


Review

Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives

Hamed Taherdoost^{1,2,3} 

- ¹ Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada; hamed.taherdoost@gmail.com or hamed@hamta.org
- ² Research and Development Department, Hamta Group—Hamta Business Corporation, Vancouver, BC V6E 1C9, Canada
- ³ Q Minded—Quark Minded Technology Inc., Vancouver, BC V6E 1C9, Canada

Abstract: Blockchain offers a cutting-edge solution for storing medical data, carrying out medical transactions, and establishing trust for medical data integration and exchange in a decentralized open healthcare network setting. While blockchain in healthcare has garnered considerable attention, privacy and security concerns remain at the center of the debate when adopting blockchain for information exchange in healthcare. This paper presents research on the subject of blockchain's privacy and security in healthcare from 2017 to 2022. In light of the existing literature, this critical evaluation assesses the current state of affairs, with a particular emphasis on papers that deal with practical applications and difficulties. By providing a critical evaluation, this review provides insight into prospective future study directions and advances.

Keywords: blockchain technology; security and privacy; medical industry



Citation: Taherdoost, H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. *Sci* **2023**, *5*, 41. <https://doi.org/10.3390/sci5040041>

Academic Editors: Claus Jacob and Ahmad Yaman Abdin

Received: 18 September 2023
Revised: 16 October 2023
Accepted: 27 October 2023
Published: 30 October 2023



Copyright: © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent years, there has been an increase in the use of blockchain across a variety of industries, including healthcare [1–3]. This is not unexpected given that blockchain is an immutable, transparent, and decentralized distributed database [4] that may be used to create a trustworthy value chain. The digitization of the healthcare business is leading to the creation of medical information systems. While healthcare is a vital aspect of an individual's life, so are its associated data, which aid in the diagnosis of sickness and support future actions. In the past, information was written and recorded on media that may be easily altered and destroyed [5,6]. These systems need to possess the capacity to communicate data safely and efficiently [7]. Also, they need to enable increased anonymity, privacy, and access control for each user. If there is little or no security, privacy, and trust, people will be reticent to share their sensitive information, or they may delay obtaining treatment [8]. Data protection becomes necessary. Consequently, blockchain technology, a developing technology that claims to safeguard data leaks and data from vulnerabilities, has come to light [9].

Due to its distributed nature, blockchain technology might alter this dependency. It offers the capacity to overcome failure and assaults in a distributive and unchanging manner. Moreover, it gives a record of the data's ownership and legitimacy [10]. Hence, blockchain is increasingly seen as a general-purpose technology with applications in a variety of sectors and use cases, including healthcare, insurance, supply-chain management, contract administration, dispute resolution, and identity management [11]. Blockchain is characterized by its special characteristics of transparency, traceability, reliability, and decentralization. Hence, blockchain may be able to solve security, confidentiality, and interoperability problems. Blockchain enables parties who lack confidence to conduct a wide range of network transactions. A distributed network of devices' data may be recorded and stored in a blockchain [12].

The application of blockchain in healthcare has the potential to transform the storage and sharing of patient data, making the processes safer and more efficient. Concerns exist, however, about the security and privacy of blockchain in healthcare, especially with the safeguarding of sensitive patient data. The purpose of this literature study is to offer an overview of the available research on the security and privacy of blockchain in healthcare. Hasselgren et al. [13] carried out a scoping assessment on the healthcare use of blockchain technology. The authors concluded that blockchain has the potential to enhance healthcare security and privacy, but stress that there are still obstacles to overcome, such as the requirement for interoperability and the legal environment. Azaria et al. [14] argued that in today's digital age, the privacy and security of patient data in the healthcare business are of the utmost importance and need to be preserved in a digital format. This may be accomplished via the use of blockchain technology to monitor healthcare data. This will aid in reaching the desired end goal of authenticity, accountability, and assurance for data exchange. The application of healthcare blockchains for safe data exchange in the healthcare industry was examined in the study by Zhang et al. [15]. It examined several technological solutions, such as anonymous signatures and encryption methods, to solve privacy and security issues. The essay also investigated possible healthcare uses for blockchain technology and classified blockchain usage scenarios.

Overall, the evidence demonstrates that blockchain has the potential to enhance the security and privacy of patient data storage and exchange. Yet, there are still obstacles to overcome, including interoperability, regulatory difficulties, and the requirement for suitable access controls. To fully explore the possibilities of blockchain in healthcare and guarantee that it is utilized responsibly to safeguard patient privacy and security, further study is required. This article describes the critical review undertaken in response to the aforementioned queries. While there are other fascinating studies of this issue in the literature [16–18], this article is distinct in terms of technique and aims.

This review conducts research on the security and privacy of blockchain in healthcare from 2017 to 2022 according to specific research questions (Figure 1). Through a critical evaluation of the existing literature, it examines the current state of affairs, focusing on practical applications and challenges. By providing a critical assessment, this review offers a valuable insight into potential future research directions and advancements.

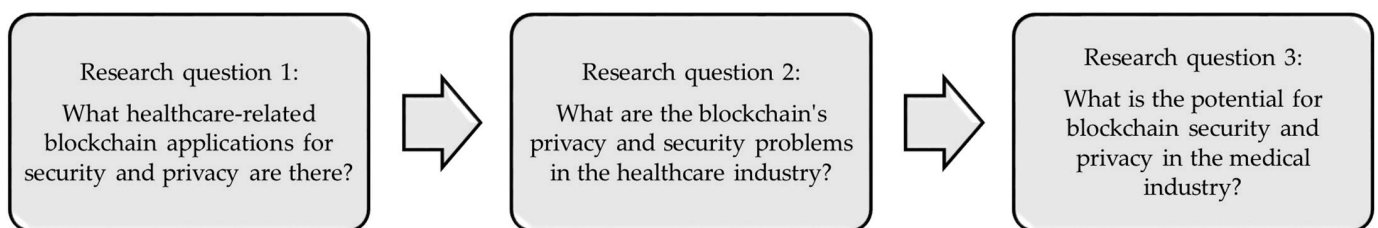


Figure 1. Research questions.

2. Background

2.1. Blockchain

Blockchain was popularized by Bitcoin's success [19] and may be used to conduct secure and trustworthy transactions over an untrusted network without depending on a centralized third party. We shall now discuss the core components of the blockchain [20,21]. Based on the rights granted to network nodes, three kinds of blockchain systems exist:

1. Private blockchain: Access control governs how the private blockchain network functions, requiring authorization or an invitation before users may join.
2. Public ledger system: The public blockchain is accessible to anybody at any moment who wishes to participate as a basic node or a miner for economic benefits.
3. Blockchain consortium: The consortium blockchain, which hovers between public and private blockchains, is referred to as "semi-private". It is given to a collection of authorized organizations that are often used in enterprises to advance business.

Blockchain's fundamental elements serve as an example of its structural underpinnings. Decentralization, first and foremost, is a key feature; data are stored and verified throughout a network of nodes, doing away with the necessity for a central point of control [22]. Additionally, data integrity is ensured by cryptographic hashing since each block contains a cryptographic hash of the preceding one, making it very difficult to tamper with the data [23]. Proof-of-work and proof-of-stake consensus processes make it easier to add additional blocks, while smart contracts automate and enforce contracts directly [24]. Blockchain is a trustworthy source of truth due to the immutability of the ledger and its dependence on public key cryptography, which guarantees the security and transparency of transactions [25].

By tackling interoperability difficulties and putting patients at the center of the ecosystem, blockchain's operating principles have the potential to completely transform the healthcare sector [26]. Patients may individually allow or deny access to their medical information and have more control over it thanks to decentralized data storage and cryptographic security [27]. This improves patient-centered care by enhancing privacy while simultaneously making it easier for authorized parties to share medical information [28]. For applications like corporate use cases, blockchain's transparency is crucial since it allows for control over network rights in private and consortium blockchains, guaranteeing that only authorized entities access the network.

Blockchain will aid in addressing some of the interoperability issues in healthcare and may be crucial in placing patients at the center of the ecosystem [29]. It improves interoperability, security, and privacy, and it may place patients at the heart of the ecosystem [30]. Blockchain may be used for remote monitoring, mobile apps, and medical data management systems that provide patients with ownership of their records as well as for accessing and sharing patient medical information [31].

2.2. Security in Healthcare

The security of healthcare data is achieved in several ways. Several studies have managed this by using administrative, physical, and technological concepts. To better safeguard the secure and safe patient data included in digital health information, these standards are made up of a variety of security methods that are used by healthcare organizations [32,33]. Patient data access is restricted using security protocols to protect it from unauthorized individuals. Operational controls may be used to do this inside a covered entity [34].

By securely storing and exchanging sensitive patient data, blockchain technology has the potential to transform the healthcare sector [14,17]. Data security is crucial in the healthcare sector because it protects sensitive patient data including medical histories, medications, and test results. Any compromise of this information might have negative effects on patients.

Blockchain technology appeals to healthcare businesses because it offers a safe, decentralized method of data sharing and keeping. Blockchain is simply a digital ledger that securely and impenetrably records transactions [19]. The information is kept in blocks, and each block is connected to the one before it in a chain, hence the term "blockchain". The following characteristics of blockchain technology make it appropriate for managing safe healthcare data:

4. Decentralized storage: Data stored in a standard data storage system are centralized, leaving them susceptible to hackers. With the use of blockchain technology, data are disseminated over the network and kept decentralized, making them far more difficult for hackers to access.
5. Immutability: Information stored on a blockchain cannot be changed or removed once it has been added. This feature makes the data tamper-proof by ensuring their integrity.
6. Encryption: Data are protected using cutting-edge encryption methods in blockchain technology, guaranteeing that only authorized parties have access to them.

7. Smart contracts: These self-executing legal pacts may automate the data exchange and access control processes. By guaranteeing that only those with permission may access the data, this feature adds an extra degree of protection.
8. Transparency: Blockchain technology promotes transparency by making the data accessible to all network participants. This feature may promote accountability while reducing fraud.

Security needs to come first when using blockchain technology in the healthcare industry. Given the sensitivity and confidentiality of healthcare data, several crucial security measures and best practices should be emphasized [35]. Cryptographic techniques are essential for maintaining the confidentiality and integrity of data and enabling data encryption and digital signatures [36]. Tools for access control and identity management such as role-based access control (RBAC) [37] and multi-factor authentication (MFA) [38] allow secure user authentication and restrict access to data. Additionally, frequent security audits and persistent monitoring are required to spot and promptly fix security concerns.

By offering a safe and decentralized method of storing and exchanging sensitive medical data, blockchain has the potential to transform the healthcare sector. Before there can be broad acceptance, there are still issues that need to be resolved. They consist of statutory and regulatory frameworks, interoperability problems, and the need for uniform protocols [39].

2.3. Privacy in Healthcare

Many issues in healthcare have been identified as possible candidates for blockchain technology solutions, including enhancing the security and privacy of patient data [17]. Since medical records include sensitive information that needs to be kept private, privacy is a crucial issue in the healthcare industry. Patients may suffer as a result of unauthorized access to such data, and healthcare professionals may face legal repercussions.

Blockchain technology offers certain advantages that make it a desirable choice for boosting healthcare privacy. It is a decentralized and distributed ledger, which means that data are spread among several network nodes. As a result, there is less chance of a centralized point of failure or attack target. Second, blockchain technology enables the development of smart contracts that can automate data sharing and enforce privacy laws [14]. The ability to encrypt and pseudonymize data stored on a blockchain allows for the protection of personal information while still enabling authorized parties to access the essential data.

Blockchain technology has the potential to enhance patient privacy, but some issues need to be resolved. The interoperability of various blockchain platforms is one of the biggest issues since healthcare providers may be utilizing dissimilar systems that cannot connect [40]. Another difficulty is the complexity of putting blockchain technology into practice, which calls for resources and technological know-how that may not be accessible in all healthcare settings.

Blockchain technology combines several privacy-enhancing technologies to bolster the security of sensitive patient data. Healthcare data may be sent and stored securely thanks to encryption, with access limited to those with the necessary decryption keys who are permitted to do so. Smart contracts' consent management allows patients to choose exactly who may access their data, aligning healthcare data governance with patient preferences [18,41].

The use of zero-knowledge proofs on the blockchain offers a novel way to validate information without revealing the underlying data, thus enhancing data secrecy [42]. The idea of off-chain data storage is crucial for very sensitive data, guaranteeing that crucial information is kept outside the blockchain with just a reference (cryptographic hash) recorded there, reducing the danger of data disclosure [43]. Blockchain adds a further degree of anonymity by identifying transactions with cryptographic addresses rather than real-world identities, working in combination with various privacy-enhancing technologies. This pseudonymity increases patient confidentiality by making it less likely that private infor-

mation will be connected to particular blockchain transactions [44]. Blockchain improves transparency and accountability in healthcare data management by automating consent management and data access rights. This not only assures regulatory adherence but also offers an auditable record of data treatment [45].

In conclusion, by offering a decentralized and secure platform for storing and exchanging patient data, blockchain technology can potentially improve healthcare privacy. Before blockchain technology is extensively used in healthcare settings, several issues need to be resolved.

2.4. Data Interoperability and Standards in Healthcare Blockchain

The key technological hurdle in using blockchain technology in the healthcare industry is interoperability [46]. The seamless interchange of healthcare data is made more difficult by the diverse character of healthcare systems, each of which uses different electronic health record (EHR) systems and medical equipment with their own specific data formats and standards. It takes careful planning and data translation to integrate these many systems into a blockchain network. This difficulty is exacerbated by legacy systems that are inherently incompatible with blockchain technology [47].

Several possibilities and solutions exist to overcome these interoperability issues and realize the full potential of blockchain in healthcare. The creation of standardized data models and standards for healthcare data inside blockchain networks is one viable route. To provide a common language for data across various systems, these standards include standardized data formats for patient records, prescription information, test findings, and more [48].

Middleware, which permits connection between existing systems and blockchain networks, is another essential element [49]. These solutions make data translation and transmission between formats simple. Building consensus on data standards is also crucial. Collaboration between healthcare organizations, regulators, and technology providers is essential to develop these standards and lay the foundation for efficient data exchange and interoperability [50].

The use of blockchain-based identity management solutions may improve data security and interoperability [51]. These systems provide a safe basis for data transmission by discretely handling patient identities and access rights. The integration process is also made easier by systems that can map and translate data from diverse sources into a uniform format for blockchain [52]. Planning, data transformation, standards consensus, middleware solutions, cooperation, and identity management are just a few of the strategies shown in Figure 2 for overcoming interoperability issues in healthcare blockchain integration.

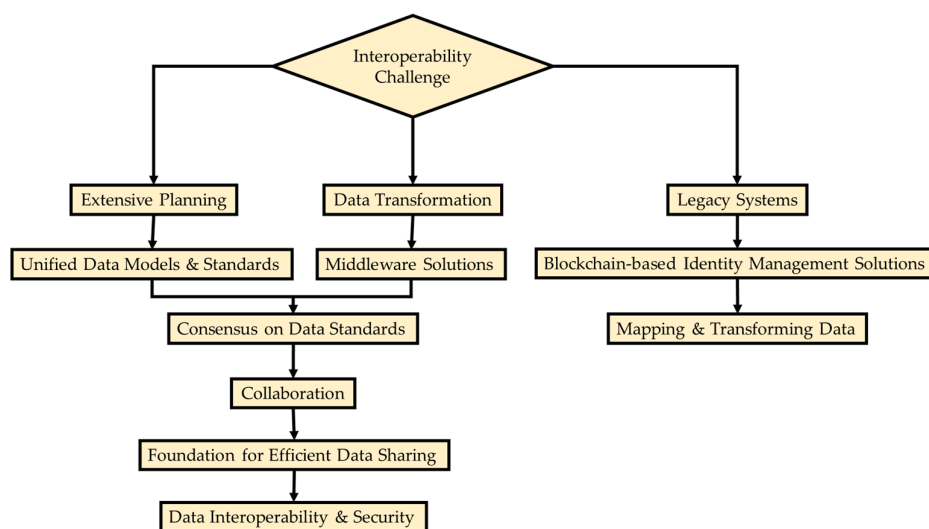


Figure 2. Blockchain in healthcare: interoperability challenges and solutions.

3. Methods

3.1. Data Acquisition

The Scopus database was used to find the study data. Scopus is recognized as one of the most thorough databases, and its dataset includes some of the most reliable literature. In this research, publications about blockchain, security and privacy, and healthcare were searched for and further examined on 14 March 2023.

3.2. Search Terms

The search phrases listed in Table 1 below were combined and then entered into the Scopus database search engine, which discovered articles mentioning these searched items to appear in the associated publications.

Table 1. Search keywords.

Term String	Keywords	Type
Term string 1	"Blockchain" AND "Healthcare" AND "Security"	Search within "article title"
Term string 2	"Block-chain" AND "Healthcare" AND "Security"	Search within "article title"
Term string 3	"Blockchain" AND "Health" AND "Security"	Search within "article title"
Term string 4	"Block-chain" AND "Health" AND "Security"	Search within "article title"
Term string 5	"Blockchain" AND "Medical" AND "Security"	Search within "article title"
Term string 6	"Block-chain" AND "Medical" AND "Security"	Search within "article title"
Term string 7	"Blockchain" AND "Healthcare" AND "Privacy"	Search within "article title"
Term string 8	"Block-chain" AND "Healthcare" AND "Privacy"	Search within "article title"
Term string 9	"Blockchain" AND "Health" AND "Privacy"	Search within "article title"
Term string 10	"Block-chain" AND "Health" AND "Privacy"	Search within "article title"
Term string 11	"Blockchain" AND "Medical" AND "Privacy"	Search within "article title"
Term string 12	"Block-chain" AND "Medical" AND "Privacy"	Search within "article title"

3.3. Inclusion and Exclusion Criteria

Inclusion criteria

- I. Studies were released between 2017 and 2022.
- II. The journal serves as the only domain of the research.
- III. Both privacy and security should be the main topics of research.
- IV. Articles that proposed a system, model, or framework.

Exclusion criteria

- I. The removal of articles in the press.
- II. Non-English-language articles.
- III. Exclusion of book chapters, dissertations, monographs, conferences, reviews, and works based on interviews.
- IV. Case studies

3.4. Selection

There were 331 Scopus results checked out. There were 65 that warranted further examination (Figure 3).

3.5. Limitations

Seldom do critical assessments offer a thorough analysis of all relevant material. They are unable to judge the quality of the selected studies, especially qualitative studies that lack a design hierarchy [53]. Also, it is common for critical evaluations to skip describing the general research strategy, the technique for eliminating and including articles, the limitations of the search strategy, the efficiency of the search process, and the analytical methodology [54,55]. The review procedure is constrained by this review database, known as Scopus.

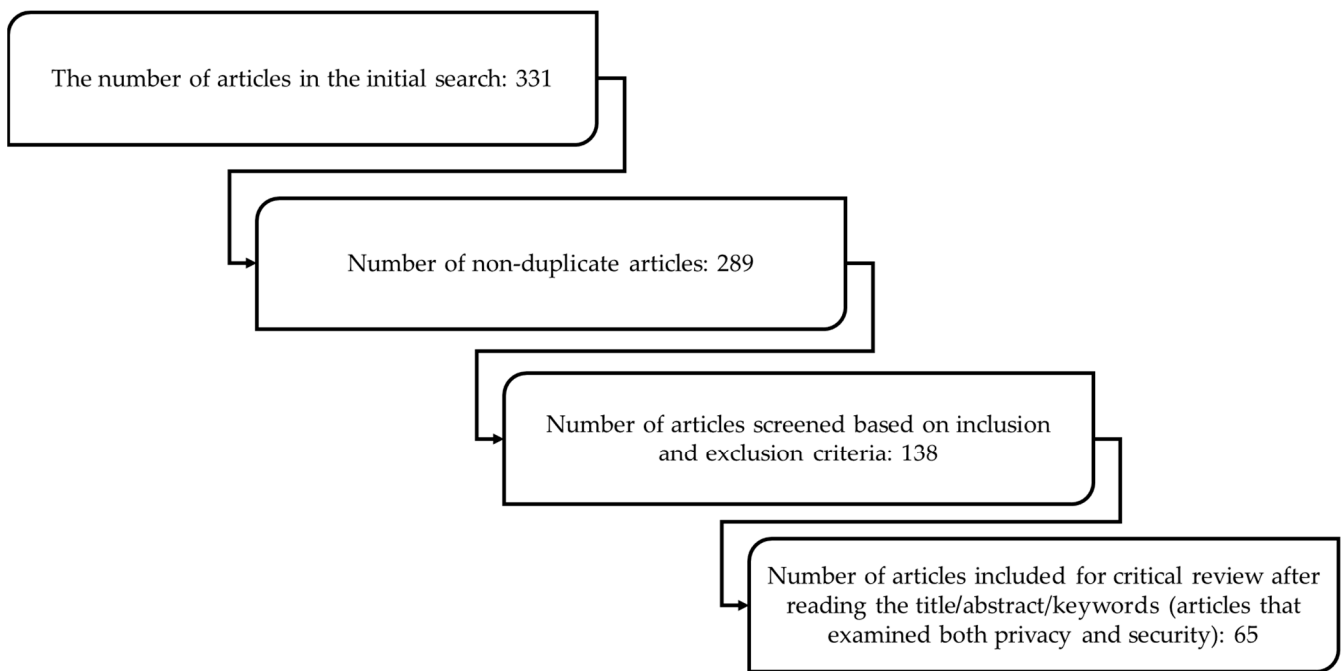


Figure 3. Selection process.

4. Results and Discussion

To guarantee data privacy, security, and integrity in the healthcare sector, the outcomes described above utilize blockchain and cryptography technology. These studies often strive to address long-standing privacy and security problems in the sector. The findings demonstrate the capability of these technologies to share and restrict access to medical data safely and effectively while protecting the privacy of both patients and doctors. The suggested protocols meet the anticipated security criteria while having competitive computation and communication costs.

A new paradigm for exchanging medical picture data through a decentralized network is made possible by the use of blockchain and federated learning in the research by Kumar et al. [56]. The InterPlanetary File System-based infrastructure that has been developed for off-chain storage of health data enables the healthcare system to remain extremely secure, scalable, and resilient while still preserving patient privacy. The findings show that transmitting data to the blockchain has an influence mostly on execution time and computing effort, which is reasonable given the privacy and security that the architecture and encryption offer [57–61].

Several studies [62–67] suggested solutions that put the patient in control of approving and denying access rights, which make it simple for healthcare practitioners and organizations to adhere to privacy laws. The suggested solutions also provide safe payment procedures, enabling both individuals and hospitals to dependably pay for diagnostic and storage services.

The suggested techniques can withstand a variety of assaults, including impersonation, collusion, and man-in-the-middle attacks, according to a security analysis and extensive experimentation. The findings also show that the suggested solutions have strong anti-attack capabilities, balanced storage space allocation, and high-security encryption performance, all of which enhance the storage and transmission of health privacy data both within and outside the healthcare system.

In the Internet of Medical Things (IoMT) situations, the suggested solutions make use of customized smart contracts and modified attribute-based cryptographic primitives to ensure safe search, privacy preservation, and individualized access control. One of the constraints of sensor nodes in the Internet of Things (IoT) devices is space, hence the method in some of the research has been space-optimized [68]. The results of a study by

Yugha et al. [68] showed that the suggested approach provides a safe and efficient method for facilitating the efficient exchange of IoT medical data while protecting patient privacy.

The aforementioned studies demonstrate the promise of blockchain and cryptography technologies for safe, private, and effective access control and healthcare data exchange. The suggested methods are appropriate for IoMT applications because they have competitive computation and communication costs while meeting anticipated security requirements. The outcomes show that these technologies are practical and efficient in resolving long-standing privacy and security problems in the healthcare sector. Figure 4 shows the papers' implications for healthcare privacy and security.

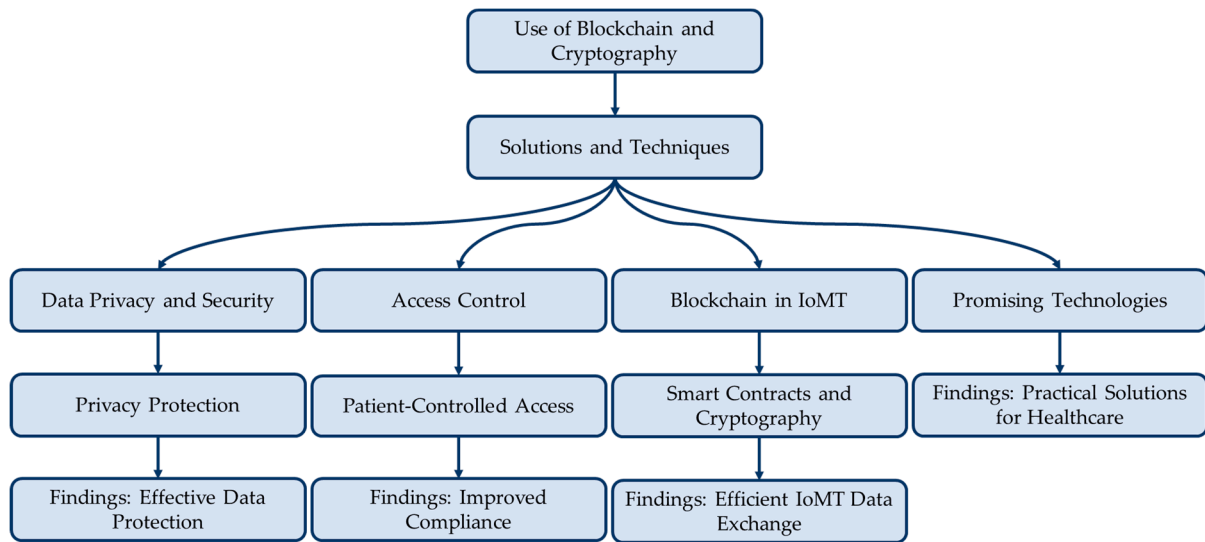


Figure 4. Privacy and security in healthcare with blockchain and cryptography.

Research question 1: What healthcare-related blockchain applications for security and privacy are there?

The safety and privacy of patient information are major issues in the healthcare sector. To safeguard patients' rights and prevent data breaches, electronic health records (EHRs) need to be secure and private since they include sensitive and private information about patients. Blockchain technology is one use that may enhance EHR security and privacy. EHR systems built on blockchain technology may provide a safe and unhackable platform for exchanging and storing patient data (Table 2). The decentralized nature of the blockchain can prevent data breaches and guarantee data integrity, while the use of smart contracts and cryptocurrency payments can guarantee that only authorized users have access to the data. Patient-controlled access is another example in which patients may decide who has access to their data and give or remove that access as necessary (Table 3). By enabling patients to give or cancel access to their data at any moment and guaranteeing that it is only available to authorized parties, access control utilizing blockchain technology may also enhance data privacy. Neither of them demonstrates the utilization of smart contracts.

Table 2. Health records applications.

Use Case	Smart Contract	Reference
EHRs		[69]
Personal health record (PHR) management and sharing		[57]
EHR management		[58]
EHR blockchain technology		[70]
EHR privacy using blockchain		[71]
EHR and service automation		[72]

Table 2. *Cont.*

Use Case	Smart Contract	Reference
EHR system with smart contract and cryptocurrency payments		[73]
PHR		[74]
EHR sharing		[75]
Patient record management		[76]

Table 3. Access control.

Use Case	Smart Contract	Reference
Patient-controlled access		[62]
Access control		[63]
Access control for healthcare data using blockchain		[64]
Medical records access		[65]
Healthcare data gateway		[66]
Medical care information preservation using extended chaotic map technology		[67]

Strong security and privacy safeguards are also needed for PHR administration and sharing. PHRs, which include medical histories, test findings, and diagnoses, contain sensitive information about individuals’ health. The privacy of patients can be secured, and only authorized people can access the data with the help of blockchain-assisted data sharing (Table 4). The exchange of EHRs can also protect privacy, and the security and privacy of healthcare data can be increased by using privacy-preserving K-nearest neighbors (K-NN) training for IoT data [77,78]. Healthcare blockchain privacy may provide safe and unhackable platforms for storing and exchanging medical data, protecting the confidentiality and integrity of the information (Table 5). Authentication and permission for healthcare data on the blockchain can further increase data security and privacy, ensuring that only authorized individuals have access to the data (Table 6). Table 7 displays research works that concentrated on improving security measures. Additionally, other uses of the applications are presented individually in Table 8.

Table 4. Data management.

Use Case	Smart Contract	Reference
Health IoT data sharing		[62]
Secure data communication		[63]
Sharing		[79]
Medical data sharing		[80]
Blockchain-assisted data sharing		[81]
Medical data sharing		[82]
IoT-enabled privacy-preserving healthcare data transfer		[83]
Data sharing		[60]
Health information exchange		[84]
Secure sharing of medical data between multiple entities		[85]
Medical data sharing and privacy-preserving system		[86]
Healthcare data management		[87]
Collaborative medical decision-making		[88]
Healthcare big data management		[89]
Protected health information (PHI) sharing		[90]
Data transmission		[91]
Healthcare information management		[43]
Data storage		[59]
Blockchain-enabled COVID-19 medical record protection		[92]
Blockchain and AI-enabled medical data transmission		[93]

Table 5. Privacy enhancement.

Use Case	Smart Contract	Reference
Privacy preserving		[94]
Privacy enhancement		[95]
Privacy-preserving e-health system		[96]
Privacy-preserving data sharing		[97]
Privacy protection		[98]
Improved privacy-preserving location sharing in healthcare.		[99]
Medical-data privacy protection		[100]
Medical privacy protection		[101]
Privacy-preserving medical data sharing		[102]
Privacy-preserving electronic health data sharing		[61]
Privacy-preserving K-NN training for IoT data		[77]
Health data privacy		[103]
Privacy protection scheme for medical data		[104]
Healthcare blockchain privacy		[105]

Table 6. Authentication.

Use Case	Smart Contract	Reference
Authentication		[106]
PPBA authentication		[107]
Machine learning authentication		[78]
Identity authentication		[108]
Authentication and authorization for healthcare data on the blockchain		[109]
IoT: anonymity		[110]

Table 7. Security enhancement.

Use Case	Smart Contract	Reference
Security enhancement		[111]
Medical data security		[112]
Biomedical security		[113]
Collaborative analysis		[114]
Improved security and privacy in the patient healthcare framework		[115]

Table 8. Other applications.

Use Case	Smart Contract	Reference
Contact tracing		[116]
Verifiable data classification		[117]
Security and privacy in IoT healthcare		[68]
Federated learning		[56]

Research question 2: What are the blockchain's privacy and security problems in the healthcare industry?

Healthcare has severe privacy and security problems. Security and privacy are crucial problems in healthcare because of the sensitivity of medical data and the potential damage that unauthorized access or data breaches might bring to people or organizations. By offering a decentralized and secure platform for data exchange and storage, blockchain technology provides a remedy. Secure search and individualized access control are made possible by cryptographic primitives, while access control and data privacy are guaranteed by smart contracts.

By simulation and experimental research, several suggested solutions have been verified and analyzed, proving the viability, effectiveness, and security of these systems. Several

studies have shown that blockchain-based systems may retain competitive computing and communication costs while meeting anticipated security requirements. Other approaches, such as modified attribute-based cryptographic primitives and certificateless public-key encryption technology, have also proven successful in preserving privacy and enabling individualized access control in healthcare settings. However, healthcare practitioners and organizations need to carefully assess these solutions to make sure they adhere to privacy laws and are practical and scalable in real-world contexts.

Research question 3: What is the potential for blockchain security and privacy in the medical industry?

In the coming years, it is anticipated that the healthcare sector will continue to prioritize enhancing security and privacy. Blockchain technology is being used more often as a method to safeguard healthcare data. User privacy is protected via a smart medical cloud platform where data may be utilized but not borrowed. To improve data security and privacy, one approach is the integration of new technologies like blockchain, federated learning, and edge computing. For instance, federated learning may enable collaborative data analysis without disclosing sensitive information, while blockchain technology can be utilized to provide secure access control and avoid data manipulation. Also, by processing data near its origin rather than sending it to a centralized place, edge computing may help lower the risk of data breaches.

Another possibility is implementing tougher rules and guidelines to guarantee private health information safety. It is more crucial than ever to protect health data from unwanted access and breaches as the volume of data grows. Regulations that attempt to safeguard the privacy and security of personal health information include the General Data Protection Regulation and the Health Insurance Portability and Accountability Act. Such laws and standards will probably keep being created and implemented to guarantee the security of health data in the future.

5. Research Directions and Applications

A wide range of intriguing research topics and useful applications are presented by the dynamic interaction of blockchain technology with the healthcare industry. The most pressing of them is the need to solve the interoperability and scalability issues. Researchers have to work hard to provide cutting-edge technologies that enable blockchain networks to effectively manage the sizable amount of healthcare data while ensuring smooth connection across various networks, thus promoting wider adoption.

Several intriguing future research avenues and applications become apparent. Healthcare blockchain networks should prioritize scalability and interoperability to provide effective data processing and smooth network connectivity. The security properties of blockchain may also be very useful for cross-border healthcare data transmission, especially in situations where foreign patients are being treated. By guaranteeing medication authenticity and patient safety, blockchain can also change the administration of the medical supply chain. Furthermore, by combining AI and blockchain, powerful data analytics capabilities may be unlocked while maintaining data privacy. Blockchain may provide safe solutions for patients to regulate data access and monetize their health information. Patients' permission and identity management demand attention. Blockchain technology may help healthcare businesses achieve compliance with laws, particularly those relating to data protection. Blockchain technology may improve the security of IoT medical equipment, protecting the integrity of patient data gathered by these devices. The user interfaces and seamless integration with the current healthcare infrastructure of blockchain-based EHRs and telemedicine systems may be improved. This article explores key study areas, illuminating how blockchain technology has the potential to revolutionize the healthcare industry.

6. Conclusions

The text explains how blockchain technology can be used in healthcare to address some of the long-standing challenges faced by the industry. Blockchain is seen as an innovative

solution that can help store medical data, perform medical transactions, and facilitate the integration and exchange of medical data in a decentralized open healthcare network. Despite the attention that blockchain has received in healthcare, there are still concerns about privacy and security when adopting this technology for information exchange. The paper presents research conducted on the subject of blockchain's privacy and security in healthcare from 2017 to 2022. The research review aims to evaluate the current state of affairs, with a specific focus on practical applications and difficulties.

The review concludes that blockchain technology has practical applications in resolving privacy and security issues in healthcare. By using blockchain technology, EHRs and PHRs can be more secure and private by providing a decentralized and unhackable platform for storing and exchanging sensitive patient information. Additionally, blockchain can enable patients to have greater control over who has access to their data through patient-controlled authentication. However, healthcare organizations and practitioners need to carefully assess the suitability of blockchain solutions in their particular contexts to ensure compliance with privacy laws and practicality. Despite its potential, blockchain technology is not a one-size-fits-all solution, and it may require customization to meet specific needs.

Overall, the review offers critical insights into the current state of blockchain's use in healthcare, and it highlights areas that require further research and development to advance the technology's applications in healthcare.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. McGhin, T.; Choo, K.-K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [[CrossRef](#)]
2. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [[CrossRef](#)]
3. Epiphaniou, G.; Daly, H.; Al-Khateeb, H. Blockchain and healthcare. In *Blockchain and Clinical Trial: Securing Patient Data*; Springer: Cham, Switzerland, 2019; pp. 1–29.
4. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
5. Kuo, T.-T.; Zavaleta Rojas, H.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478. [[CrossRef](#)] [[PubMed](#)]
6. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemeč Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [[CrossRef](#)]
7. Khan, F.A.; Gumaiei, A.; Derhab, A.; Hussain, A. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access* **2019**, *7*, 30373–30385. [[CrossRef](#)]
8. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
9. Yaqoob, S.; Khan, M.M.; Talib, R.; Butt, A.D.; Saleem, S.; Arif, F.; Nadeem, A. Use of blockchain in healthcare: A systematic literature review. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 644–653. [[CrossRef](#)]
10. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.; Tariq, M.A.; Rafferty, L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust. Comput.* **2020**, *23*, 2067–2087. [[CrossRef](#)]
11. Burniske, C.; Vaughn, E.; Cahana, A.; Shelton, J. *How Blockchain Technology Can Enhance Electronic Health Record Operability*; Ark Invest: New York, NY, USA, 2016.
12. Taherdoost, H. Blockchain-Based Internet of Medical Things. *Appl. Sci.* **2023**, *13*, 1287. [[CrossRef](#)]
13. Hasselgren, A.; Kravevska, 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](#)]
14. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.

15. Zhang, R.; Xue, R.; Liu, L. Security and privacy for healthcare blockchains. *IEEE Trans. Serv. Comput.* **2021**, *15*, 3668–3686. [[CrossRef](#)]
16. Roman-Belmonte, J.M.; De la Corte-Rodriguez, H.; Rodriguez-Merchan, E.C. How blockchain technology can change medicine. *Postgrad. Med.* **2018**, *130*, 420–427. [[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. Engelhardt, M.A. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [[CrossRef](#)]
19. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. [[CrossRef](#)]
20. Ma, S.; Deng, Y.; He, D.; Zhang, J.; Xie, X. An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain. *IEEE Trans. Dependable Secur. Comput.* **2020**, *18*, 641–651. [[CrossRef](#)]
21. Lin, C.; He, D.; Huang, X.; Khan, M.K.; Choo, K.-K.R. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2440–2452. [[CrossRef](#)]
22. Sultan, A.; Mushtaq, M.A.; Abubakar, M. IOT security issues via blockchain: A review paper. In *ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology*; ACM: New York, NY, USA, 2019; pp. 60–65.
23. Anwar, M.R.; Apriani, D.; Adianita, I.R. Hash Algorithm In Verification Of Certificate Data Integrity And Security. *Aptisi Trans. Technopreneurship (ATT)* **2021**, *3*, 181–188. [[CrossRef](#)]
24. Busayatananphon, C.; Boonchieng, E. Financial technology DeFi protocol: A review. In Proceedings of the 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Chiang Rai, Thailand, 26–28 January 2022; pp. 267–272.
25. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R.; Khan, S. A review of Blockchain Technology applications for financial services. *BenchCouncil Trans. Benchmarks Stand. Eval.* **2022**, *2*, 100073. [[CrossRef](#)]
26. Sexena, P.; Singh, P.; John, A.; Rajesh, E. Blockchain Powered EHR in Pharmaceutical Industry. In *Digitization of Healthcare Data Using Blockchain*; Wiley: Hoboken, NJ, USA, 2022; pp. 137–157.
27. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [[CrossRef](#)]
28. Khatri, S.; Alzahrani, F.A.; Ansari, M.T.J.; Agrawal, A.; Kumar, R.; Khan, R.A. A systematic analysis on blockchain integration with healthcare domain: Scope and challenges. *IEEE Access* **2021**, *9*, 84666–84687. [[CrossRef](#)]
29. Pirtle, C.; Ehrenfeld, J. Blockchain for healthcare: The next generation of medical records? *J. Med. Syst.* **2018**, *42*, 172. [[CrossRef](#)] [[PubMed](#)]
30. Paranjape, K.; Parker, M.; Houlding, D.; Car, J. Implementation considerations for blockchain in healthcare institutions. *Blockchain Healthc. Today* **2019**, *2*, 1–9. [[CrossRef](#)]
31. Chen, H.S.; Jarrell, J.T.; Carpenter, K.A.; Cohen, D.S.; Huang, X. Blockchain in healthcare: A patient-centered model. *Biomed. J. Sci. Tech. Res.* **2019**, *20*, 15017.
32. Mohanasundaram, S.; Ramirez-Asis, E.; Quispe-Talla, A.; Bhatt, M.W.; Shabaz, M. Experimental replacement of hops by mango in beer: Production and comparison of total phenolics, flavonoids, minerals, carbohydrates, proteins and toxic substances. *Int. J. Syst. Assur. Eng. Manag.* **2022**, *13*, 132–145. [[CrossRef](#)]
33. Sriram, G. Edge computing vs. Cloud computing: An overview of big data challenges and opportunities for large enterprises. *Int. Res. J. Mod. Eng. Technol. Sci.* **2022**, *4*, 1331–1337.
34. Hassan, N.H.; Ismail, Z. A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Soc. Behav. Sci.* **2012**, *65*, 1007–1012. [[CrossRef](#)]
35. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183. [[CrossRef](#)]
36. Das, S.; Namasudra, S. A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. *Comput. Electr. Eng.* **2022**, *101*, 107991. [[CrossRef](#)]
37. Rahman, M.U.; Guidi, B.; Baiardi, F.; Ricci, L. Context-aware and dynamic role-based access control using blockchain. In Proceedings of the Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020), Caserta, Italy, 15–17 April 2020; pp. 1449–1460.
38. Almadani, M.S.; Alotaibi, S.; Alsobhi, H.; Hussain, O.K.; Hussain, F.K. Blockchain-based multi-factor authentication: A systematic literature review. *Internet Things* **2023**, *23*, 100844. [[CrossRef](#)]
39. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [[CrossRef](#)]
40. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2021**, *34*, 11475–11490. [[CrossRef](#)]
41. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [[CrossRef](#)]
42. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5760–5772. [[CrossRef](#)]

43. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf. Process. Manag.* **2021**, *58*, 102535. [[CrossRef](#)]
44. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34. [[CrossRef](#)]
45. Liu, W.; Zhu, S.; Mundie, T.; Krieger, U. Advanced block-chain architecture for e-health systems. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; pp. 1–6.
46. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain technology use cases in healthcare. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41.
47. Appelbaum, D.; Cohen, E.; Kinory, E.; Stein Smith, S. Impediments to blockchain adoption. *J. Emerg. Technol. Account.* **2022**, *19*, 199–210. [[CrossRef](#)]
48. Alnafrani, M.; Acharya, S. SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking. *Health Policy Technol.* **2021**, *10*, 100510. [[CrossRef](#)]
49. Leng, J.; Chen, Z.; Huang, Z.; Zhu, X.; Su, H.; Lin, Z.; Zhang, D. Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions. *Machines* **2022**, *10*, 858. [[CrossRef](#)]
50. Hasan, M.R.; Deng, S.; Sultana, N.; Hossain, M.Z. The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges. *Libr. Hi Tech* **2021**, *39*, 814–833. [[CrossRef](#)]
51. Villarreal, E.R.D.; Garcia-Alonso, J.; Moguel, E.; Alegria, J.A.H. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access* **2023**, *11*, 5629–5652. [[CrossRef](#)]
52. Shae, Z.; Tsai, J. Transform blockchain into distributed parallel computing architecture for precision medicine. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; pp. 1290–1299.
53. Taherdoost, H. Towards Nuts and Bolts of Conducting Literature Review: A Typology of Literature Review. *Electronics* **2023**, *12*, 800. [[CrossRef](#)]
54. Grant, M.J.; Booth, A. A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Inf. Libr. J.* **2009**, *26*, 91–108. [[CrossRef](#)] [[PubMed](#)]
55. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [[CrossRef](#)]
56. Kumar, R.; Kumar, J.; Khan, A.A.; Zakria; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. *Comput. Med. Imaging Graph.* **2022**, *102*, 102139. [[CrossRef](#)] [[PubMed](#)]
57. 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](#)]
58. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* **2022**, *164*, 152–167. [[CrossRef](#)]
59. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. *J. Supercomput.* **2021**, *77*, 7916–7955. [[CrossRef](#)]
60. Majdoubi, D.E.; Bakkali, H.E.; Sadki, S. SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework. *J. Healthc. Eng.* **2021**, *2021*, 4145512. [[CrossRef](#)]
61. Chentharu, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE* **2020**, *15*, e0243043. [[CrossRef](#)]
62. Younis, M.; Lalouani, W.; Lasla, N.; Emokpae, L.; Abdallah, M. Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. *IEEE Syst. J.* **2022**, *16*, 3746–3757. [[CrossRef](#)]
63. 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](#)]
64. Alzubi, O.A.; Alzubi, J.A.; Shankar, K.; Gupta, D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4360. [[CrossRef](#)]
65. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [[CrossRef](#)]
66. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst.* **2016**, *40*, 218. [[CrossRef](#)] [[PubMed](#)]
67. Mohammad Hossein, K.; Esmaili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Comput. Commun.* **2021**, *180*, 31–47. [[CrossRef](#)]
68. Yugha, R.; Chithra, S.; Bhalaji, N.; Karthika, S. Privacy Protected IoT-Blockchain using ZKP for Healthcare application. *Control Eng. Appl. Inform.* **2022**, *24*, 76–87.
69. Barka, E.; Al Baqari, M.; Kerrache, C.A.; Herrera-Tapia, J. Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records. *J. Sens. Actuator Netw.* **2022**, *11*, 85. [[CrossRef](#)]
70. Boumezbeur, I.; Zarour, K. Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. *Acta Inform. Pragensia* **2022**, *11*, 105–122. [[CrossRef](#)]
71. Karunakaran, C.; Ganesh, K.; Ansar, S.; Subramani, R. A privacy preserving framework for health records using blockchain. *Pertanika J. Sci. Technol.* **2021**, *29*, 3081–3098. [[CrossRef](#)]

72. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [[CrossRef](#)]
73. Shanthashalini, K.; Nithya, M. Blockchain based healthcare system to ensure data integrity and security in green computing environments. *J. Green Eng.* **2020**, *10*, 10244–10260.
74. Thwin, T.T.; Vasupongayya, S. Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. *Secur. Commun. Netw.* **2019**, *2019*, 8315614. [[CrossRef](#)]
75. 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](#)]
76. Tith, D.; Lee, J.S.; Suzuki, H.; Wijesundara, W.M.A.B.; Taira, N.; Obi, T.; Ohya, N. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. *Healthc. Inform. Res.* **2020**, *26*, 3–12. [[CrossRef](#)] [[PubMed](#)]
77. Ul Haque, R.; Hasan, A.S.M.T.; Jiang, Q.; Qu, Q. Privacy-preserving k-nearest neighbors training over blockchain-based encrypted health data. *Electronics* **2020**, *9*, 96. [[CrossRef](#)]
78. Al-Otaibi, Y.D. K-nearest neighbour-based smart contract for internet of medical things security using blockchain. *Comput. Electr. Eng.* **2022**, *101*, 108129. [[CrossRef](#)]
79. Saidi, H.; Labraoui, N.; Ari, A.A.A.; Maglaras, L.A.; Emati, J.H.M. DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data. *IEEE Access* **2022**, *10*, 101011–101028. [[CrossRef](#)]
80. 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](#)]
81. 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](#)]
82. 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](#)]
83. Elhoseny, M.; Haseeb, K.; Shah, A.A.; Ahmad, I.; Jan, Z.; Alghamdi, M.I. Iot solution for ai-enabled privacy-preserving with big data transferring: An application for healthcare using blockchain. *Energies* **2021**, *14*, 5364. [[CrossRef](#)]
84. Lee, D.; Song, M. MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address. *IEEE Access* **2021**, *9*, 158122–158139. [[CrossRef](#)]
85. 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](#)] [[PubMed](#)]
86. Zou, R.; Lv, X.; Zhao, J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Inf. Process. Manag.* **2021**, *58*, 102604. [[CrossRef](#)]
87. Omar, A.A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gener. Comput. Syst.* **2019**, *95*, 511–521. [[CrossRef](#)]
88. Yang, J.; Onik, M.M.H.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. *Appl. Sci.* **2019**, *9*, 1370. [[CrossRef](#)]
89. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [[CrossRef](#)]
90. 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](#)]
91. Yang, H.; Shen, J.; Lu, J.; Zhou, T.; Xia, X.; Ji, S. A Privacy-Preserving Data Transmission Scheme Based on Oblivious Transfer and Blockchain Technology in the Smart Healthcare. *Secur. Commun. Netw.* **2021**, *2021*, 5781354. [[CrossRef](#)]
92. Huang, Z.; Guo, Y.; Huang, H.; Duan, R.; Zhao, X. Analysis and Improvement of Blockchain-Based Multilevel Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. *Secur. Commun. Netw.* **2022**, *2022*, 1926902. [[CrossRef](#)]
93. 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](#)]
94. Zhao, J.; Wang, W.; Wang, D.; Wang, X.; Mu, C. PMHE: A wearable medical sensor assisted framework for health care based on blockchain and privacy computing. *J. Cloud Comput.* **2022**, *11*, 96. [[CrossRef](#)]
95. de Moraes Rossetto, A.G.; Sega, C.; Leithardt, V.R.Q. An Architecture for Managing Data Privacy in Healthcare with Blockchain. *Sensors* **2022**, *22*, 8292. [[CrossRef](#)] [[PubMed](#)]
96. Zhang, G.; Yang, Z.; Liu, W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Comput. Netw.* **2022**, *203*, 108586. [[CrossRef](#)]
97. Xu, L.; Lin, M.; Feng, Y.; Sun, Y. BPDST: Blockchain-Based Privacy-Preserving Data Sharing on Thin Client for Electronic Medical Records. *J. Comput. Inf. Technol.* **2022**, *29*, 235–250. [[CrossRef](#)]
98. Upadhyay, S.; Kumar, M.; Kumar, A.; Karnati, R.; Mahommad, G.B.; Althubiti, S.A.; Alenezi, F.; Polat, K. Feature Extraction Approach for Speaker Verification to Support Healthcare System Using Blockchain Security for Data Privacy. *Comput. Math. Methods Med.* **2022**, *2022*, 8717263. [[CrossRef](#)] [[PubMed](#)]
99. Lee, T.F.; Chang, I.P.; Kung, T.S. Blockchain-based healthcare information preservation using extended chaotic maps for hipaa privacy/security regulations. *Appl. Sci.* **2021**, *11*, 10576. [[CrossRef](#)]

100. Wang, B.; Li, Z. Healthchain: A privacy protection system for medical data based on blockchain. *Future Internet* **2021**, *13*, 247. [[CrossRef](#)]
101. Wu, H.; Dwivedi, A.D.; Srivastava, G. Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. *ACM Trans. Multimed. Comput. Commun. Appl.* **2021**, *17*, 60. [[CrossRef](#)]
102. 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](#)]
103. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE Internet Things J.* **2019**, *6*, 8770–8781. [[CrossRef](#)]
104. Huang, L.; Lee, H.H. A Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8859961. [[CrossRef](#)]
105. Fu, J.; Wang, N.; Cai, Y. Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. *Sensors* **2020**, *20*, 1898. [[CrossRef](#)]
106. Jia, X.; Luo, M.; Wang, H.; Shen, J.; He, D. A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things. *IEEE Internet Things J.* **2022**, *9*, 21838–21850. [[CrossRef](#)]
107. Sarier, N.D. Privacy Preserving Biometric Authentication on the blockchain for smart healthcare. *Pervasive Mob. Comput.* **2022**, *86*, 101683. [[CrossRef](#)]
108. Wen, H.; Wei, M.; Du, D.; Yin, X. A Blockchain-Based Privacy Preservation Scheme in Mobile Medical. *Secur. Commun. Netw.* **2022**, *2022*, 9889263. [[CrossRef](#)]
109. Rao, K.R.; Naganjaneyulu, S. Permissioned Healthcare Blockchain System for Securing the EHRs with Privacy Preservation. *Ing. Des Syst. Inf.* **2021**, *26*, 393–402. [[CrossRef](#)]
110. Luong, D.A.; Park, J.H. Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK. *IEEE Access* **2022**, *10*, 55739–55752. [[CrossRef](#)]
111. Deshmukh, V.; Pathak, S.; Bothe, S. MobEdge: Mobile blockchain-based privacy-edge scheme for healthcare Internet of Things-based ecosystems. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e7210. [[CrossRef](#)]
112. Ranjith, J.; Mahantesh, K. Blockchain-based Knapsack System for Security and Privacy Preserving to Medical Data. *SN Comput. Sci.* **2021**, *2*, 245. [[CrossRef](#)]
113. Liu, H.; Crespo, R.G.; Martínez, O.S. Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts. *Healthcare* **2020**, *8*, 243. [[CrossRef](#)]
114. Zhou, Z.; Liu, Y. Blockchain-Based Encryption Method for Internal and External Health Privacy Data of University Physical Education Class. *J. Environ. Public Health* **2022**, *2022*, 7506894. [[CrossRef](#)]
115. Ali, A.; Rahim, H.A.; Pasha, M.F.; Dowsley, R.; Masud, M.; Ali, J.; Baz, M. Security, privacy, and reliability in digital healthcare systems using blockchain. *Electronics* **2021**, *10*, 2034. [[CrossRef](#)]
116. Zhang, C.; Xu, C.; Sharif, K.; Zhu, L. Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. *Comput. Stand. Interfaces* **2021**, *77*, 103520. [[CrossRef](#)]
117. Zheng, X.; Zhao, Y.; Li, H.; Chen, R.; Zheng, D. Blockchain-based verifiable privacy-preserving data classification protocol for medical data. *Comput. Stand. Interfaces* **2022**, *82*, 103605. [[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.