

Systematic Mapping Study: Blockchain Applied to Healthcare

Vitor Gonçalez Lindbergh(✉) and Itamir de Morais Barroca Filho

Federal University of Rio Grande do Norte, Digital Metropolis Institute, Natal, Rio Grande do Norte, Brazil
vitor.goncalez.054@ufrn.edu.br, itamir.filho@ufrn.br

Abstract. This study presents a systematic mapping of Blockchain technology in healthcare, aiming to provide an overview of the field and identify areas for future research. The research focuses on blockchain's characteristics, problems, platforms, and challenges in healthcare applications. An extensive search in the Scopus database resulted in 35 selected publications, which were analyzed to extract data. Findings highlight blockchain's transformative potential in healthcare, characterized by decentralized architecture, data security, and interoperability. The extracted data includes platforms and technologies used for architecture, engineering, and development of blockchain applications. Key challenges identified are scalability, interoperability, privacy concerns, and regulatory compliance. The study underscores blockchain's promise to improve healthcare data storage, sharing, and management but also emphasizes the need to address technical and regulatory challenges. It suggests a collaborative approach involving diverse stakeholders to optimize blockchain's healthcare implementation. The research is limited by its technical focus, potentially overlooking broader challenges in policy and regulations.

Keywords: Blockchain Healthcare · Blockchain Technology · Smart Contracts · DLT in Medicine · EHR Blockchain · Medical Data Interoperability · Healthcare Data Privacy

1 Introduction

The healthcare sector, a prime target for cybercriminals, has seen costly cyberattacks in the U.S., with breaches like Anthem Inc.'s affecting 78.8 million records. These attacks cause financial loss and jeopardize patient health when medical records become inaccessible. Healthcare organizations globally face numerous cyberattacks, particularly on networks and applications. Small healthcare entities often underestimate cybercrime risks and neglect cybersecurity, making them more susceptible. According to 2022 research, small healthcare organizations were twice as likely to be hit with cyberattacks. The most frequent causes of healthcare data breaches in the U.S. are hacking and IT security incidents, followed by unauthorized access or disclosure of sensitive information [31].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14815, pp. 178–195, 2024.
https://doi.org/10.1007/978-3-031-65154-0_11

With the advent of big data, the size and complexity of healthcare records are increasing, and they are still not optimized. The security of healthcare records is becoming increasingly crucial for protecting data from security breaches and criminal activity. If unauthorized users can gain access to patient data, it can be sold or leaked to the market, with patients' personal information being revealed to anyone with access [40].

Healthcare data requires a high level of security and privacy. Privacy refers to persons having the right to allow or disclose personal information to others. Data must always be free of threats and secure at all times. If these conditions are not met, the technologies used may not function correctly or be deemed reliable [40].

In this current context, constant care and attention to the data involved in the health sector are necessary. Technology advancement must benefit society. The application and feasibility of these new technologies must be studied and tested to bring greater security to all parties involved, be they hospitals, patients, doctors, or employees.

Blockchain is a technology that ensures data storage and transmission, is transparent and secure, and works without a central control entity. Being secured, decentralized, and distributed, Blockchain has become extremely popular in practically all domains. There is no need for a central authority to govern the network because it is decentralized. To obtain agreement among nodes, data are archived via a consensus process. The ledger is distributed, and it is maintained by all of the network's nodes. Blockchain security is achieved by many concepts, including cryptography, consensus mechanisms, immutability, replication, and data traceability [3].

In this research, a systematic mapping study is utilized to explore the use of Blockchain technology in Healthcare. While a systematic review is recommended to understand the current evidence on the subject, we initiate with a systematic mapping to gain a broad understanding of the field, as proposed by Petersen et al. [30].

Systematic Mapping Studies are designed to provide a broad overview of a research area, establish if research evidence exists on a topic, and indicate the quantity of the evidence. The mapping study results can identify areas suitable for conducting Systematic Literature Reviews and areas where a primary study is more appropriate [19].

The main goal of a Systematic Mapping study is to provide an overview of a research area and identify the quantity and type of research and results available within it [30]. Therefore, the systematic study encompasses a broader scope, making it suitable for preliminary exploration of a particular topic. Filtering research and papers based on research questions to extract, classify, and categorize data.

2 Method

This study aims to collect information regarding the use of blockchain technology in healthcare. This information is collected through previously defined research questions, which will direct the data collection to answer them. In this way, we seek to develop a state-of-the-art regarding the technology applied in the area and its future trends.

The methodology proposed [30] is applied to this study, which consists of developing a systematic mapping. A systematic mapping study provides a structure of the type of research reports and results that have been published by categorizing them. It often gives a visual summary, the map, of its results. It requires less effort while providing a more coarse-grained overview.

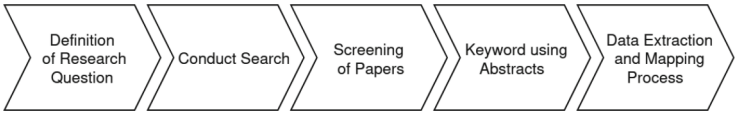

Fig. 1. The Systematic Mapping Process.

In the model presented in Fig. 1, the first step consists of defining the research questions. The second step is to query a database using a search string. Third, with a number of results returned, papers are screened. Fourth, a selection is done by reading research abstracts without going deeper into the work. Finally, data extraction is done with analysis and deepening in the remaining selected research.

Following this process, divided into stages, the search is expected to be directed to papers, works, and research that will accurately answer the defined questions.

2.1 Research Questions

Research questions must be elaborated as the first step to achieving the main objectives of systematic mapping research. These will serve as a study guide in search of the answers. The research questions addressed by this study are:

RQ1: *What are the main characteristics of healthcare applications based on blockchain?*

RQ2: *What problems do blockchain-based applications try to solve in healthcare?*

RQ3: *What are the blockchain platforms used in blockchain applications for healthcare?*

RQ4: *What are the challenges related to healthcare applications based on blockchain?*

While RQ1 and RQ2 are more general regarding the state of blockchain technologies today and what is expected in the future, RQ3 and RQ4 focus on more technical requirements regarding application development.

Search Process. The Scopus search base was used because it is one of the main research sources for the Computer Science subject area. Using the search string, quantitative information was collected regarding the area, type, and year of publication.

The search string filter was entered with search within Keywords. Results include publications in conferences, books, journals, magazines, etc. No year of publication range was added.

Despite having generic questions regarding definitions and challenges, the objective was to restrict the search through keywords to practical work involving architecture, engineering, and software development. For this, keyword categories were divided and defined:

- Technology.
  - Goal of Search: Related to blockchain technology.
  - Keywords: "blockchain" OR "DLT" OR "distributed ledger" OR "distributed ledger technology" OR "shared ledger"
- Development.
  - Goal of Search: Development-related search.
  - Keywords: "application" OR "architecture" OR "software" OR "system" OR "technology"
- Programming.
  - Goal of Search: Technical details of blockchain development and programming.
  - Keywords: "smart contract" OR "chaincode"
- Area.
  - Goal of Search: Related to the healthcare.
  - Keywords: "healthcare" OR "EHR" OR "EMR" OR "PHR" OR "electronic health record" OR "electronic medical records" OR "health" OR "personal health record"

The technology and area keyword categories must be clear, as they are the main themes of this work. The development category focuses on practical articles that encompass engineering and development. Programming focuses on specific technical details of blockchain development.

Contextualizing the keywords in the programming category: A smart contract is a computer program that stores rules for negotiating the terms of a contract. Programs can autonomously verify and execute contract-related agreements, reducing the cost of constructing and managing a centralized database [16]. In other words, smart contracts are how to program business rules on the blockchain. These rules run automatically as scheduled events and triggers occur. Chaincode is how smart contracts are called on the Hyperledger blockchain platforms. Smart contracts and chaincode are synonymous.

The search string is defined: ("blockchain" OR "DLT" OR "distributed ledger" OR "distributed ledger technology" OR "shared ledger") AND ("application" OR "architecture" OR "software" OR "system" OR "technology") AND ("smart contract" OR "chaincode") AND ("healthcare" OR "EHR" OR "EMR" OR "PHR" OR "electronic health record" OR "electronic medical records" OR "health" OR "personal health record")

Inclusion and Exclusion Criteria. The process of selecting articles involved eliminating those that did not fully address the research questions, aiming to curate a collection that aligns with the goals of this study. For this to be achieved, the exclusion criteria used were removing articles that do not address the search string, are not written in English, are not focused on infrastructure or blockchain technology, and have fewer than 5 pages. No date filter was applied, as the work intends to be as broad as possible, and the blockchain technology is still very recent [26].

Quality Assessment. According to CRD Guidelines and the Cochrane Reviewers' Handbook [19], the purpose of asserting a quality level for the studies is to minimize bias and maximize internal and external validity. Presenting the following points:

- Bias (Systematic error): A tendency to produce results that depart systematically from the 'true' results. Unbiased results are internally valid.
- Internal validity (Validity): The extent to which the design and conduct of the study are likely to prevent systematic error. Internal validity is a prerequisite for external validity.
- External validity (Applicability): The extent to which the effects observed in the study apply outside the study.

Detailed quality assessments are usually based on "quality instruments," which are checklists of factors that must be evaluated for each study. If quality items within a checklist are assigned numerical scales, numerical quality assessments can be obtained. Checklists are also developed by considering bias and validity problems that can occur at the different stages in an empirical study: Design, Conduct, Analysis, and Conclusions [19].

For the quality checklist, the following questions are defined [25]:

- Does the article clearly describe the purpose of the research?
- Does the article describe the literature review, background, or context?
- Does the article present related work?
- Does the article present an architecture proposal or a research methodology?
- Does the article contain research results?
- Does the article present a conclusion?

Data Collection. The data extracted to categorize the articles were authors, application context, publication year, journal, and keywords. As inputs for the research questions, the extracted data includes modern healthcare applications problems and challenges, blockchain platforms experimented with, blockchain applications and architecture definition and main characteristics, the technologies and frameworks used for developing blockchain in healthcare, and blockchain challenges that are yet to be overcome.

3 Results

This topic provides a comprehensive summary of the study's outcomes. It details every phase of its implementation and offers a broad summary of the articles and papers that were fundamental in addressing the research questions. That includes the stages for the selection, the articles list, publication year, and the word cloud of the articles' keywords.

3.1 Search Results

The research process is divided into 4 stages, as shown in Fig. 2.

In the first stage of the research, 364 works were obtained in the query result. In these, we applied the exclusion criteria of less than 5 pages, duplicated, not written in English, and out of the blockchain technology application context. In the second stage, the titles and abstracts of 190 works were read and analyzed, returning 46 publications to stage 3. In stage 3, the quality checklist was applied with a score, and 1 point was assigned to each question. Only studies that completed the entire quality checklist, with maximum marks (score = 6), were selected.

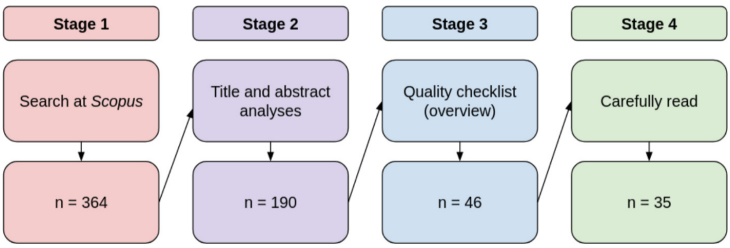

Fig. 2. Stages of the paper selection process.

In stage 4, the last one, all 35 selected articles and conference papers were carefully read and used to answer the defined research questions.

Articles list: Google sheets docs

3.2 Papers Overview

After 4 stages of the research process, this topic provides information about the 35 selected works.

Regarding the publication type of the papers, 86% of them are articles, and 14% are conference papers. As presented in Fig. 3, the data covers articles and papers from 2018 to 2023, reflecting a small range of publication timelines. Notably, there is a progressive increase in the number of publications each year from 2018 through 2022, starting with one article in 2018 and peaking at twelve in 2022. It is worth noting that this research was carried out in the second half of 2023. This must be considered when analyzing the number of articles selected from 2023.

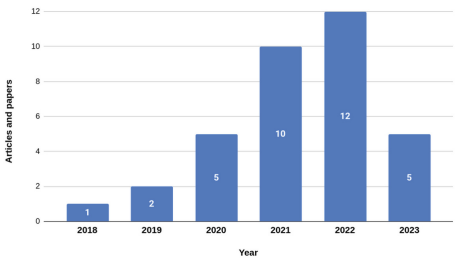

Fig. 3. Distribution of the selected works by year of publication.

Remarkably, the number of publications on the subject has increased in recent years. Although it was primarily implemented in economics with cryptocurrencies [26], the technology began to be tested in other sectors over the last few years, including the biomedical area. Blockchain technology can be witnessed in medicine, genomics, telemedicine, telemonitoring, e-health, neuroscience, and personalized healthcare applications by its mechanism of stabilizing and securing the data set with which users can interact through different types of transactions [32]. With greater popularity in the sector, more use cases are discovered, and technologies, frameworks, and tools are developed.

A word cloud was created with all the keywords extracted from the selected articles, shown in Fig. 4.

All works were developed in the health area and classified by specific themes to address blockchain technology, as shown in Table 1: Data storage and sharing, Internet of Things (IoT), 5G network, and machine learning.

This classification was made to categorize areas of blockchain research in healthcare: Research focused on blockchain and its data storage and sharing characteristics or its joint application with other information technology topics, such as networks or artificial intelligence. It is categorized by the level of detail that each work addresses each of these topics. As blockchain technology, all articles deal with security and data sharing, but if emphasis is placed on applications focused on sensors, for example, the research was classified in the IoT category.

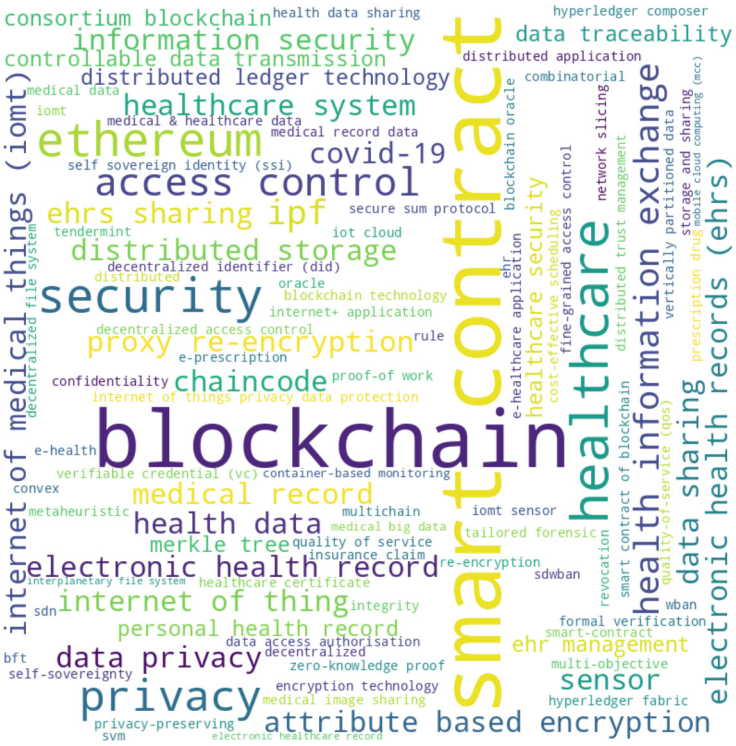

Fig. 4. Word cloud generated from the keywords of all selected works.

The works in the"Data storage and sharing" category address the development of applications in healthcare and specific characteristics of blockchain. These characteristics deal with how data is stored and shared in blockchain systems, permissions and access control, encryption, consensus mechanism, and network performance.

The articles categorized as "Internet of Things (IoT)" address blockchain-based applications and architecture to process, store, and manage healthcare data from sensors and devices. The article [13] approaches blockchain to secure network slicing (NS) in e-health environments and [38] attends a blockchain-based privacy-preserving support vector machine (SVM) classification for a COVID-19 Healthcare System, a machine learning topic.

4 Discussion

This research focused on the architecture, engineering, and development of blockchain applications in healthcare. In addition to answering blockchain's definitions, problems, and challenges, we sought information about how and what is being used in its development, obtaining details of applied technologies.

Table 1. Selected articles categories by the context of the application.

Category	Articles
Data storage and sharing	[1,2,4–12,15–18,23,24,27,29,34,35,37,39–41].
Internet of Things (IoT)	[3,14,20–22,28,33,36].
5G network	[13].
Machine learning	[38]

RQ1: What Are the Main Characteristics of Healthcare Applications Based on Blockchain? The main characteristics of healthcare applications based on blockchain, as derived from the provided answers, can be summarized under several key themes as follows.

Distributed Architecture and Decentralization: Blockchain's decentralized nature eliminates reliance on central authorities, reducing single points of failure and bottlenecks [5,15,36,39]. This architecture ensures data consistency and integrity by storing copies of data across multiple nodes [13,39].

Data Security and Privacy: Blockchain technology enhances data security through cryptographic algorithms and secure, tamper-proof data storage [9,23,34,41]. Smart contracts and distributed ledgers provide robust access control, ensuring that only authorized entities can access sensitive medical data [7,29,35,38].

Immutability and Traceability: Once data is recorded on a blockchain, it cannot be altered or deleted, ensuring the integrity and non-repudiation of medical records [6,8,17,28]. This feature is crucial for the provenance of records and patient-doctor interactions [23,27].

Data Sharing and Interoperability: Blockchain facilitates the secure and efficient exchange of health records among various stakeholders, promoting interoperability and patient-centric data management [8,10,14,16]. This aspect is especially relevant for integrating disparate systems and devices in the Internet of Medical Things (IoMT) [3,20,33].

Real-time Processing and Efficiency: Blockchain applications can support real-time disease detection, process scheduling, and efficient management of medical data [18,21,40]. The use of smart contracts automates various processes in the blockchain, enhancing the overall efficiency of healthcare systems [11,22,24].

Compliance and Legal Considerations: Blockchain applications can aid in meeting compliance requirements, such as those under the General Data Protection Regulation (GDPR), by providing transparent, verifiable, and secure data handling mechanisms [1,4,12].

Cost-Effectiveness and Scalability: By eliminating intermediaries and administrative overhead, blockchain can reduce operational costs and optimize processes in healthcare [2,8,40]. Combining blockchain with technologies like IPFS (InterPlanetary File System) addresses scalability issues [2,3,17].

Support for Clinical Research and Trials: Blockchain can facilitate clinical trial accountability, auditability, and data sharing, offering a trusted environment for medical research and large-scale data analysis [12,15].

Healthcare applications based on blockchain offer a transformative approach to managing health data. They enhance data security, integrity, and accessibility while providing a decentralized framework that fosters interoperability, real-time processing, cost-effectiveness, and support for legal compliance and research initiatives.

RQ2: What Problems Do Blockchain-Based Applications Try to Solve in Healthcare? Blockchain-based applications in healthcare are designed to address a variety of critical issues:

Privacy and Data Transparency: One of the primary issues blockchain aims to solve is the lack of transparency in how health data is collected, stored, and used [5,23]. This includes addressing the need for privacy and security in health data sharing and ensuring individual consent is explicitly obtained [5,36].

Fragmentation of Health Data: Patient information is often scattered across different locations and organizations, leading to fragmented, duplicated, and mismatched records [7,15,37]. Blockchain seeks to unify these disparate data sources, allowing for more coherent and efficient data management.

Security Concerns in Data Sharing: The theft of Electronic Health Records (EHRs) and data breaches are significant concerns in the current system due to poor security and policy enforcement [8,10,16]. Blockchain provides a more secure and reliable platform for sharing sensitive health information.

Centralization and Single Points of Failure: Traditional health informatics systems and IoT networks suffer from centralization, leading to single points of failure and control, which blockchain technology aims to eliminate [3,9,11,12,20,27,35,39].

Interoperability and Standardization Issues: Existing systems often lack uniform storage standards and efficient data exchange methods, resulting in silos of healthcare information [14,17,37,39]. Blockchain facilitates better interoperability and standardization across different healthcare systems.

Authenticity and Integrity of Medical Records: Blockchain applications strive to ensure the integrity and authenticity of medical records and prescriptions to prevent illegal or unauthorized use [1,6,11,29].

Efficiency and Cost-Effectiveness in Health Care Management: Issues like the high cost of healthcare services, inefficient task scheduling, and resource allocation in IoMT systems are addressed using blockchain for more secure, efficient, and cost-effective management [21,22,40].

Trust Issues, Verification, and Compliance with Legal and Regulatory Standards: Blockchain technology is applied to overcome trust and verification issues

in health data sharing and transactions [1,2,14]. Blockchain applications can help ensure compliance with privacy laws such as GDPR, addressing concerns about data protection, minimization, transfer, and storage [4].

Scalability and Performance Challenges: With the growing volume of healthcare data and increased use of IoMT devices, scalability becomes a critical issue, which blockchain technology addresses through decentralized data management [13,24,36].

Blockchain-based applications in healthcare seek to improve data transparency, security, interoperability, and efficiency while addressing the challenges of data fragmentation, centralization, compliance, and trust in the healthcare sector.

RQ3: What Are the Blockchain Platforms Used in Blockchain Applications for Healthcare? Various blockchain platforms and technologies are utilized in blockchain applications for healthcare, each offering specific features and capabilities suitable for different healthcare needs. Data extracted regarding platforms and technologies are listed below and in Table 2, highlighting the main ones mentioned.

Hyperledger Fabric: Widely used for its modular and versatile framework, Hyperledger Fabric is a preferred choice for many healthcare applications [5,7,8,11,12,15,28,39,40]. It often employs smart contracts (Chaincode) and integrates with other technologies like IPFS for decentralized file storage and Docker for containerization.

Ethereum: Ethereum is another popular platform due to its robust smart contract capabilities and Ethereum Virtual Machine (EVM) [1–4,6,9,10,13,14,16,17,20,22–24,27,29,33–36,41]. It is frequently used alongside IPFS for decentralized storage and tools like Remix IDE, MetaMask, Truffle for development and deployment, and Ganache for blockchain network setup [4,35,36].

InterPlanetary File System (IPFS): IPFS is widely used in conjunction with blockchain platforms like Ethereum and Hyperledger Fabric for efficient and secure decentralized storage of healthcare data [1–3,5,7–9,13,16,17,20,23,24,27,29,35,37,39]. It is a protocol and is commonly used for data storage, while blockchain stores the address for the data in a hash format, responsible for accessing the data.

Hyperledger Indy, Aries, and Ursa: These Hyperledger frameworks are used for identity management and transaction interactions, providing tools for storing, transmitting, and verifying digital credentials [34].

Oracles: Oracles like Chainlink insert real-world data into the blockchain [13].

Cryptography and Security Protocols: Technologies like Threshold Proxy Re-Encryption (TPRE) and public key encryption are used for enhancing data security and privacy [5,8,23,24].

Cloud Computing and Virtualization: Platforms like Amazon Web Services (AWS) are used for cloud computing (Virtual machines, Function-as-a-Service, etc.) and deploying blockchain nodes [4,9,12,27], while virtualization tools like

Kubernetes facilitate the dynamic use of resources [13,24]. Docker and Docker Compose are used for containerization and deployment [13,24,28,34,39,40].

Consensus Mechanisms: Various consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerant (BFT) mechanisms are employed for securing transactions and maintaining the blockchain [13,21, 24,37]. The choice of the consensus algorithm is based on business logic and technical architecture. It influences the speed of validation and inclusion of new data (blocks) into the blockchain, affecting the system's scalability.

Programming Languages and Custom Solutions: For smart contract development, Solidity programming language [1,2,4,6,9,10,13,14,16,17,20,24,27,29, 33–36,41], Go and Rust [5,8,11,12,28]. Custom blockchain solutions are developed in other programming languages, like Python [38] and Java [27,37], and are tailored to specific healthcare needs. Additional tools and frameworks include Node.js for backend development and interaction with the blockchain [3,13,34,36,39].

Blockchain applications in healthcare leverage various platforms and technologies, each contributing unique features such as secure data handling, smart contract functionality, decentralized storage, and identity management. These technologies are integrated to create robust, secure, and efficient systems for managing healthcare data and processes.

RQ4: What Are the Challenges Related to Healthcare Applications Based on Blockchain? Healthcare applications based on blockchain face several challenges that impact their scalability, efficiency, and practical implementation.

Scalability and Data Management: A significant challenge is handling the increasing volume of data on the blockchain, which can burden the system and affect scalability. This issue is aggravated by blockchain's data redundancy and the need for modern large-scale data processing [1,35,39,41]. Storing large amounts of data directly on the blockchain is often impractical [10,14,16,27].

Interoperability and Integration: Ensuring interoperability among different blockchain systems and integrating them with existing health IT systems is a significant challenge [20,23,36,37]. The lack of interoperability between different blockchain networks and the challenge of synchronizing interacting blockchains are significant, especially in multi-blockchain architectures [18,24,27]. This includes the difficulty of managing multiple deployments of smart contracts and achieving seamless communication between various blockchain platforms and healthcare applications.

Security and Privacy Concerns: While blockchain enhances data security, there are concerns about maintaining the privacy of sensitive health information. This includes the risk of privacy leakage when using public blockchains [2,6,9,27] and the challenges in device authentication and protecting data from unauthorized access [1,33].

Smart Contract Complexity and Limitations: The complexity of writing and managing smart contracts, particularly in terms of encoding complex data access

Table 2. Main blockchain technologies used on healthcare applications.

Category	Technology	Papers
Platform	Ethereum	[1–4,6,9,10, 13,14,16, 17,20,22– 24,27,29, 33–36,41].
Platform	Hyperledger Fabric	[5,7,8,11, 12,15,28, 39,40].
Protocol	InterPlanetary File System (IPFS)	[1–3,5,7– 9,13,16,17, 20,23,24, 27,29,35, 37,39].
Smart contracts programming language	Solidity	[1,2,4,6,9, 10,13,14, 16,17,20, 24,27,29, 33–36,41].
Smart contracts programming language	Go and Rust[a]	[5,8,11,12, 28].
Application programming language	Node.js	[3,13,34,36, 39].
Application programming language	Python and Java[a]	[27,37,38]

[a] A few papers deploy those languages; some use both in the same research, so they were put in the same category.

policies, is a challenge [5,11,38,41]. Moreover, the immutable nature of smart contracts raises issues regarding their upgradability and flexibility [23,29].

Regulatory and Compliance Issues: Ensuring compliance with laws and regulations such as GDPR is a challenge, especially considering the immutable nature of blockchain, which can conflict with data removal requests [18,23,24]. Meeting governmental policies and standards also adds complexity to blockchain implementations in healthcare [36].

Resource Efficiency, Energy Consumption, and Economic Considerations: Blockchain networks, particularly those using consensus mechanisms like Proof of Work, can be resource-intensive and require significant computational power [1,13,21,34]. The economic costs associated with transactions on the blockchain and the need for appropriate incentive models for participation are concerns, especially in public blockchains [1,13,28,29]. Furthermore, writing data to public blockchains can be expensive due to limited space and high transaction costs. This has led to the exploration of off-chain storage solutions like IPFS, but balancing cost and speed remains a critical point [1,13,16].

Technical Challenges, User-Friendly Features, and Patient-Centric Control Trade-offs: The lack of user-friendly features for key management and the potential for users to forget their credentials pose challenges [23]. There are also technical hurdles in terms of integrating blockchain with mobile applications and other healthcare technologies [5,13,34]. Additionally, in patient-centric solutions, the trade-off between patient controllability and the overhead of managing data-sharing requests is a notable challenge [12].

While blockchain technology offers significant advantages for healthcare applications, such as enhanced security and decentralized data management, it also presents scalability, interoperability, privacy, technical complexity, regulatory compliance, and resource consumption challenges. Addressing these challenges is crucial for the successful implementation and widespread adoption of blockchain in healthcare.

5 Conclusion

The exploration of blockchain applications in the healthcare sector, as delineated through research questions RQ1 to RQ4, unveils a multifaceted landscape of opportunities and challenges. Blockchain technology, primarily recognized for its foundational role in cryptocurrencies, emerges as a transformative force in healthcare, offering novel approaches to data management, security, and interoperability.

The fundamental attractiveness of blockchain in the healthcare sector lies in its capacity to foster decentralized, transparent, and immutable record-keeping, guaranteeing system trustworthiness and integrity. As highlighted in RQ1, key characteristics of blockchain applications in healthcare include enhanced data security, improved interoperability, and patient-centric data management. The technology facilitates secure, real-time data exchange, reducing errors and discrepancies while combating fraud and operational inefficiencies. Smart contracts, integral to blockchain healthcare platforms, include business logic and automated processes, further enhancing system efficiency.

However, the implementation of blockchain in healthcare presents some challenges. RQ4 reveals that scalability is a significant hurdle, particularly in handling vast amounts of healthcare data. The immutability of blockchain, while advantageous for data integrity, complicates compliance with regulations like the GDPR, which mandates the right to be forgotten. This immutability brings

logic complexity to engineering and development, summed up to the complexity of smart contracts development and deployment. Additionally, there are challenges in integrating blockchain with existing healthcare IT systems.

Despite these challenges, the potential of blockchain to revolutionize healthcare data management is evident. Blockchain applications can potentially mitigate the fragmentation of patient data between different organizations, enhance the security and privacy of medical records, and improve the overall efficiency of healthcare systems. To fully realize this potential, however, there is a need for concerted efforts to address the identified challenges. This includes developing scalable blockchain solutions, creating user-friendly interfaces for key management, and ensuring compliance with privacy regulations.

In conclusion, blockchain technology is a healthcare innovation, promising a paradigm shift in storing, managing, accessing, and utilizing patient data. While the path forward is filled with technical, regulatory, and operational challenges, the intersection of blockchain with healthcare holds immense promise. Navigating the complexities and unlocking the full potential of blockchain in healthcare necessitates a collaborative approach involving technologists, healthcare professionals, policymakers, and patients.

6 Limitations of This Study

The search keywords can be considered a limitation in the study in the context that with the addition of words such as “smart contract” and “chaincode”, the search is directed to papers that involve development. This work sought to extract information about platforms, technologies, and development in blockchain, analyzing their application goals and challenges through research questions. Focusing on the technical part can be a limitation when the challenges of implementing blockchain systems include a broader scope, such as policy, legislation, and societal impacts.

7 Future Works

Despite these limitations, the use of blockchain technology in healthcare reveals a promising scenario that encourages cooperation between institutions and participants. It is a technically viable system that can bring positive returns to its users regarding the security and usability of their data. Therefore, we intend to continue our research and future work on data storage performance on blockchains compared to traditional database systems. We must analyze the new possibilities and challenges of working with data in a distributed and decentralized way, including ways of using this data as models for artificial intelligence.

References

1. Akkaoui, R., Hei, X., Cheng, W.: EdgeMediChain: a hybrid edge blockchain-based framework for health data exchange. IEEE Access **8**, 113467–113486 (2020)
2. Alnuaimi, A., Alshehhi, A., Salah, K., Jayaraman, R., Omar, I.A., Battah, A.: Blockchain-based processing of health insurance claims for prescription drugs. IEEE Access **10**, 118093–118107 (2022)
3. Azbeg, K., Ouchetto, O., Andaloussi, S.J.: Access control and privacy-preserving blockchain-based system for diseases management. IEEE Trans. Comput. Soc. Syst. **10**(4), 1515–1527 (2022)
4. Barati, M., et al.: Privacy-aware cloud auditing for GDPR compliance verification in online healthcare. IEEE Trans. Industr. Inf. **18**(7), 4808–4819 (2021)
5. Bigini, G., Zichichi, M., Lattanzi, E., Ferretti, S., D'Angelo, G.: Decentralized health data distribution: A DLT-based architecture for data protection. In: 2022 IEEE International Conference on Blockchain (Blockchain), pp. 97–104. IEEE (2022)
6. Cao, S., Zhang, Q., Wang, D., Xiangli, P., Zhang, X.: Hybrid smart contracts for privacy-preserving-aware insurance compensation. In: 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1533–1538. IEEE (2022)
7. Chelladurai, M.U., Pandian, S., Ramasamy, K.: A blockchain based patient centric electronic health record storage and integrity management for e-health systems. Health Policy Technol. **10**(4), 100513 (2021)
8. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F.: A Novel Blockchain Based Smart Contract System for eReferral in Healthcare: HealthChain. In: Huang, Z., Siuly, S., Wang, H., Zhou, R., Zhang, Y. (eds.) Health Information Science. HIS 2020. LNCS, vol. 12435. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61951-0_9
9. Chinnasamy, P., Albakri, A., Khan, M., Raja, A.A., Kiran, A., Babu, J.C.: Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system. Appl. Sci. **13**(6), 3970 (2023)
10. 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. Urban Areas **39**, 283–297 (2018)
11. Garcia, R.D., Zutião, G.A., Ramachandran, G., Ueyama, J.: Towards a decentralized e-prescription system using smart contracts. In: 2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS), pp. 556–561. IEEE (2021)
12. Gohar, A.N., Abdelmawgoud, S.A., Farhan, M.S.: A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IOT. IEEE Access **10**, 92137–92157 (2022)
13. Gonçalves, J.P.d.B., de Resende, H.C., Villaca, R.d.S., Municio, E., Both, C.B., Marquez-Barja, J.M.: Distributed network slicing management using blockchains in e-health environments. Mob. Netw. Appl. **26**(5), 2111–2122 (2021)
14. Hasan, K., Chowdhury, M.J.M., Biswas, K., Ahmed, K., Islam, M.S., Usman, M.: A blockchain-based secure data-sharing framework for software defined wireless body area networks. Comput. Netw. **211**, 109004 (2022)
15. Hylock, R.H., Zeng, X.: A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. J. Med. Internet Res. **21**(8), e13592 (2019)

16. Jabarulla, M.Y., Lee, H.N.: Blockchain-based distributed patient-centric image management system. Appl. Sci. **11**(1), 196 (2020)
17. Kaur, J., Rani, R., Kalra, N.: Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. Cluster Comput. **27**(1), 1–15 (2023)
18. Khan, A.A., et al.: QoS-Ledger: smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. Electronics **10**(24), 3083 (2021)
19. Kitchenham, B., Charters, S.: Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01, School of Computer Science and Mathematics, Keele University (2007)
20. 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. Supercomputing 1–40 (2021)
21. Lakhan, A., Mohammed, M.A., Elhoseny, M., Alshehri, M.D., Abdulkareem, K.H.: Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the internet of medical things (IoMT) in fog-cloud system. Soft. Comput. **26**(13), 6429–6442 (2022)
22. Lakhan, A., et al.: Smart-contract aware ethereum and client-fog-cloud healthcare system. Sensors **21**(12), 4093 (2021)
23. Madine, M.M., et al.: Blockchain for giving patients control over their medical records. IEEE Access **8**, 193102–193115 (2020)
24. Malamas, V., Kotzanikolaou, P., Dasaklis, T.K., Burmester, M.: A hierarchical multi blockchain for fine grained access to medical data. Ieee Access **8**, 134393–134412 (2020)
25. Mayer, A.H., Da Costa, C.A., Righi, R.d.R.: Electronic health records in a blockchain: a systematic review. Health Inf. J. **26**(2), 1273–1288 (2020)
26. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf
27. Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A.: Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access **7**, 66792–66806 (2019)
28. Nie, Z., Long, Y., Zhang, S., Lu, Y.: A controllable privacy data transmission mechanism for internet of things system based on blockchain. Int. J. Distrib. Sens. Netw. **18**(3), 15501329221088450 (2022)
29. Pericàs-Gornals, R., Mut-Puigserver, M., Payeras-Capellà, M.M.: Highly private blockchain-based management system for digital COVID-19 certificates. Int. J. Inf. Secur. **21**(5), 1069–1090 (2022)
30. Petersen, K., et al.: Systematic mapping studies in software engineering. In: 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), pp. 1–10 (2008)
31. Petrosyan, A.: Healthcare and cyber security in the u.s. (2023). https://www.statista.com/topics/8795/healthcare-and-cyber-security-in-the-us/#topicOverview. Accessed 23 Jan 2024
32. Rabah, K.: Challenges and opportunities for blockchain powered healthcare systems: a review. Mara res. j. med. health sci. **1**(1), 45–52 (2017)
33. Rahman, M.Z.U., Surekha, S., Satamraju, K.P., Mirza, S.S., Lay-Ekuakille, A.: A collateral sensor data sharing framework for decentralized healthcare systems. IEEE Sens. J. **21**(24), 27848–27857 (2021)

34. 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 **10**, 101011–101028 (2022)
35. Sharma, P., Borah, M.D., Namasudra, S.: Improving security of medical big data by using blockchain technology. Comput. Electr. Eng. **96**, 107529 (2021)
36. Sharma, P., Namasudra, S., Chilamkurti, N., Kim, B.G., Gonzalez Crespo, R.: Blockchain-based privacy preservation for IOT-enabled healthcare system. ACM Trans. Sens. Netw. **19**(3), 1–17 (2023)
37. Shuaib, K., Abdella, J., Sallabi, F., Serhani, M.A.: Secure decentralized electronic health records sharing system based on blockchains. J. King Saud Univ. Comput. Inf. Sci. **34**(8), 5045–5058 (2022)
38. Smahi, A., Xia, Q., Gao, J., Xia, H.: An efficient and secure blockchain-based SVM classification for a COVID-19 healthcare system. In: 2021 6th International Conference on Mathematics and Artificial Intelligence, pp. 122–129 (2021)
39. Sun, Z., Han, D., Li, D., Weng, T.H., Li, K.C., Mei, X.: MedRSS: a blockchain-based scheme for secure storage and sharing of medical records. Comput. Ind. Eng. **183**, 109521 (2023)
40. Tanwar, S., Parekh, K., Evans, R.: Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J. Inf. Secur. Appl. **50**, 102407 (2020)
41. Xu, B., Xu, L.D., Wang, Y., Cai, H.: A distributed dynamic authorisation method for internet+ medical & healthcare data access based on consortium blockchain. Enterp. Inf. Syst. **16**(12), 1922757 (2022)