has this evolved?

This systematic review looked for articles published between 2017 and 2022 on the use of blockchain technology in the exchange of medical data. Figure 3 provides a bibliometric summary of the selected articles. Only two articles were published over the years 2017 and 2018. In 2019, four papers were published. The years 2020 and 2021 each have nine items. With 24 papers published in 2022, the growth rate has risen. It contains 48 percent of all papers in this review. This demonstrates that blockchain research in medical data sharing is very important, and expanding, and shows no indication of slowing down. Blockchain enables enterprises to offer proper patient care and provide access to high-quality healthcare services. With this technology, health information exchange, a substantial strain owing to its repetitive nature and time-consuming nature, is swiftly alleviated.

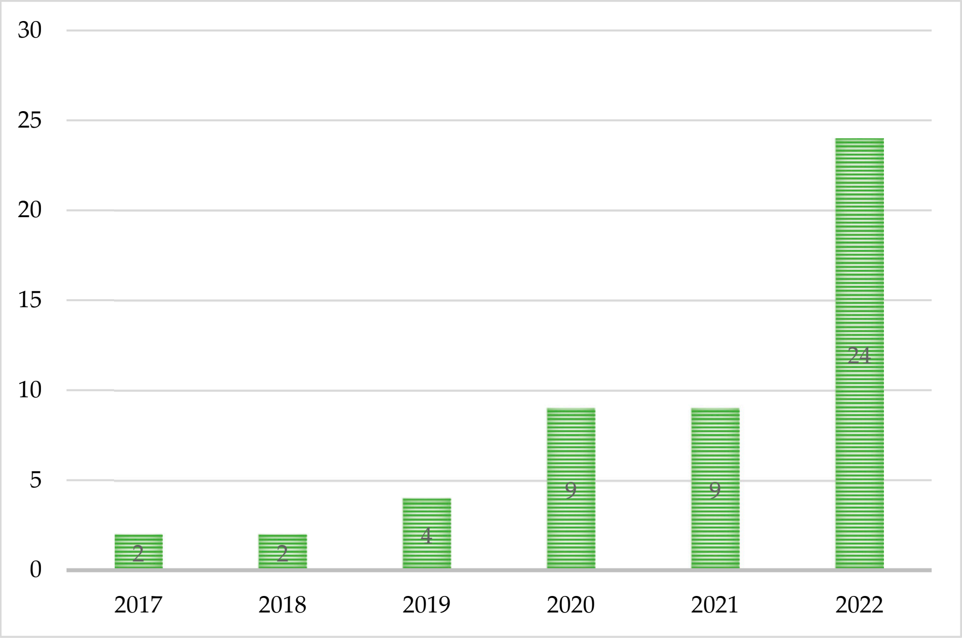

Figure 3. The trend of publishing articles between 2017 and 2022.

Adoption and implementation of blockchain in healthcare systems and organizations for the sharing of medical data should be thoroughly evaluated. Various factors, including regulatory frameworks, technological challenges, interoperability, data protection, and stakeholder acceptance, need to be considered. Several research and development initiatives are investigating the potential of blockchain for medical data sharing, as its popularity and importance have risen dramatically. Initially, research concentrated on the theoretical foundations and viability of blockchain in this domain, resulting in the development of frameworks, methods, and protocols tailored to address the unique challenges of medical data sharing. As the technology advanced, efforts were made to improve the effectiveness and functionality of blockchain in the sharing of medical data, including refining data storage and retrieval, optimizing consensus processes, and exploring integration with other cutting-edge technologies such as edge computing and IoT.

Despite growing interest and research in this area, blockchain technology for the sharing of medical data is still in its infancy. Numerous proposed solutions are still in the experimental or proof-of-concept stages and require additional validation, standardization, and integration with the current healthcare infrastructure. To accomplish a widespread blockchain adoption in the healthcare industry, adoption, regulation, interoperability, and scalability issues need to be resolved. These developments are required to ensure the successful deployment of blockchain technology for the secure and efficient exchange of medical data, which will benefit healthcare stakeholders and facilitate the improvement of healthcare outcomes.

RQ2: What are the latest developments in blockchain-based medical data-sharing research?

There are several instances in which blockchain is utilized to share medical data. Rajput et al. [44] propose a system for healthcare management that leverages blockchain technology to create a tamper-protection application by taking into account secure rules. In an emergency case, these regulations specify extendable access control, auditing, and tamper resistance. Hu et al. [45] propose CrowdMed-II, a blockchain-based health data management architecture that might solve the aforementioned issues with health data. In their framework, they investigate the architecture of significant smart contracts and suggest two smart contract structures. In addition, a unique search contract for searching patients is introduced. They assess their efficacy based on Ethereum's execution costs. The paper by Hashim et al. [46] presents a transaction-based smart contract-triggering method for inter-blockchain communication, allowing the exchange of electronic health records (EHRs) across separate blockchains. They employ local and global smart contracts that will be executed whenever a blockchain-based transaction is generated. Local smart contracts are used to share EHRs inside a blockchain, while global smart contracts are used to share EHRs across blockchains that are independent of one another. Using the Hyperledger Fabric blockchain technology, the experimental setup is executed. In a health federation arrangement, inter-blockchain communication between two separate fabric networks is handled by a global smart contract using Hyperledger Cactus for EHR exchange.

Wu et al. [47] build a blockchain-enabled framework for dynamic access control coupled with local differential privacy (LDP) techniques to offer attribute-based privacy protection in transaction processing. In the framework, they develop four kinds of smart contracts to suit the needs of anonymous transactions, dynamic access control, advantageous matching decisions, and the assessment of disclosed data. To provide granular privacy protection, they categorize critical EMR parameters into distinct tiers and randomize them before data publication using differential privacy budgets. In addition, they create a data quality function that illustrates the disruption caused by LDP-based privacy preferences from the requester's perspective, and they propose suitable many-to-many matching selections among participants for advantageous transactions. Specifically in the study by Kumar et al. [48], deep learning and permissioned blockchain uses a blockchain system to register, verify (using zero-knowledge evidence), and validate communicating entities by utilizing a consensus process based on smart contracts. The authenticated data are then utilized to propose a unique DL strategy that combines a stacked sparse variational autoencoder (SSVAE) with self-attention-based bidirectional long short-term memory (SA-BiLSTM). In this system, SSVAE encodes or converts healthcare data to a new format, while SA-BiLSTM detects and enhances the attack detection process.

Several blockchain implementations, encryption strategies, and IoT-based systems are the three main categories of current system platforms for exchanging medical data. Table 3 outlines research proposing blockchain solutions for exchanging medical data.

4.1. Types of Blockchain

There are four primary forms of blockchain networks, including public blockchains, private blockchains, consortium blockchains, and hybrid blockchains. Each of these systems has advantages, disadvantages, and optimal applications. The paper by Zhang and Lin [49] offers a blockchain-based safe and privacy-preserving protected health information (PHI) sharing (BSPP) protocol for enhancing e-health system diagnostics. Initially, the data architecture and consensus procedures for the two types of blockchains—private blockchain and consortium blockchain—need to be designed. The private blockchain is responsible for storing PHI, while the consortium blockchain maintains the PHI's safe indexes. To ensure privacy preservation, access control, data security, and secure search, all data, including PHI, keywords, and patient identities, are encrypted with a public key using keyword search. Two kinds of blockchains, private and consortium blockchains, are developed in another research by Shamshad et al. [50] by defining their consensus, data formats, and procedures. A private blockchain is responsible for the maintenance of EHRs, while a consortium blockchain keeps the safe indexes of EHRs. To achieve data security, secure search, access management, and the protection of patient privacy, all EHRs are public-key encrypted with an appropriate search phrase.

4.2. Encryption

Encryption of medical data facilitates electronic data transmission and the sharing of clinical patient data and documentation. Regardless of location, patient medical data may be exchanged within a health system or transmitted to permitted health systems. In the study by Yang et al. [51], first, the encrypted medical data are saved in the cloud, and then the storage address and medical-related information are entered into the blockchain, thus ensuring efficient storage and eliminating the risk of irreversible data change. The proposed approach combines attribute-based encryption (ABE) and attribute-based signature (ABS) to enable the exchange of medical data in many-to-many interactions. The ABE provides data privacy and fine-grained access control, while the ABS confirms the source of medical data while safeguarding the signer's identity. In addition, the majority of medical data ciphertext decryption activities are outsourced by the data user to the cloud service provider (CSP), which may significantly minimize the computing strain. In a separate investigation, Sun et al. [52] conduct a hash computation on the EMR and record the resulting value on the blockchain to assure the data's integrity and validity. They encrypt the EMR and put it in the distributed storage protocol interplanetary file system. The encrypted keyword index information of EMRs was saved on Ethereum, and instead of relying on a centralized third party, a smart contract implemented on Ethereum was utilized to perform keyword searches. In addition, they use the ABE method to guarantee that only the access policy-compliant qualities may decode the encrypted EMR. Zhang et al. [53] address these issues by providing a distributed PHR-sharing mechanism based on blockchain and ciphertext policy ABE (CP-ABE), which enables efficient encryption and decryption. In addition to maintaining the data's integrity and tracking its source, blockchain records all activities on the data as transactions. In addition, the nodes of the blockchain serve as attribute authority for the CP-ABE cryptosystem. Tracing cryptographic techniques enables the identification of rogue blockchain nodes. Furthermore, the recovery of ciphertext is made fair via the use of smart contracts. To circumvent the restricted storage capacity of blockchain, our innovative solution employs both on-chain and off-chain storage options.

In the study by Zhang et al. [54], the deniably authenticated searchable encryption scheme (DASES) utilizes blockchain to assure the integrity, immutability, and traceability of image data, while circumventing the blockchain's storage and processing limitations. Not only can the DASES survive an inside keyword guessing attack (IKGA), but it can also offer good privacy protection and validate the validity of medical picture data. Secondly, they demonstrate that the DASES meets the ciphertext and trapdoor indistinguishability conditions. Regrettably, the DASES is less efficient than other comparable systems in the literature, but its largest asset is its capacity to provide an improved identity privacy protection and enhanced security. The application created by Cheng et al. [55] enables the physician to access the patient's personal history EMRs with the patient's permission to comprehend the patient's sickness history and build a new medical record for the patient. The server calculates the ciphertext and adds it to the patient's medical record to complete the case update. Via hierarchically storing patient information, medical staff information, and medical records, Yuan et al. [56] devise a three-chain paradigm. The combination of interplanetary file system (IPFS) technology and the encryption algorithm guarantees the security and efficiency of data storage off-chain. Attributes are used to classify users, and ABE technology is used for the secondary encryption of the key and ciphertext channel. However, hierarchical encryption drastically reduces the chance of a system assault. Zhang et al. [57] provide a unique blockchain-based data sharing system (BDSS) with fine-grained access control and permission revocation for the medical context. With this concept, they divide the EMR into public and private sections. Next, they employ symmetric searchable encryption (SSE) technology to encrypt these two pieces independently, and ABE technology to encrypt the symmetric keys used by SSE technology. Based on CP-ABE, Tan et al. [58] present a blockchain-enabled security and privacy protection system for COVID-19 medical records with traceable and direct revocation. With this system, all public keys, revocation lists, etc., are maintained on a blockchain, and the blockchain is used for consistent identity authentication. The system management server is responsible for producing the system settings and publishing the COVID-19 medical practitioners' and users' private keys. Using policy matching, the cloud server provider (CSP) maintains the CEMRs and creates the intermediate decryption parameters. If the user has private keys and intermediate decrypt parameters, he or she may compute the decryption key. Chen et al. [59] offer BFHS, a blockchain-based method for the safe, granular exchange of EHRs. On BFHS, they encrypt EHRs using ciphertext-policy ABE and upload them to the IPFS for storage, whilst the matching index is encrypted with proxy re-encryption and stored on a medical consortium blockchain. In addition, a credit evaluation system was developed and included in the smart contract. The combination of smart contracts, proxy re-encryption, a credit assessment system, and IPFS provides patients with a secure EHR sharing environment and a dynamic access control interface.

4.3. Ciphertext

Ciphertext is the result of an encryption algorithm transforming plaintext into encrypted text. Ciphertext cannot be read until it has been decrypted (converted to plaintext) using a key. Decryption cipher is a method that converts ciphertext to plaintext. Yang et al. [60] propose a novel blockchain-based keyword search protocol with dual authorization for the exchange of EHRs. The certificateless cryptosystem eliminates key escrow and certificate administration. The development of the authorization matrix enables the dual authorization of user identities and searchable departments. Moreover, the matrix may manage user access privileges. The ciphertext index signal value enables an authoritative control over the ciphertext index. The ciphertext MAC verification code kept on the blockchain can check for the legality of ciphertext, and smart contracts are utilized to guarantee fair transactions. Yang et al. [61] encrypt keywords using the certificateless cryptosystem, which eliminates the certificate administration and key escrow issues. The suggested approach also enables multi-user searches, and the user authorization table may be utilized to adjust medical data users' access rights. In addition, the root values of the Merkle trees are recorded in the blockchain to assure the search results' immutability, integrity, and traceability. In addition, a smart contract facilitates a fair transaction between a cloud service provider and customers of medical data without the need for trusted third parties. They demonstrate that the suggested technique is safe against the random oracle model's keyword-guessing attack. Lai et al. [62] propose a secure medical data-sharing system based on a traceable ring signature and blockchain as a solution to the issue of medical institutions' challenges in exchanging medical data. First, a certificateless traceable ring signature mechanism based on distributed key generation is suggested to preserve data integrity and privacy. The combination of a smart contract with access control and a self-controlling object (SCO) enables the outsourcing of decryption and the sharing of data. In addition, the suggested approach leverages the IPFS to store the seas of medical privacy data and encrypts the hash index to store it, which increases data sharing efficiency. Using the consensus process, they may choose the proxy node and upload the SCO package to the blockchain node for data exchange after the blockchain has been incorporated.

4.4. IoT-Based Systems

With healthcare mobility solutions, IoT may automate the workflow of patient care by automating the workflow of patient care. Data transfer, machine-to-machine connectivity, and interoperability have increased the productivity of healthcare sectors. Healthcare professionals and patients may save time with IoT integration. Chen et al. [63] presented a health IoT-based blockchain data-sharing system that protects privacy. To allow patients to construct granular privacy protection, they devised a privacy-preserving mechanism based on the content extraction signature system. They created a Byzantine fault-tolerant leader election method that improves the Raft algorithm's security and data-sharing efficiency. In addition, they built a summary contract to facilitate the retrieval of data. Pang et al. [64] propose a patient-controlled EHR-sharing system based on blockchain technology and cloud computing. To prevent tampering, the medical abstract and access strategy are kept on the blockchain. To accomplish fine-grained access control, they suggest encrypting EHRs using ABE and multi-keyword encryption. In addition, they suggested a node-state-checkable practical Byzantine fault tolerance consensus method to prevent Byzantine nodes from gaining access to the consortium blockchain. Nie et al. [65] present a new blockchain-based safe-sharing system with searchable encryption and a concealed data structure through IoT devices. Data owners' EHR ciphertexts are kept in the interplanetary file system (IPFS). A user with the appropriate access rights may search for the needed data using the data owner's time-limited authorization and validate the search result's legitimacy. With a symmetric key, the data user may then obtain the appropriate EHR ciphertext from IPFS. In IoT applications, the technique combines searchable encryption and smart contracts to provide safe search, time management, verified keyword search, quick search, and forward privacy. Wang et al. [66] present a consortium-based blockchain-based PHR management and sharing system that is both security-conscious and privacy-preserving. The PHR ciphertext of Internet of medical things (IoMT) is stored using the interplanetary file system (IPFS). Hence, zero-knowledge proof may be used to validate keyword index authentication on the blockchain. In addition, the system combines modified attribute-based cryptographic primitives with custom-tailored smart contracts to offer safe search, privacy preservation, and individualized access control in IoMT situations. Wu et al. [67] present a triple-subject purpose-based access control (TS-PBAC) model that is compatible with a blockchain-enabled reliable transaction network, and they design an individual-centric security and privacy-preserving mechanism for access control with varying purposes and roles in IoMT scenarios. Particularly, they develop a hierarchical purpose tree (HPT) and associated regulations to ensure the legality of an external user who has several purposes. They create a LDP-based policy and role-based access control mechanism in an edge computing paradigm to award fine-grained permissions to authorized users to increase the privacy of sensitive characteristics against an internal attacker.

Table 3. Summary of studies that propose blockchain systems in medical data sharing.

Blockchain Role	**Year**	**Capability**	**Smart Contract**	**Reference**
Trust-less medical data sharing	2017	Access control mechanism	✓	[68]
Blockchain-based data sharing for electronic medical records	2017	Receive data from the shared pool once identities and cryptographic keys have been validated		[69]
Efficient and secure medical data sharing	2018	The enhanced consensus technique delivers EMR consensus without significant network congestion or energy consumption		[70]
Secure and privacy-preserving data sharing	2019	Session-based flexible healthcare data sharing		[71]

Table 3. *Cont.*

Blockchain Role	Year	Capability	Smart Contract	Reference
Blockchain-based searchable encryption	2019	Complete control over data access	✓	[72]
Efficient healthcare data sharing	2019	Mutual authentication and the generation of a session key		[73]
Privacy-preserving data sharing	2019	Fine-grained access control, keyword search, and privacy protection		[74]
Secure and privacy-preserving data sharing	2020	Using bilinear mapping and intractable issues, the authentication process's security danger may be neutralized.		[75]
Efficient and secure data sharing	2020	Verification by zero-knowledge proof, decryption using proxy re-encryption technology, and PBFT-based distributed consensus		[76]
Privacy-preserving data sharing	2020	The data usage ontology and the automatable discovery and access matrix comprise the dynamic consent model	✓	[77]
Fine-grained access control and privacy protection	2020	In the random oracle paradigm, keyword indistinguishability against adaptively selected keyword assaults		[78]
Protected data sharing	2020	Couples with privacy-sensitive information are stored on the consortium blockchain, while non-sensitive data are shared on the public blockchain		[79]
Privacy-preserving medical data sharing	2021	Scheme for anonymously transmitting medical data based on proxy re-encryption algorithm and cloud servers		[80]
Secure data sharing	2021	Proxy re-encryption protocols		[81]
Protected data sharing	2021	Searchable encryption and K-anonymity	✓	[82]
Consortium-based data sharing	2021	Allowing data requesters to comply with data access requirements and to build their standing within a consortium		[83]
Secure and privacy-preserving data sharing	2021	The outsourced business has no access to the server or its data	✓	[84]
Secure and distributed data sharing	2021	Data ownership, data traceability, data consistency, privacy protection, data security, and distributed storage		[85]
Secure data storage and sharing	2021	Certificateless public key cryptography and elliptic curve cryptography (ECC)		[86]
Hierarchical data sharing with access control	2022	Fine-grained access control, efficient retrieval across encrypted PHRs with low-consumed hierarchical key distribution and key leakage resistance, as well as efficient aggregative authentication		[87]
Searchable encryption with access control	2022	Algorithm for key-policy ABE	✓	[88]
Privacy-preserving data sharing	2022	The condition is concealed inside the re-encryption key so that the proxy cannot discover it	✓	[89]

Table 3. *Cont.*

Blockchain Role	Year	Capability	Smart Contract	Reference
Protected and integrated data sharing	2022	Storing encrypted medical data in dispersed storage mode and integrating patient data across offline institutions and platforms		[90]
Privacy-enhanced data storage and exchange	2022	Patients' personal information is held on off-chain storage (IPFS), while other information is saved on the blockchain ledger, which is available to all participants	✓	[91]
Hybrid storage with access control	2022	Feasibility of recovery of the encryption keys	✓	[92]
Secure data sharing with access control	2022	Immutability, fine-grained access control, and traceability	✓	[93]

In the sphere of blockchain-based medical data sharing, there are common concepts and tendencies. These papers highlight the use of blockchain technology to facilitate the secure and trustless sharing of medical data, addressing issues of trust, security, and privacy. These solutions seek to provide a tamper-resistant and transparent infrastructure for storing and sharing sensitive medical information by leveraging the distributed and decentralized nature of blockchain in conjunction with cryptographic techniques.

In these blockchain-based systems, privacy and data security are top priorities. Several methods, including encryption techniques, access control mechanisms, and privacy-preserving algorithms, are used to protect the privacy of patient information while allowing authorized parties to access relevant data. In addition, attribute-based access control and fine-grained access control mechanisms are frequently employed, enabling data owners to define access policies based on particular attributes or duties. Frequently, consortium or permissioned blockchains are utilized, allowing multiple trusted parties to collaborate and administer the shared data. Moreover, interoperability, consent management, and compliance with regulations such as the General Data Protection Regulation (GDPR) are also essential considerations for these solutions. These trends highlight the growing interest in utilizing blockchain technology to establish secure, privacy-preserving, and interoperable medical data-sharing systems.

Various research studies are garnering interest in the application of blockchain technology to the exchange of medical data. Several approaches and frameworks have been proposed by researchers to resolve the challenges associated with health data exchange. These methods make use of blockchain characteristics such as tamper resistance, secure rules, extendable access control, auditing, and counterfeit protection. They investigate the architecture of smart contracts, devise methods for inter-blockchain communication, and assess the efficacy of these systems by calculating execution costs. Integrating encryption methods such as attribute-based encryption (ABE) and ciphertext-policy ABE (CP-ABE) with blockchain ensures privacy protection, granular access control, and secure search. Consideration is given to public, private, consortium, and hybrid blockchains for the secure storage and management of medical data. Moreover, techniques such as hash computation, deniably authenticated searchable encryption schemes (DASES), and smart contracts are utilized to guarantee data integrity, validity, and traceability. By integrating blockchain technology with encryption techniques, researchers hope to develop dependable systems that improve data security, privacy, and the exchange of medical information.

RQ3: What are the issues of using blockchain to share medical data?

Using blockchain technology for sharing medical data presents several issues that need to be addressed. Firstly, scalability is a major concern. Blockchain networks may struggle to manage the large volumes of data involved in sharing EMRs among multiple stakeholders. Scaling the blockchain to accommodate these demands is essential for efficient data sharing [69]. Ensuring the privacy and confidentiality of sensitive medical data is paramount in healthcare systems. While blockchain offers immutability and transparency, it presents challenges in protecting patient privacy and maintaining data confidentiality. Innovative solutions must be developed to address these concerns and provide robust privacy measures in blockchain-based medical data-sharing systems [70].

Another significant issue is the performance and efficiency of blockchain networks. Public blockchains, in particular, can experience slow transaction-processing speeds and high energy consumption. These limitations hinder the real-time access and responsiveness required for sharing medical data effectively. Optimizing blockchain performance and energy efficiency is crucial to ensure seamless data sharing [74]. Additionally, the interoperability of blockchain with the existing healthcare infrastructure is a challenge. Integrating blockchain into diverse systems and ensuring compatibility with legacy systems is complex. Achieving seamless interoperability among different healthcare providers and systems is crucial for effective medical data sharing. Addressing this issue requires careful planning and implementation strategies [75].

Regulatory and legal considerations play a significant role in blockchain-based medical data sharing. Compliance with data protection laws, such as GDPR, is necessary. However, the decentralized nature and immutability of blockchain can make it difficult to meet certain regulatory obligations, such as data deletion and consent management. Developing frameworks that align with regulatory requirements is vital to ensure compliance while leveraging the benefits of blockchain technology [91]. Lastly, establishing a governance framework and building trust among participating entities are critical aspects of blockchain-based medical data sharing. The distributed nature of blockchain requires robust consensus mechanisms and trust models to guarantee data integrity and reliability. Creating effective governance structures that address the needs and concerns of all stakeholders is essential for successful implementation [81].

The use of blockchain for sharing medical data poses several challenges. Scalability, privacy and confidentiality, performance and efficiency, interoperability, regulatory compliance, and governance and trust are among the key issues that need to be addressed. Overcoming these challenges is crucial for the successful implementation of blockchain-based solutions in healthcare, enabling secure, efficient, and privacy-preserving sharing of medical data. Table 4 provides an overview of the various research papers pertaining to blockchain-based medical data-sharing schemes.

Table 4. Challenges and possible solutions of blockchain-based medical data-sharing schemes.

Category	Study	Challenges	Possible Solutions
Access Control and Privacy	[51]	Attribute-based access control, privacy preservation, data sharing efficiency	Utilize attribute-based encryption, design access control policies, optimize data sharing efficiency
	[52]	Fine-grained access control, scalability, data validation	Implement access control mechanisms with granular permissions, employ scalability solutions such as sharding or sidechains, ensure data validation through smart contracts
	[54]	Searchable encryption for medical images, deniable authentication, access control	Develop deniably authenticated searchable encryption schemes, implement access control mechanisms, ensure confidentiality of medical images
	[53]	Decentralized attribute-based sharing, data privacy, attribute management	Design decentralized attribute-based sharing mechanisms, address privacy concerns, implement effective attribute management

Table 4. *Cont.*

Category	Study	Challenges	Possible Solutions
	[67]	Access control in IoT, privacy preservation, data publishing	Implement privacy-preserving access control mechanisms, address IoT-specific challenges, enable secure data publishing
Data Sharing and Integration	[55]	Cross-domain data sharing, edge computing integration, data integrity	Integrate edge computing with blockchain for cross-domain sharing, ensure data integrity through consensus mechanisms
	[48]	Industrial healthcare systems, secure data sharing, deep learning integration	Utilize permissioned blockchain for secure sharing, leverage deep learning techniques for efficient data analysis
	[76]	Privacy preservation, data security, access control	Employ privacy-enhancing techniques, ensure secure data storage and transmission, implement access control protocols
	[88]	Edge-based IoMT, secure data sharing, privacy preservation	Leverage blockchain for secure data sharing, integrate with edge-based IoMT, employ privacy-preserving techniques
	[89]	Fine-grained data sharing, privacy preservation, secure storage	Design fine-grained data-sharing protocols, employ privacy-preserving techniques, ensure secure storage
Emergency and Healthcare-Specific	[44]	Emergency data sharing, data privacy, secure communication	Design emergency-specific data sharing frameworks, address privacy concerns, ensure secure communication through encryption
	[85]	Rehabilitation medical record sharing, data privacy, interoperability	Design rehabilitation-specific data-sharing schemes, address data privacy concerns, establish interoperability standards
	[86]	Anonymous data sharing, secure communication, scalability	Develop anonymous data-sharing protocols, ensure secure communication through blockchain, optimize scalability
	[80]	Medical data privacy, consent management, auditability	Design privacy-preserving mechanisms using blockchain, implement consent management frameworks, provide auditing capabilities
	[75]	Trust and privacy concerns, access control, data provenance	Address trust and privacy through blockchain's transparent and immutable nature, implement access control mechanisms, track data provenance
Data Integrity and Consistency	[64]	Checkable-state PBFT consensus algorithm, data consistency, auditing	Implement checkable state PBFT consensus algorithm, ensure data consistency, provide auditing mechanisms
	[81]	Privacy preservation, data integrity, secure sharing protocols	Utilize privacy-enhancing technologies, ensure data integrity through cryptographic mechanisms, design secure sharing protocols
	[70]	Data integrity, interoperability, efficient access control	Implement cryptographic mechanisms, standardize data formats, design efficient access control mechanisms
	[73]	Data privacy, integrity, access control	Utilize encryption techniques, implement access control mechanisms, ensure data integrity through hashing or digital signatures
	[74]	Data integrity verification, user authentication, secure storage	Use cryptographic techniques for integrity verification, implement user authentication protocols, employ secure storage mechanisms

Table 4. *Cont.*

Category	Study	Challenges	Possible Solutions
Governance and Compliance	[68]	Trust and security issues in data sharing among multiple cloud providers	Use blockchain to create a trustless environment, implement secure data sharing protocols
	[91]	GDPR compliance, data storage, data sharing	Ensure GDPR compliance through blockchain, implement secure data storage mechanisms, enable secure data sharing
	[92]	Privacy preservation, secure sharing protocols, consortium blockchain governance	Employ privacy-preserving mechanisms, design secure sharing protocols, establish governance frameworks for consortium blockchains
	[93]	Multi-hop permission delegation, controllable delegation depth, access control	Develop multi-hop permission delegation schemes, enable control over delegation depth, implement access control mechanisms
	[83]	Data protection, transparency, consortium governance	Implement data protection mechanisms, ensure transparency through blockchain, establish governance frameworks for consortium blockchains

Using blockchain technology for sharing medical data presents several technical challenges that need to be addressed for successful implementation in healthcare systems. Scalability is a major concern due to the large volumes of data involved, requiring the blockchain networks to be scaled appropriately. The privacy and confidentiality of sensitive medical data need to be ensured, necessitating the development of innovative solutions such as attribute-based encryption and robust access control policies. Performance and efficiency issues, including slow transaction-processing speeds and high energy consumption, need to be optimized for real-time data access. Interoperability with existing healthcare infrastructure requires careful integration and compatibility planning. Regulatory compliance, particularly with data protection laws like GDPR, is crucial, and frameworks aligning with these requirements need to be developed. Establishing a governance framework and building trust among participants is essential, necessitating robust consensus mechanisms and effective governance structures. Overcoming these challenges will enable the secure, efficient, and privacy-preserving sharing of medical data, leading to improved healthcare outcomes.

5. Conclusions

As medical technology progresses, there is a rising demand for healthcare professionals throughout the globe to communicate an expanding number of data safely. Blockchain is commonly used in the healthcare industry to provide a comprehensive knowledge of patient information and monitor data-sharing permission. It is a robust technology that enables numerous parties to view and exchange data securely. Considering the huge difficulty that healthcare organizations confront in digitizing and exchanging health information, it is not surprising that many are striving to enhance healthcare operations via the use of blockchain. Using publications published between 2017 and 2022, this review examines the present status, research trends, and problems of blockchain in medical data exchange to address the existing gap.

To attain this purpose, RQs were formulated and a predetermined technique was used to reduce the number of articles reviewed to 50. They were then studied further. Our results show that blockchain technology development and its use in the exchange of medical data are growing. Hence, most of blockchain's potential remain untapped. Most of the studies propose a unique framework, architecture, or methodology for medical data exchange by utilizing blockchain technology. As there are a multitude of benefits in exchanging patient data in a safe, decentralized manner, it is difficult to comprehend why the industry has not determined and concluded on using this concept earlier. Nevertheless, as with many factors in the commercial sector, there are actual reasons as to why it is difficult to exchange healthcare data. It seems that countless challenges must be addressed before blockchain can become the dominant industrial technology.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Stanfill, M.H.; Marc, D.T. Health information management: Implications of artificial intelligence on healthcare data and information management. *Yearb. Med. Inform.* **2019**, *28*, 56–64. [CrossRef] [PubMed]
2. Adamu, J.; Hamzah, R.; Rosli, M.M. Security issues and framework of electronic medical record: A review. *Bull. Electr. Eng. Inform.* **2020**, *9*, 565–572.
3. Enaizan, O.; Zaidan, A.A.; Alwi, N.; Zaidan, B.B.; Alsalem, M.A.; Albahri, O.; Albahri, A. Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health Technol.* **2020**, *10*, 795–822.
4. Hulsen, T. Sharing is caring—Data sharing initiatives in healthcare. *Int. J. Environ. Res. Public Health* **2020**, *17*, 3046. [PubMed]
5. Ghafur, S.; Van Dael, J.; Leis, M.; Darzi, A.; Sheikh, A. Public perceptions on data sharing: Key insights from the UK and the USA. *Lancet Digit. Health* **2020**, *2*, e444–e446. [PubMed]
6. Schwalbe, N.; Wahl, B.; Song, J.; Lehtimaki, S. Data sharing and global public health: Defining what we mean by data. *Front. Digit. Health* **2020**, *2*, 612339.
7. Kish, L.J.; Topol, E.J. Unpatients—Why patients should own their medical data. *Nat. Biotechnol.* **2015**, *33*, 921–924.
8. Wang, Y.; Li, P.-F.; Tian, Y.; Ren, J.-J.; Li, J.-S. A shared decision-making system for diabetes medication choice utilizing electronic health record data. *IEEE J. Biomed. Health Inform.* **2016**, *21*, 1280–1287. [CrossRef]
9. Singh, C.; Chauhan, D. IoT–Blockchain Integration-Based Applications Challenges and Opportunities. *Mob. Radio Commun. 5g Netw. Proc. MRCN* **2020**, *2020*, 87–116.
10. Lin, B.; Huang, Y.; Zhang, J.; Hu, J.; Chen, X.; Li, J. Cost-driven off-loading for DNN-based applications over cloud, edge, and end devices. *IEEE Trans. Ind. Inform.* **2019**, *16*, 5456–5466. [CrossRef]
11. Thilakanathan, D.; Chen, S.; Nepal, S.; Calvo, R.; Alem, L. A platform for secure monitoring and sharing of generic health data in the Cloud. *Future Gener. Comput. Syst.* **2014**, *35*, 102–113. [CrossRef]
12. Yang, J.-J.; Li, J.-Q.; Niu, Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Gener. Comput. Syst.* **2015**, *43*, 74–86. [CrossRef]
13. Zhu, H.; Liu, X.; Lu, R.; Li, H. Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM. *IEEE J. Biomed. Health Inform.* **2016**, *21*, 838–850. [CrossRef] [PubMed]
14. Michalas, A.; Weingarten, N. Healthshare: Using attribute-based encryption for secure data sharing between multiple clouds. In Proceedings of the 2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS), Thessaloniki, Greece, 22–24 June 2017; pp. 811–815.
15. Fang, H.S.A.; Tan, T.H.; Tan, Y.F.C.; Tan, C.J.M. Blockchain personal health records: Systematic review. *J. Med. Internet Res.* **2021**, *23*, e25094. [CrossRef]
16. Westphal, E.; Seitz, H. Digital and decentralized management of patient data in healthcare using blockchain implementations. *Front. Blockchain* **2021**, *4*, 732112. [CrossRef]
17. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
18. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.-K.R. Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review. *IEEE Trans. Eng. Manag.* **2020**, *70*, 353–368. [CrossRef]
19. Abu-Elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-Alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. *Int. J. Med. Inform.* **2020**, *142*, 104246. [CrossRef]
20. Saha, A.; Amin, R.; Kunal, S.; Vollala, S.; Dwivedi, S.K. Review on "Blockchain technology based medical healthcare system with privacy issues". *Secur. Priv.* **2019**, *2*, e83. [CrossRef]
21. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef]
22. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A review of secure and privacy-preserving medical data sharing. *IEEE Access* **2019**, *7*, 61656–61669. [CrossRef]
23. Dubovitskaya, A.; Novotny, P.; Xu, Z.; Wang, F. Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review. *Oncology* **2020**, *98*, 403–411. [CrossRef]
24. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain technologies: The foreseeable impact on society and industry. *Computer* **2017**, *50*, 18–28. [CrossRef]

25. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.
26. Raval, S. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*; O'Reilly Media, Inc.: Sevastopol, CA, USA, 2016.
27. Roehrs, A.; Da Costa, C.A.; da Rosa Righi, R. OmniPHR: A distributed architecture model to integrate personal health records. *J. Biomed. Inform.* **2017**, *71*, 70–81. [CrossRef] [PubMed]
28. Sleiman, M.D.; Lauf, A.P.; Yampolskiy, R. Bitcoin message: Data insertion on a proof-of-work cryptocurrency system. In Proceedings of the 2015 International Conference on Cyberworlds (CW), Visby, Sweden, 7–9 October 2015; pp. 332–336.
29. Aumasson, J.-P. *Serious Cryptography: A Practical Introduction to Modern Encryption*; No Starch Press: San Francisco, CA, USA, 2017.
30. Sharma, D.; Sharma, S.K. The use of blockchain technology in IoT-based healthcare: A concise guide. In *Blockchain Technology Solutions for the Security of Iot-Based Healthcare Systems*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 183–198.
31. Greenspan, G. *Blockchains vs Centralized Databases*; MultiChain: London, UK, 2016.
32. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology?—A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]
33. Wang, H.; Wang, Y.; Cao, Z.; Li, Z.; Xiong, G. An overview of blockchain security analysis. In Proceedings of the Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, 14–16 August 2018; Revised Selected Papers 15. Springer: Singapore, 2019; pp. 55–72.
34. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
35. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
36. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
37. Taherdoost, H. Blockchain and Machine Learning: A Critical Review on Security. *Information* **2023**, *14*, 295. [CrossRef]
38. Mazlan, A.A.; Daud, S.M.; Sam, S.M.; Abas, H.; Rasid, S.Z.A.; Yusof, M.F. Scalability challenges in healthcare blockchain system—A systematic review. *IEEE Access* **2020**, *8*, 23663–23673. [CrossRef]
39. Taherdoost, H. Blockchain-Based Internet of Medical Things. *Appl. Sci.* **2023**, *13*, 1287. [CrossRef]
40. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. *Inf. Process. Manag.* **2021**, *58*, 102397. [CrossRef]
41. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-based data preservation system for medical data. *J. Med. Syst.* **2018**, *42*, 141. [CrossRef]
42. Lin, J.; Niu, J.; Li, H. PCD: A privacy-preserving predictive clinical decision scheme with E-health big data based on RNN. In Proceedings of the 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, USA, 1–4 May 2017; pp. 808–813.
43. Taherdoost, H. Towards Nuts and Bolts of Conducting Literature Review: A Typology of Literature Review. *Electronics* **2023**, *12*, 800. [CrossRef]
44. Rajput, A.R.; Li, Q.; Ahvanooey, M.T. A blockchain-based secret-data sharing framework for personal health records in emergency condition. *Healthcare* **2021**, *9*, 206. [CrossRef]
45. Hu, C.; Li, C.; Zhang, G.; Lei, Z.; Shah, M.; Zhang, Y.; Xing, C.; Jiang, J.; Bao, R. CrowdMed-II: A blockchain-based framework for efficient consent management in health data sharing. *World Wide Web* **2022**, *25*, 1489–1515. [CrossRef]
46. Hashim, F.; Shuaib, K.; Sallabi, F. Connected Blockchain Federations for Sharing Electronic Health Records. *Cryptography* **2022**, *6*, 47. [CrossRef]
47. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927. [CrossRef]
48. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.K.M.N.; Shorfuzzaman, M. Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8065–8073. [CrossRef]
49. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef] [PubMed]
50. Shamshad, S.; Minahil; Mahmood, K.; Kumari, S.; Chen, C.M. A secure blockchain-based e-health records storage and sharing scheme. *J. Inf. Secur. Appl.* **2020**, *55*, 102590. [CrossRef]
51. Yang, X.; Li, T.; Pei, X.; Wen, L.; Wang, C. Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology. *IEEE Access* **2020**, *8*, 45468–45476. [CrossRef]
52. Sun, J.; Ren, L.; Wang, S.; Yao, X. A blockchain-based framework for electronic medical records sharing with fine-grained access control. *PLoS ONE* **2020**, *15*, e0239946. [CrossRef]
53. Zhang, L.; Zhang, T.; Wu, Q.; Mu, Y.; Rezaeibagha, F. Secure Decentralized Attribute-Based Sharing of Personal Health Records with Blockchain. *IEEE Internet Things J.* **2022**, *9*, 12482–12496. [CrossRef]
54. Zhang, Y.L.; Wen, L.; Zhang, Y.J.; Wang, C.F. Deniably authenticated searchable encryption scheme based on Blockchain for medical image data sharing. *Multimed. Tools Appl.* **2020**, *79*, 27075–27090. [CrossRef]

55. Cheng, Y.; Gong, B.; Jia, Z.; Yang, Y.; He, Y.; Zhang, X. Efficient and Secure Cross-Domain Sharing of Blockchain Electronic Medical Records Based on Edge Computing. *Secur. Commun. Netw.* **2021**, *2021*, 7310771. [CrossRef]
56. Yuan, J.; Ma, Y.; Luo, W.; Han, G. B-SSMD: A Fine-Grained Secure Sharing Scheme of Medical Data Based on Blockchain. *Secur. Commun. Netw.* **2022**, *2022*, 2719951. [CrossRef]
57. Zhang, L.; Zou, Y.; Yousuf, M.H.; Wang, W.; Jin, Z.; Su, Y.; Seokhoon, K. BDSS: Blockchain-based Data Sharing Scheme With Fine-grained Access Control And Permission Revocation In Medical Environment. *KSII Trans. Internet Inf. Syst.* **2022**, *16*, 1634–1652. [CrossRef]
58. Tan, L.; Yu, K.; Shi, N.; Yang, C.; Wei, W.; Lu, H. Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 271–281. [CrossRef]
59. Chen, J.; Yin, X.; Ning, J. A fine-grained and secure health data sharing scheme based on blockchain. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4510. [CrossRef]
60. Yang, X.; Wang, J.; Xi, W.; Tian, T.; Wang, C. A blockchain-based keyword search scheme with dual authorization for electronic health record sharing. *J. Inf. Secur. Appl.* **2022**, *66*, 103154. [CrossRef]
61. Yang, X.; Tian, T.; Wang, J.; Wang, C. Blockchain-based multi-user certificateless encryption with keyword search for electronic health record sharing. *Peer-Peer Netw. Appl.* **2022**, *15*, 2270–2288. [CrossRef]
62. Lai, C.; Ma, Z.; Guo, R.; Zheng, D. Secure medical data sharing scheme based on traceable ring signature and blockchain. *Peer-Peer Netw. Appl.* **2022**, *15*, 1562–1576. [CrossRef]
63. Chen, S.; Fu, X.; Si, H.; Wang, Y.; Gao, S.; Wang, C. Blockchain for Health IoT: A privacy-preserving data sharing system. *Softw.-Pract. Exp.* **2022**, *52*, 2026–2044. [CrossRef]
64. Pang, Z.; Yao, Y.; Li, Q.; Zhang, X.; Zhang, J. Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm. *IEEE Access* **2022**, *10*, 87803–87815. [CrossRef]
65. Nie, X.; Zhang, A.; Chen, J.; Qu, Y.; Yu, S. Time-Enabled and Verifiable Secure Search for Blockchain-Empowered Electronic Health Record Sharing in IoT. *Secur. Commun. Netw.* **2022**, *2022*, 1103863. [CrossRef]
66. Wang, Y.; Zhang, A.; Zhang, P.; Qu, Y.; Yu, S. Security-Aware and Privacy-Preserving Personal Health Record Sharing Using Consortium Blockchain. *IEEE Internet Things J.* **2022**, *9*, 12014–12028. [CrossRef]
67. Wu, G.; Wang, S.; Ning, Z.; Li, J. Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. *IEEE Internet Things J.* **2022**, *9*, 8091–8104. [CrossRef]
68. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
69. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]
70. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef]
71. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
72. Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429. [CrossRef]
73. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A Blockchain-Based Medical Data Sharing and Protection Scheme. *IEEE Access* **2019**, *7*, 118943–118953. [CrossRef]
74. Wang, S.; Zhang, D.; Zhang, Y. Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable. *IEEE Access* **2019**, *7*, 102887–102901. [CrossRef]
75. Cheng, X.; Chen, F.; Xie, D.; Sun, H.; Huang, C. Design of a Secure Medical Data Sharing Scheme Based on Blockchain. *J. Med. Syst.* **2020**, *44*, 52. [CrossRef]
76. Huang, H.; Zhu, P.; Xiao, F.; Sun, X.; Huang, Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Comput. Secur.* **2020**, *99*, 102010. [CrossRef]
77. Jaiman, V.; Urovi, V. A Consent Model for Blockchain-Based Health Data Sharing Platforms. *IEEE Access* **2020**, *8*, 143734–143745. [CrossRef]
78. Niu, S.; Chen, L.; Wang, J.; Yu, F. Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain. *IEEE Access* **2020**, *8*, 7195–7204. [CrossRef]
79. Cao, Y.; Sun, Y.; Min, J. Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system. *Meas. Control* **2020**, *53*, 1286–1299. [CrossRef]
80. Chen, Z.; Xu, W.; Wang, B.; Yu, H. A blockchain-based preserving and sharing system for medical data privacy. *Future Gener. Comput. Syst.* **2021**, *124*, 338–350. [CrossRef]
81. Zou, R.; Lv, X.; Zhao, J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Inf. Process. Manag.* **2021**, *58*, 102604. [CrossRef]
82. Chen, Y.; Meng, L.; Zhou, H.; Xue, G. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6685762. [CrossRef]
83. Purohit, S.; Calyam, P.; Alarcon, M.L.; Bhamidipati, N.R.; Mosa, A.; Salah, K. HonestChain: Consortium blockchain for protected data sharing in health information systems. *Peer-Peer Netw. Appl.* **2021**, *14*, 3012–3028. [CrossRef]

84. Park, Y.H.; Kim, Y.; Lee, S.O.; Ko, K. Secure outsourced blockchain-based medical data sharing system using proxy re-encryption. *Appl. Sci.* **2021**, *11*, 9422. [CrossRef]
85. Zhang, J.; Li, Z.; Tan, R.; Liu, C. Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology. *BioMed Res. Int.* **2021**, *2021*, 3540830. [CrossRef]
86. Yang, X.; Li, X.; Li, T.; Wang, X.; Wang, C.; Li, B. Efficient and anonymous multi-message and multi-receiver electronic health records sharing scheme without secure channel based on blockchain. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4371. [CrossRef]
87. Zhang, J.; Yang, Y.; Liu, X.; Ma, J. An Efficient Blockchain-Based Hierarchical Data Sharing for Healthcare Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7139–7150. [CrossRef]
88. Nie, X.; Zhang, A.; Chen, J.; Qu, Y.; Yu, S. Blockchain-Empowered Secure and Privacy-Preserving Health Data Sharing in Edge-Based IoMT. *Secur. Commun. Netw.* **2022**, *2022*, 8293716. [CrossRef]
89. Lin, G.; Wang, H.; Wan, J.; Zhang, L.; Huang, J. A blockchain-based fine-grained data sharing scheme for e-healthcare system. *J. Syst. Archit.* **2022**, *132*, 102731. [CrossRef]
90. Li, C.; Liu, J.; Qian, G.; Wang, Z.; Han, J. Double chain system for online and offline medical data sharing via private and consortium blockchain: A system design study. *Front. Public Health* **2022**, *10*, 1012202. [CrossRef] [PubMed]
91. Bai, P.; Kumar, S.; Kumar, K.; Kaiwartya, O.; Mahmud, M.; Lloret, J. GDPR Compliant Data Storage and Sharing in Smart Healthcare System: A Blockchain-Based Solution. *Electronics* **2022**, *11*, 3311. [CrossRef]
92. Zhang, D.; Wang, S.; Zhang, Y.; Zhang, Q.; Zhang, Y. A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain. *Secur. Commun. Netw.* **2022**, *2022*, 2759787. [CrossRef]
93. Gao, Y.; Zhang, A.; Wu, S.; Chen, J. Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing. *High-Confid. Comput.* **2022**, *2*, 100084. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.