

Review

Blockchain Application in Healthcare Systems: A Review

Pranto Kumar Ghosh ¹, Arindom Chakraborty ², Mehedi Hasan ³, Khalid Rashid ^{4,*} and Abdul Hasib Siddique ⁵

¹ Department of Electrical and Computer Engineering, North South University, Dhaka 1229, Bangladesh

² Department of Electrical and Electronic Engineering, University of Science and Technology Chittagong, Chattogram 4202, Bangladesh

³ Department of Electrical and Computer Engineering, University of Maryland-College Park, College Park, MD 20740, USA

⁴ Department of Chemical Engineering, University of Delaware, Newark, DE 19716, USA

⁵ Department of Electrical and Electronic Engineering, International University of Scholars, Dhaka 1212, Bangladesh

* Correspondence: khalidr@udel.edu

Abstract: In the recent years, blockchain technology has gained significant attention in the healthcare sector. It has the potential to alleviate a wide variety of major difficulties in electronic health record systems. This study presents an elaborate overview of the existing research works on blockchain applications in the healthcare industry. This paper evaluates 144 articles that discuss the importance and limits of using blockchain technologies to improve healthcare operations. The objective is to demonstrate the technology's potential uses and highlight the difficulties and possible sectors for future blockchain research in the healthcare domain. The paper starts with an extensive background study of blockchain and its features. Then, the paper focuses on providing an extensive literature review of the selected articles to highlight the current research themes in blockchain-based healthcare systems. After that, major application areas along with the solutions provided by blockchain in healthcare systems are pointed out. Finally, a discussion section provides insight into the limitations, challenges and future research directions.



Citation: Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. *Systems* **2023**, *11*, 38. <https://doi.org/10.3390/systems11010038>

Academic Editor: William T. Scherer

Received: 21 November 2022

Revised: 1 January 2023

Accepted: 4 January 2023

Published: 8 January 2023



Copyright: © 2023 by the authors. 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

High maintenance and management costs are the dire problems that modern healthcare systems face [1]. The healthcare system is highly complex, containing several domains, each comprising physicians, researchers, practitioners, supportive staff, management employees, and patients [2]. As a result, categorization and management of patient data becomes a daunting challenge [3,4]. This challenge is further exacerbated by dissimilar data structures and disparate workflows in different healthcare domains. For these reasons, the lack of efficient interchange of healthcare-related information among various healthcare domains poses a great hindrance [5].

To tackle health information records and exchange, a system is required to be developed, managed, and maintained. A third party develops and maintains traditional personal health record and electronic health record systems, with trust, privacy, and data security remaining important challenges [6]. However, the third-party-based existing healthcare recording systems cannot satisfy stakeholders' privacy needs [7]. As a result, the traditional electronic healthcare model lacks transparency because of privacy and data security issues.

In resolving the security-related concerns and the severe problem of enormous and highly diverse data in healthcare systems, blockchain technology offers significant prospects [8]. Blockchain is a decentralized, distributed database, peer-to-peer network, and digital ledger [9]. The blockchain could link many computers via nodes, and requires no transactions to build a new block that helps send safe information from one person to another. The client may

access all the allowed and verifiable medical-related information using a blockchain secured by cryptography. Anyone may choose transactions and also add a new chain to the block. The master key of a blockchain is a hash, and by using this hash function, a blockchain can generate unique identifiers for cryptocurrency to add data.

Since traditional electronic health record and personal health record-based health information exchange systems have failed to cope with privacy and security-related issues, stakeholders are hesitant about collaborating and co-operating for the exchange of health information. As a result, the cost of healthcare has increased, which is a great burden on both patients and healthcare providers. To solve these trust-related problems, researchers and policymakers nowadays are turning towards blockchain technology. As per IBM, many leading healthcare organizations predict blockchain will bring a significant change to the healthcare system by upgrading healthcare management systems and by establishing a decentralized architecture for the interchange of electronic healthcare information [10]. By 2022, the blockchain technology market is anticipated to account for over USD 500 million [11]. Although several studies on blockchain in the healthcare industry have been conducted, the existing literature cannot provide a comprehensive picture of the application areas. Therefore, it becomes inevitable to conduct an extensive study to explore the applications of blockchain in the healthcare industry. Many servers are now being built to provide services to clients via mobile devices. In this current time of internet services, it is possible to create and transmit a huge amount of medical data every week or daily by using mobile devices and many applications. The current healthcare system has the potential to solve limitations in a variety of fields, such as cost limitation, tactical limitation, maintaining standardization, and individual behavioral constraint to services [12]. However, healthcare system providers do not always use the latest advantage of the technology in the supply chain. For example, they do not use the new accumulation and distribution of medical supplies in the proper way. In fact, a report on Healthcare Finance revealed that nearly USD 25.7 billion is required every year for unnecessary supply management and operations [13]. A massive amount of work needs to focus on a smart healthcare system to improve the limitations and satisfy rising expectations for better healthcare. It could work on design and development issues based on smart devices, tools, better facilities, and an updated healthcare organization. It could also develop smart healthcare on customer-connected apps, biosensors and the most updated emergency service systems [14]. Therefore, to build a better network, we need to identify consensus algorithms that are already being used in many blockchain networks and determine which ones are compatible with IoT-based infrastructure for the improvement of healthcare services [15]. There is another way to mitigate the large data storage problem of blockchain with the faster data sharing process called Distributed Data Storage System (DDSS) [16]. It uses data caching and file translation to keep track of multiple documents with the same name in the same place. However, sometimes when a massive file is uploaded to DDSS, it reuses the file into several smaller data objects, for example, 256 kb, and also connects all these objects to an empty object to retrieve the complete file using Distributed Hash Tables (DHT) [17]. Some sensors can collect data automatically from users and can transfer them to a certain storage or cloud for further processing by physicians, nurses, and medical staff [18]. Several pieces of rules and regulations have been proposed to save individual patients' privacy. These laws always require appropriate security management for controlling, sharing, and exchanging the health of patient data, and failure to follow them is strongly prosecuted, with severe penalties being imposed on electronic healthcare systems (EHRs) [19]. According to the report by IBM, almost 70% of healthcare leaders foretell the huge impact of blockchain on the areas of health domain improvement and the clinical trial system, regulatory compliance, and creating a decentralized structure for sharing electronic health records (EHR) [20].

Because of the availability of better data security and management at lower cost, blockchain-based healthcare management systems are gaining more and more popularity both in practical and research sectors. Throughout the last decade, the research interest in blockchain-based healthcare systems has skyrocketed. For future research, there is a

lack of comprehensive information gathering and representation of the prior activities in this sector. Current review papers offer succinct summaries of recent developments in this field and highlight the benefits and drawbacks of the solutions put forth by academics. However, these review papers do not provide an extensive evaluation of multiple aspects of blockchain in healthcare system such as the research themes that are being followed, the areas of healthcare in which blockchain is mostly used for, applications of blockchain in certain areas and existing blockchain-based healthcare systems. For future research, there is a lack of comprehensive information gathering and representation of the prior activities in this sector. Current review papers offer brief summaries of recent developments in the blockchain-based healthcare system and highlight the benefits and drawbacks of the solutions put forth by academics. This research aims to conduct an extensive study of the existing literature and identify potential blockchain applications in various healthcare disciplines. This research also discusses the research direction, challenges and future research course in blockchain-based healthcare system. An exhaustive review of the existing literature to cluster the knowledge related to blockchain in healthcare is the ultimate contribution of this study.

2. Background Study of Blockchain

2.1. What Is BlockChain

Blockchain is a decentralized, unchangeable database that simplifies the tracking of assets and recording of transactions in a corporate network. A blockchain is made up of an expanding collection of documents, known as blocks that are safely connected to one another using encryption. Each block includes transaction information, a timestamp, and a cryptographic hash of the preceding block. The timestamp shows that the transaction data was there at the moment the block was produced. The blocks effectively create a chain since each block holds information about the one before it, making them interconnected. Thus, once a transaction has been recorded, it cannot be undone without also undoing all following blocks, rendering blockchain transactions irreversible.

2.1.1. Key Features

Decentralization is a key feature of blockchain technology. There is no central authority to control the content added to the blockchain, but rather the entry that enters the blockchain agrees to the peer-to-peer network and uses the various consensus minimization protocols here. This is further described in Section 2.1.4. Security of data is the main key focus of blockchain transaction. As data are transferred through blockchain without the involvement of any third parties, there is practically no risk of data theft or alteration. Persistence is another key feature of the blockchain. Entries can no longer be deleted once they have been recognized in the blockchain because of a shared ledger stored across many nodes [21]. In addition, an interesting feature of the pseudonymity blockchain is that it is used in many blockchains. Figure 1 illustrates the main features of blockchain technology.

Blockchain can be audited and traced to link a new block to the previous one. This is a way to form a chain of blocks. A Merkle tree is created for the transactions of blocks [22]. Each leaf value is verified and is called the root. This enables only the blockchain to preserve the root of the tree and verify the integrity of the tree structure. Figure 2 depicts the structure of blockchain technology.

2.1.2. Different Kinds of Blockchain

According to Table 1, we observe that there are three kinds of blockchain in general: private, public, and consortium [21]. There are different features depending on who can write, read, and access data on the blockchain. In public blockchain, chain data are visible to everyone, and there are opportunities for anyone to join and contribute, or even to change the original software if they wish [21]. Many places have made use of public blockchains. We see it being used a little more in cryptocurrencies. One of the two major cryptocurrencies is Bitcoin, which is discussed in [23], and the other is Ethereum, which is discussed in [24].

In a consortium blockchain, only a select number of groups can access it and participate in it. With private blockchain, this network can only be accessed and participated in from a central location; no one from the outside can access or participate in it [21]. There is still no definite idea about the definition and classification of blockchain types [25].

Table 1. Blockchain types and their properties.

Blockchain Type \ Properties	Private Blockchain	Consortium Blockchain	Public Blockchain
Efficiency	High	High	Low
Determination of consensus	An organization	Chosen node set	All miners
Constancy	Could be tampered	Could be tampered	Almost impossible
Centralized	Yes	Partial	No
Reading authorization	Public or restricted	Public or restricted	Public
Process of Consensus	Approved	Approved	Permissionless

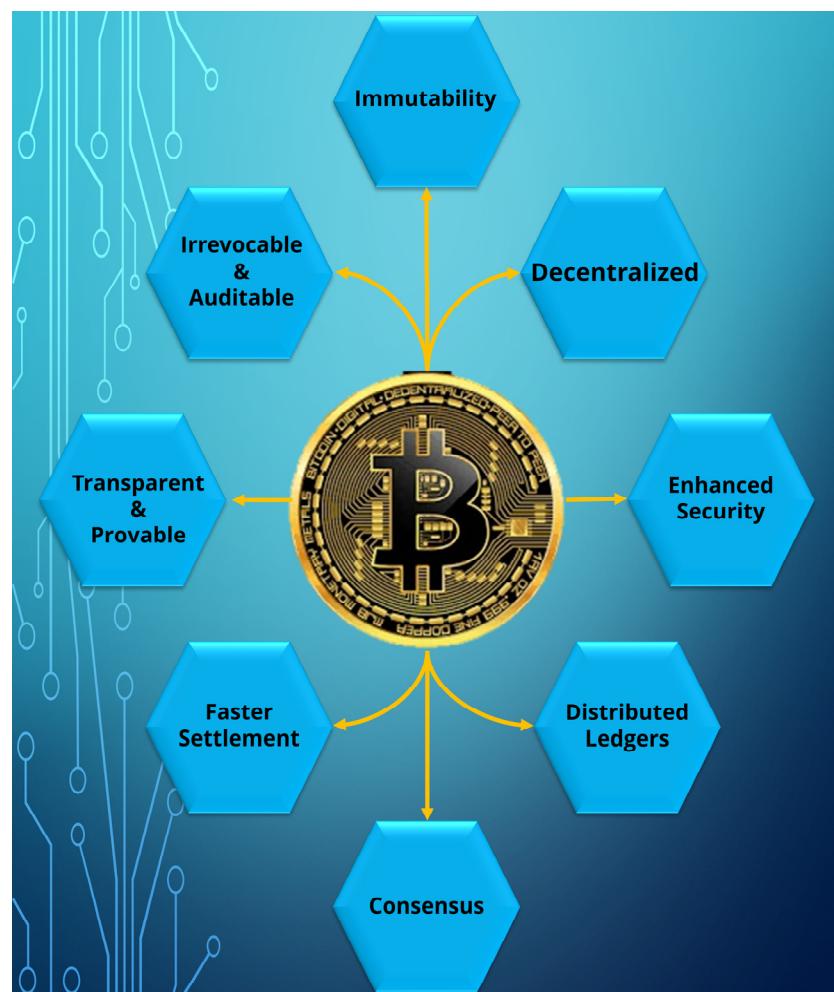


Figure 1. Key Features of Blockchain Technology.

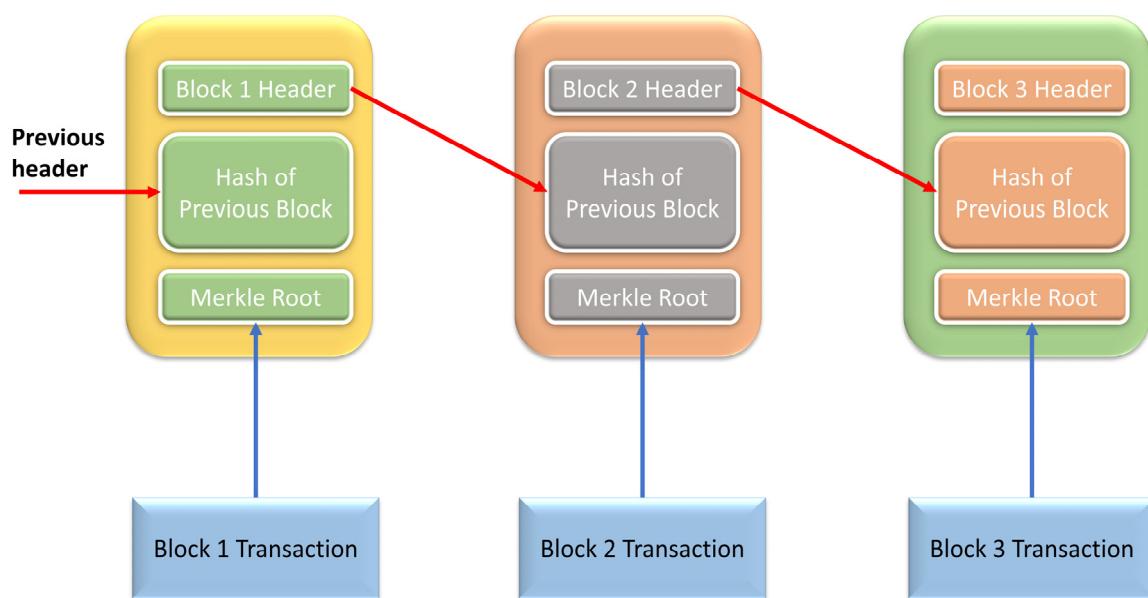


Figure 2. Blockchain structure.

2.1.3. Difference between Blockchain in Healthcare and General Sectors

Ever since its inception with the creation of Bitcoin, the primary use of blockchain has been monetary transactions. To that end, several other blockchain-based cryptocurrencies, such as Ethereum, Tether, BNB, Dogecoin, etc., have been created throughout the last decade. The decentralized, immutable, and safe nature of these cryptocurrencies has turned them into ideal choices for large-scale financial exchanges, including money lending and insurance.

The key difference between blockchain in healthcare and general applications of blockchain is that in the healthcare sector, the key usage of blockchain is to create safe and secure systems for patient or, so to say, user data management. The healthcare sector also utilizes a secure monetary transaction service based on blockchain.

The use of blockchain has evolved rapidly in recent years. A system that was created for cryptocurrencies is now being used to cast votes due to its temper-proof characteristics. The use of smart contracts enforces accountability for all parties involved and ensures the contract's integrity. The data security issue of IoT systems has been solved through the utilization of blockchain-based data communication and storage systems. The limit to the applicability of blockchain is the imagination of the user. While in this study, our focus is to review the impact of blockchain in the healthcare sector, there is no difference between the application of blockchain in healthcare and the general sector as the healthcare sector uses all the services offered by blockchain, such as money transfer, personal data security, logistics, and overall data safety.

2.1.4. Existing Blockchains

We can now use the blockchain framework or existing platforms to develop decentralized applications. The most popular are Hyperledger [26] and Ethereum [24], which both allow developers to construct new blockchain applications on top of current ones and request that they create new test nets using the protocol.

2.1.5. Mechanisms for Consensus

Data entries in a blockchain are accepted through distributed ledgers and distributed ledger data entry by a distributed consent protocol. Table 2 lists the three most widely used consensus protocols.

The proof-of-work consensus protocol is integrated with Bitcoin, which makes it highly connected with the blockchain. By applying the proof-of-work consensus protocol,

miners compete to resolve a computationally difficult riddle. The miners use brute force, looking for a hash of the suggested block that is of inferior quality to the predefined value. Among miners who calculate the value of the hash and receive a reward if the transaction is valid within the block, the big disadvantage of the proof-of-work consensus protocol is that, when a large blockchain is applied, it consumes huge amounts of power [27].

Proof-of-stake blockchain selects the node and uses part of the blockchain. With cryptocurrencies, stakes are the measure one occupies in a certain currency. It unfairly benefits the “rich” node. As an account of this, several versions of proof-of-stake blockchain are proposed to select the authorization node where the stake is associated with randomization. Ethereum plans to move from proof-of-work to proof-of-stake protocol [21]. We can observe that the practical tolerance of the Byzantine defect lies in the Byzantine Convention [28]. In practical Byzantine fault tolerance, the network of all nodes needs to be known, which eliminates the use of the practical Byzantine fault tolerance protocol in the universal blockchain. Practical Byzantine fault tolerance can be divided into three categories: committed, pre-prepared, and prepared. Here, if it is needed to move from all the nodes to these three stages, then (2/3) votes are required for each node. We observe that practical Byzantine fault tolerance is now used in Hyperledger Fabric [29].

Table 2. Comparison of consensus methods.

Possessions	PBFT	PoS	PoW
Management of nodes	Authorized	Accessible	Accessible
Adversarial tolerance	Faulty replicas less than 33.3%	Stake less than 51%	Computation power less than 25%
Expenditure of energy	Poor	Moderate	High
Instance	Hyperledger Fabric [29]	Peercoin [21]	Bitcoin [23]

2.1.6. Smart Contracts

Ethereum is the blockchain infrastructure. Its most interesting aspect is that this blockchain infrastructure also supports smart contracts [24]. It has a self-executing contract, with the provisions usually specified in predefined source code. Cryptographic contracts do not require a third party to work. This function in the intelligent contract can be activated in the blockchain and its use is inundated in the health domain [24].

2.2. Blockchain Potential in Healthcare

There is a problem in the healthcare sector, where staff-intensive domains and data can be accessed wherever the data generated from; this work is edited and criticized for trusted operations in all sectors. We can divide the operations of the healthcare sector into several parts, including health problem solving, knowledge-based care perception, clinical decision making, triage, and evaluation. In Figure 3, a way to engage the healthcare team to achieve better results is shown. Depending on the type of care, the most up-to-date experience, technologies, and expertise should be provided to the patients. When we collaborate with educational organizations, we need to provide patients with access to the healthcare department and training facilities in order that the students can build the necessary skills. In turn, educational organizations can develop skilled workers. When an organization and firm conduct research together, the health organization assists with informants, samples, test takers, and professionals. By participating in clinical trials, healthcare agencies assist in conducting, planning, developing, and reporting on trials. Instead, research institutes assist the healthcare sector with methodologies and instruments. Health organizations are involved in the education and biomedical research of health workers, which is illustrated in Figure 3. For this, the exchange of consent, patient information and evidence, as well as payment processes is required, which is the job of exchanging data. There is a rule that health organizations must protect the information that patients share.

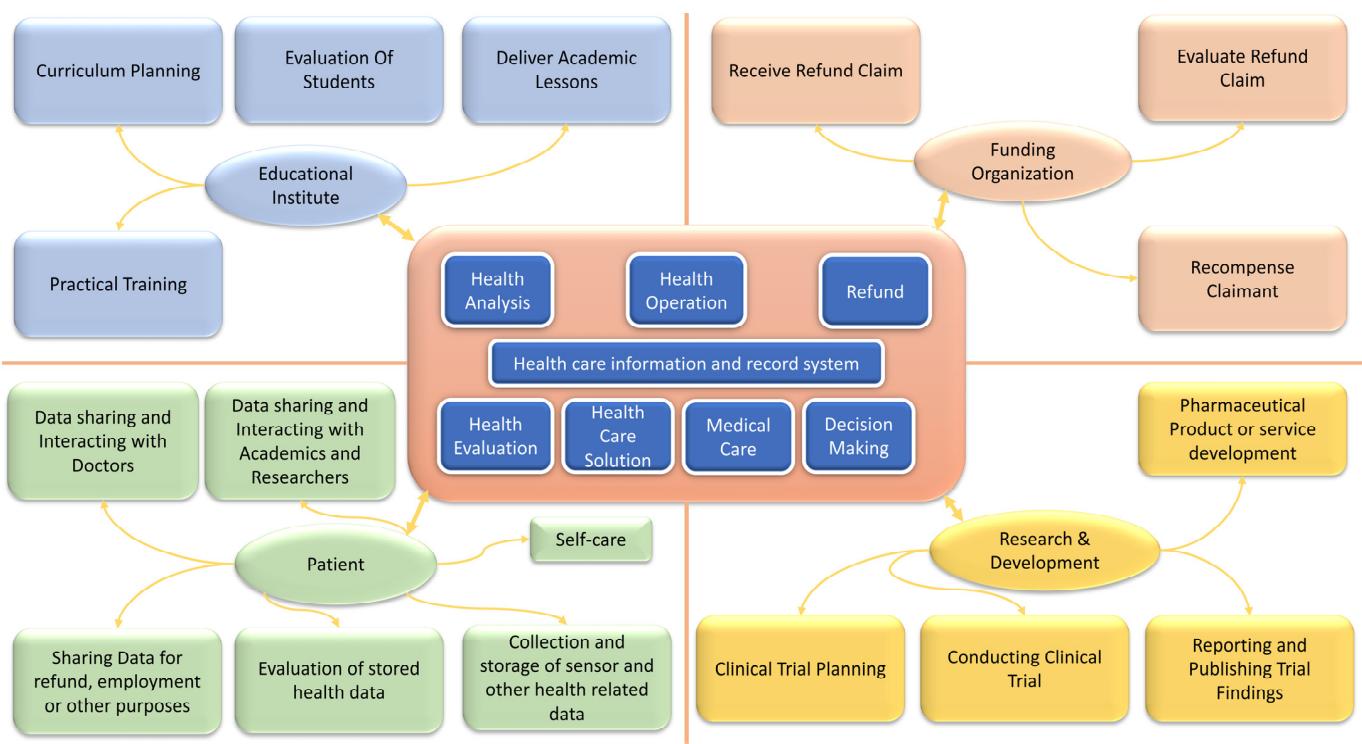


Figure 3. Map of the health sector.

Access control and data integrity are very important when keeping patient information confidential and exchanging data with others. Controlling access to them builds trust between data owners and companies. The server is fully responsible for defining and implementing policies on access control [30]. Interactivity is the ability to connect different information systems and devices, as well as access data within organizational boundaries between stakeholders, in order to improve individual and societal health. Data provenance depends on the data source. In the health area, provenance can provide the ability to monitor EHR and gain trust in EHR. According to Courtney and Ware [31], data integrity is that which works with the expected data quality. The extent to which the desired data quality requirement is met determines data integrity.

Currently, healthcare organizations are showing data demand from research institutes [32]. Unauthorized sharing and data theft destroy public trust in healthcare companies. Malpractices destroy people's trust in the healthcare ecosystem. Therefore, it is necessary to develop an alternative method. Decentralization in blockchain technology can lead to data sharing, data integrity, and access control distribution among the mentioned stakeholders and does not require the participation of any third party so that people can maintain confidence in it.

2.3. Types of Blockchain in Healthcare System: Public, Private and Consortium

Blockchain describes a way to connect a network of nodes together, and it is used to validate any network. If the participants of the node engaged in the blockchain are already familiar with the network, they are called authorized blockchains, e.g., Ripple [33] and Hyperledger Fabric [34]. Like Bitcoin [35] and Ethereum [36], blockchains can also be public. Anyone outside the public blockchain can access the network and become a member as well. Blockchain offers the ability to create and share digital ledgers and to transfer data within a P2P network. Figure 4 shows the image of the blockchain architecture. Users can manage and verify transactions. No central authority is required here. The decentralized approach notably decreases the cost of arbitration, modification, system configuration, and maintenance in communications since they are centralized. Despite having high efficiency, it often suffers from scalability problems [37].

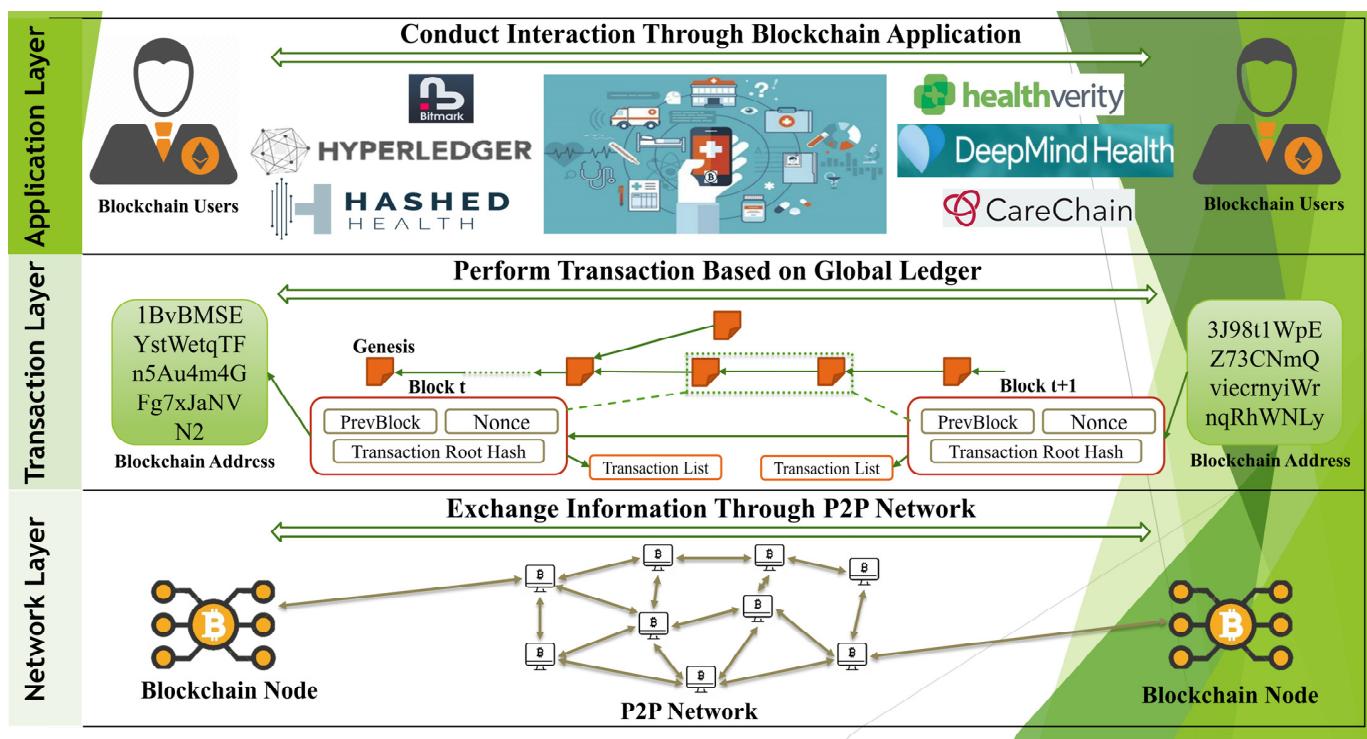


Figure 4. Blockchain Architecture.

2.3.1. Public Blockchain

A public blockchain is a blockchain that permits anyone to access the network without permission and to become a member. Any member can participate in the permitting process through a smart contract with proof of work. A blockchain is usually created with the goal of safely eliminating centralized authority. P2P blocks are placed to prove whether there is decentralization. Transactions employ the Merkle hash cryptography tree as a block before accessing the database for prior transactions. Blockchain transactions synchronize with all nodes. Everyone can enroll as a node and provide them with blockchain files. The system is protected by the repetition of a public blockchain consistent with all nodes. These blockchains have been able to solve the ineffective processes of legitimate transactions. To legitimize a transaction, a lot of electrical power is required, which increases when the nodes are connected to the network [38].

2.3.2. Private Blockchain

Private blockchains are restricted blockchains, the data of which are under strict scrutiny. Members of the P2P network also need permission to participate in transaction verification and validation. However, companies may participate in the validation and verification of transactions without permission. Permissioned blockchains have a high level of expertise for transaction verification and validation. Public blockchains have decentralized systems for secure databases, whereas private blockchains do not have decentralized systems; this is a constraint of private blockchains [39].

2.3.3. Consortium Blockchain

Consortium blockchains are partially decentralized and made up of a combination of public and private blockchains. Data transactions can be performed in both private and public blockchains, and nodes can be pre-selected. A consortium blockchain is different from a private blockchain. Blockchain consortiums consist of extremely confident entity models in private blockchains and untrustworthy public blockchain entity models. Private blockchains are known as conventional centralized systems. Strong encryption methods are

necessary for the verification and confirmation of transactions. The blockchain consortium still needs to be flawless for reliability, legitimacy, and precision [40,41].

3. Review Methodology

The following section will explain the literature selection process of this study. Figure 5 illustrates the screening process of the articles.

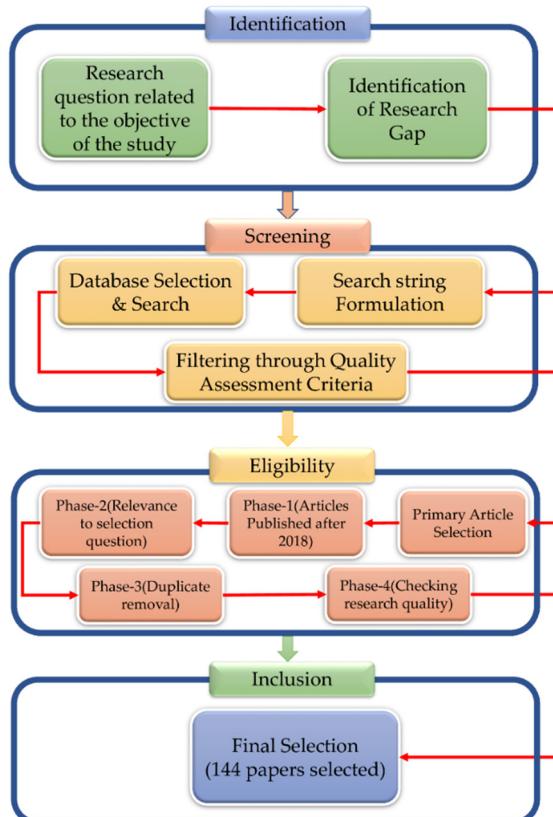


Figure 5. Article selection process.

3.1. Research Questions

At an early stage of the review process, several research questions were formulated in relation to the objective of this study. The aim of this research work is to present a detailed review of the current research scenario of blockchain application in the healthcare industry and to identify the future prospective of this field. To that end, the research questions were used to select relevant research works from prestigious publications.

1. What is the latest study profile of applications used on the blockchain in the healthcare sector?
2. In which sectors of healthcare is the blockchain being used?
3. What are the constraints in this study area?
4. What aspects of healthcare could benefit from the use of the blockchain in the future?

3.2. Search Strategy and Databases

To construct a meaningful and data-driven review paper, the right search strategy is needed, and the search keywords need to be defined to retrieve the correct information.

Before constructing search strings and paper selection criteria, extensive analysis of existing gaps in the healthcare system that could be solved with the help of blockchain is carried out. Multiple sectors were identified as potential fields where the application of blockchain would be most beneficial. The main focus of blockchain is secure data transfer and keeping records of all transactions, which could be most useful in the medical sector

where patient information is required to be kept safe and proof of all monetary transactions is of utmost importance. Other than that, blockchain technology could help establish a safe remote patient monitoring system for telemedicine and offer faster data transfer. Blockchain secures the collection and storage of data from wearable devices. As blockchain allows real-time monitoring of data for multiple users simultaneously, it can offer better decision-making by allowing multiple doctors to access the same data at the same time. Decentralized nature of blockchain could prevent patient data tampering. These are just a few gaps that could be filled through the application of blockchain.

In order to create optimal search strings, in [40–43], the authors have suggested a few steps to break down research queries, such as separate aspects, including research groups, abbreviations, where their synonyms, namely acronyms and alternate spellings, can all be combined through Boolean operators [43].

The three steps that lead to the final search string are discussed below:

1. Identification of abstract and related words in the article that were identified during the first search.
2. The use of Boolean characters such as OR and operators in the building of search strings.
3. Identification of related words, abbreviations, and synonyms.

Following the steps, we come across the following search string: (“blockchain”) and (“healthcare”) (“health”) or (“health record”) or (“ehr”) or (“phr”) or (“medical record”) or (“EMR”).

Finally, using the formulated search string, relevant research manuscripts were explored. For this purpose, only the leading research paper databases were used, which are IEEE XPLOR, ScienceDirect (Elsevier), Springer, ACM Digital Library, Sage Publication, MDPI, Taylor & Francis. From these databases, only 712 research articles were chosen primarily.

3.3. Quality Assessment

It is very important to evaluate the quality of the selected articles and the goal is to ensure that a useful and informative review is produced [43]. The research goals, background, literature review, relevant study, methodology, findings, and prospective research objectives and directions of the papers have been analyzed before choosing the research materials. In order to apply all these conditions, the quality of the chosen articles has been compared with some questions to determine whether they meet the quality criteria:

- What is the study’s aim, and what does the article say about it?
- Is there any mention of literary reviews, histories, or contexts in the article?
- Is the article relevant to current work?
- Is there a research method presented in the article?
- Is there any analysis in the article?
- Is there a conclusion in the article?

3.4. Article Selection

At the beginning of the article selection process, 712 articles were collected from various online library based on initial selection criteria. The selection phase could be separated into 4 phases.

Phase 1: The primary focus was to collect latest research materials, specifically research conducted after 2018. It should be mentioned that some of the papers are dated before 2018 but were selected based on their research merits.

Phase 2: Then, the initially selected papers were checked to determine whether they match the selection questions, and 321 papers were eliminated due to irrelevancy to this research.

Phase 3: Duplicates have been omitted in this step. After removing duplicates from 391 studies, 294 studies remained.

Phase 4: At this stage, the papers were reviewed thoroughly and were compiled to determine whether the research issues were properly connected. At this stage, only relevant and good quality research was chosen. Further, 150 papers have been omitted in this step.

Finally, after a rigorous filtering and checking process, 144 papers were selected for the final study. This procedure was performed utilizing the CASP Systematic Review Checklist [44].

4. Literature Review of Selected Articles

4.1. Bibliographic Overview

The papers selected as review materials in this research are [45–188]. Table 3 represents a short bibliographic overview of the selected papers as well as other related research materials. It can be noticed that most of the papers are written after 2018 which was one of the main selection criteria. This table provides a summary of the research materials used in this study and thus offers insight into the goal of the study at a glance.

Table 3. Bibliographic overview of selected papers for review.

Research Theme	Objective	Challenges	Year	Type	Ref
Medical Data Management and Sharing System	Creation of a blockchain-based decentralized data management system	Data security, accessibility, data transfer and privacy	2018–2021	Journal, Conference	[53–56,64–68,75,76,80,87,92,94,98,102,141,142,144,157,169–172,179,181]
Telemedicine and remote patient monitoring (RPM)	Blockchain-based secure telemedicine and RPM system	Patient monitoring, data collection, data safety and privacy	2017–2021	Journal, Conference	[49,57,59–61,69,70,72,73,77,108,109,122,123,125,128,149–152,154–156,176,177,185,187]
Electronic Health Record (EHR) System	Using blockchain to develop secure and accessible EHR system	Data security, decentralization, data accessibility and integrity	2018–2021	Journal, Conference	[71,81–83,89,126,160,162,165–168,178,182,184]
Data storage and Security	Developing secure data transmission and storage systems	Data security, data authorization, data integrity, safe transfer	2018–2021	Journal, Conference	[47,51,58,62,74,80,86,97,100,104,106,117,145,147,159,163,173,175,183,186]
Edge and Cloud computing, data analysis	Integrating blockchain with data processing systems such as cloud and edge computing for better decision making	Data security, management, reliability, data manipulation, late communication, difficult resource allocation	2018–2021	Journal, Conference	[46,48,50,52,56,108,137]
Literature Review and Case study	Review of the recent development in blockchain-based healthcare systems	Data collection, analysis, arranging and representation	2018–2021	Journal	[45,63,66,78,79,84,85,88,90,91,93,95,96,99,101,103,105,107,110–116,118–121,127,129–136,138–140,143,146,148,153,158,161,164,174,180,188]

4.2. Bibliometric Distribution

Almost one third of the selected papers were published in 2020 and 2021. Figure 6 depicts the fast growth in blockchain research in the healthcare sector, with zero papers published in 2015 and a peak at 62 papers in 2021. The majority of articles were presented at or published in conferences or journals associated with the Institute of Electrical and Electronics Engineers (IEEE).

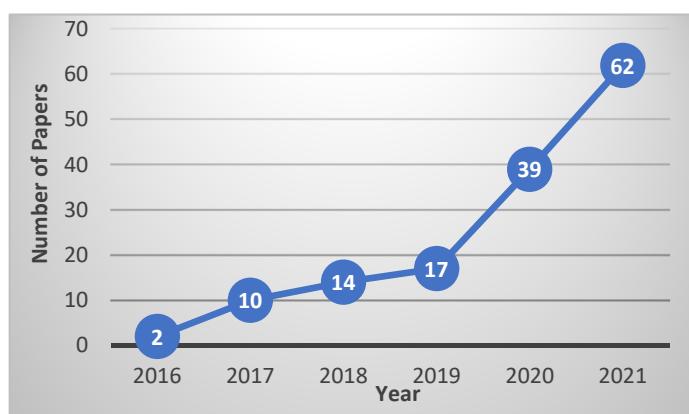


Figure 6. Number of papers published by year of publication.

5. Research Themes of Blockchain-Based Healthcare Systems

This section sheds lights on the former researches and analyzes their limitations, research themes and future research directions.

5.1. Research Themes

The four thematic fields that represent the focal issues that are addressed in this literature are conceptual evolution, performance improvement, technological development, and data management. From the previous results, we observe a continuing scholarly endeavor applied to improve intellectual and technological knowledge to maximize the productivity of the systems for healthcare and data management by means of blockchain.

5.1.1. Evolution of Concept

Analysis of present research materials reveals that research is being conducted on blockchain in healthcare for the development of concepts that help scholars achieve multi-domain efficiency [46]. Application feasibility is divided into three categories, as illustrated in Figure 7. These categories are further discussed in the following section.

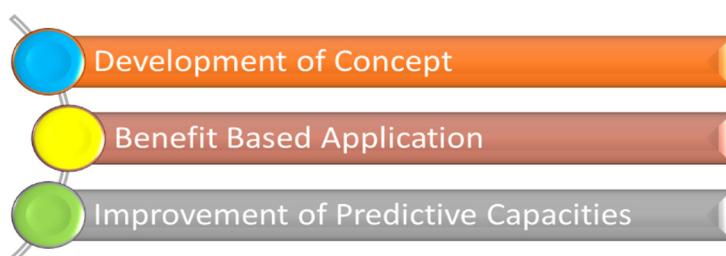


Figure 7. Evaluation of concept in blockchain-based healthcare system.

Development of concept: As blockchain provides safe communication system between multiple users without the risk of data tempering, conceptualization of an idea is much secure. While working on a novel idea or project, it is of absolute importance that all the information regarding that project be kept private and secure. Hostile data theft or tempering has been known to put entire projects in jeopardy. With the introduction of blockchain, it is now possible to create a safer environment for research and development. By analyzing the collected data, it can be seen that more attention has been paid to the development of algorithms and evidence that can help solve the data security problems faced during concept development. Additionally, blockchain can identify the real-world potential of a concept. For instance, a proof-of-work (PoW)-based system refers to a system that discourages pointless or malevolent usage of computational capabilities such as sending phishing emails or conducting denial of service attacks by requiring a not-insignificant but feasible amount of effort [47], and a consensus technique called proof of identity

(PoID), which is designed for permissionless blockchains and provides each individually identified person with an equal amount of voting power and related rewards [48], and evidence of the primitiveness of information [49,50]. The main focus of the studies is the refinement of frameworks that make blockchain efficient by inclusion and allow system architecture to build and test novelties. For more efficient frameworks, previously used ones were calculation homomorphism [51], game approach for Stackelberg [52], feature-based cryptosystems [53], and intractable sibling features [54]. For example, blockchain-based data schemes have been proposed to ensure the security and confidentiality of data transactions [55]. The human body develops novel protocols as a means of transmission for their efforts to create a blockchain-based, vast social network [56]. Fog computing has been used to create an accurate model for acknowledging human mobility to promote remote e-health surveillance [57]. Emphasis has been placed on source inclusion to avoid exclusive failure [58]. This section discusses the potential for efficient improvement of blockchain-based architectures and methodologies.

Benefit-based application: Further studies include blockchain in health care, which has the distinctive benefit of classifying and evaluating new blockchain applications. These studies have focused on enhancing the technological benefits of blockchain applications, such as via synchronization of IoT devices [58], recognition of efficient operations [57], and enhanced image processing [47]. However, most blockchain research has focused on expanding the benefits available in health care, such as joint treatment decision-making [48]. For example, blockchain adoption has been shown to be beneficial in monitoring distant patients [59,60], clinical trial management [61], DNA data transmission [62], as well as healthcare prevention, biomarker development, and medication discovery [63].

Improvement of predictive capacities: We can observe that experiments have also concentrated on the health ecosystem amenities of blockchain for promoting justice and efficient decentralization [64–66]. Researchers in [52] address the possibility to create institutions to maximize revenue and encourage autonomous fair trade. Additionally, in [67], authors discuss the necessity for mining incentives to be compensated. Researchers explored the promotion of clarity in data exchanges in the blockchain process, e.g., including the role of fair clients [68,69]. From past studies, we can notice that blockchain is rapidly becoming a reliable medium to address several technical issues in healthcare systems.

5.1.2. Advances in Technology

Blockchain technology has significantly progressed and purified the way of development of applications in the healthcare sector. In this section, we have discussed three key issues from previous studies.

Development of smart ecosystems for healthcare: Some academics have concentrated on connecting the blockchain platform approach to the healthcare ecosystem [70]. These organizations have the potential to create smart healthcare systems [71]. Adopting blockchain helps create an optimum ecosystem for telehealth [72]. Several approaches to building blockchain-based telehealth [73] and telecommunication systems [74] that could improve health services in the future have been proposed in the past.

Technological improvements in blockchain architecture: Most of the studies have focused on ways to improve the efficiency of systems and structures by improving technology. For example, the identification of unknown key exploiters [75], the usage of a limited data block shape [48], and improved transaction latency [76]. The problems that have arisen in the past with the effective installation of blockchain structures have also been taken seriously. Some problems have been identified through research. Among them are memory load [56], memory utilization [51], overheating [56], and trustworthy node detection [77]. These problems are solved through guided analysis compared to networks and methods [48,68,69]. In the future, more attention should be directed at the advancement in this field and comparative analytics to determine the most crucial networks and methods.

Building full power of prophecy: The use of blockchain technology is in the fourth stage of its evolution, with its growing integration into AI and healthcare [78]. Current

investigations into blockchain-based structures have started to incorporate parallels and peripheral automation such as cloud technology [46], wireless body areas [59], the Internet of Things [60], photoelectric cells [72], big data [79], networks, and edge computing [66]. Using such technology, researchers have been able to create blockchain structures with a predictive ability to enhance the quality of medical information technology and diagnostics [62,80]. These types of frameworks for particular utilitarian features based on healthcare have been explored before, for instance, in the production of verified data [51], the automatic settlement of claims [53], and the avoidance of prescription fraud [72]. The rest of the studies focus on developing blockchain automation to help healthcare providers with a variety of tasks, for example, considering data collection at the population level [81] and the definition of user identity [65].

5.1.3. Increase Efficiency

Many studies have been conducted to investigate the ways in which blockchain projections can help improve the effectiveness of healthcare systems. This analysis demonstrates that the researchers have concentrated mainly on two areas: methods and systems for improving competence.

Procedure: Nearly all prior research focused on increasing the efficiency of the technical parts of the procedures necessary for the implementation of blockchain health systems. Studies have concentrated, for instance, on integration times and overheads [58], overloads of communication [77], decreasing energy costs [77], and calculations of loads [56], revealing solutions to reduce all of these problems. All prior research has focused on enhancing the forthcoming future [53] and reporting systems on adverse occurrences [61]. However, in some focused studies, processes are better understood and new architectures are rigorously tested to provide more reliable processing than standard architectures [47,57,77]. Researchers are working to address challenges related to time management, data management, and related costs in order to improve the blockchain architecture. Several studies, for example, have constructed frameworks that, once established, can reduce performance and storage costs and save and store infinite amounts of information [48–50,82]. The frameworks that have been developed focus on ways to increase effective capacity in three areas: runtime, shipping times, and latency [56,82,83].

Method: As we have reviewed, we have observed that a number of approaches have been used to increase the effectiveness of blockchain-based healthcare organizations. Studies have focused, for example, on the enhancing interoperability of systems [79,84], inter-institutional access facilities [52,85], and administration of data [63,65,81]. Scholars have also focused on improving the system's scalability and performance [55,62,82]. Researchers concentrate on establishing integrated architectures based on services [73] and flexibility of implemented blockchain technology [68,69,84].

5.1.4. Management of Data

After reviewing the papers, it can be observed that the scholars have assigned the most importance to the administration of medical information and records. Earlier studies have recommended that blockchain be used as an effective solution to handle medical [54,84–87] and electronic private information [67,83,86,88]. Effective data ecosystems can be created by using blockchain for management. For example, PHRs [63] can combine large amounts of medical data and data from different sources [46,71,84,87]. We outlined three central aspects of conventional research in our theme based on SLR. Figure 8 illustrates the most popular research areas of these three central aspects. The next section elaborates further on this topic.

Information privacy: Work in the earlier literature to maintain confidentiality of data after accessing medical records on the administration of blockchain technologies in the field of health has been conducted. A lot of time has been spent investigating the administration of user authentication [66,70,81]. The confidentiality of sensorial medical information must be maintained through enhanced responsiveness, constancy, and authentication, which

complicates the challenge in the healthcare industry [86]. Previous studies have established blockchain-based architectures to enable qualified user-oriented and controllable approaches to user PHRs and various medical information [60,64,70,83,88].

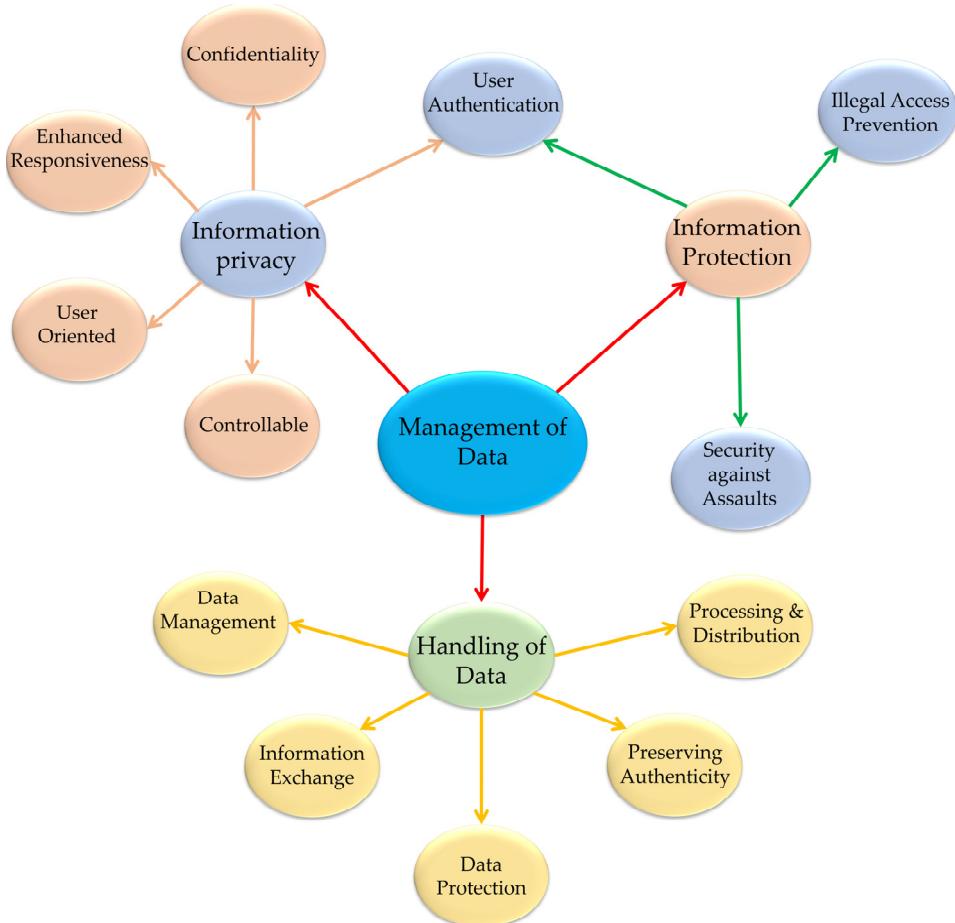


Figure 8. Popular research areas of data management in healthcare system.

Protection of information: Prevention of illegal access and security of data are crucial topics in the research of healthcare challenges in blockchain information systems. However, nearly all of the analyzed research focused on preventing illegal access [89] and safeguarding them from disguise [77]. It is suggested that several methods be used to attain this goal, such as the usage of multiple identities [52], biometric authentication [79], effective authenticity [82] and user identification [86]. However, little emphasis was placed on avoiding external assaults such as sensor data assaults [81], transactional assaults, and conspiracy assaults [88].

Handling of data: Previous research studies have legally ensured the management of healthcare information, while other work has been conducted to process, distribute, and manage ethical compliance. We examined and discovered that certain research recognized the requirement for adherence to the rules or standards and objectives [52,71,80,90]. However, much emphasis has been placed on preserving the authenticity of the information [54,73,87]. For example, legitimate information collection [81], the prevention of information theft [51,56], the prevention of dual storage costs [76], and the information permanently retained [49] are subjects discussed in earlier research. As blockchain continued to increase inter-institutional adoption, researchers turned their attention to data protection [90] from medical equipment [75] and health assurance [51]. Some research has also focused on inter-institutional information exchange [90] and facilitating the transfer of data as capabilities grow [87].

In addition, other studies focused on improving information processing [51]. The analyzed papers have proposed some ideas for this enhancement, such as efficient inclusion of multiple information [85] and the incorporation of intelligent contracts [67]. Earlier research focused on such concerns as (a) technological characteristic enhancement, (b) the administration of treatment data, and (c) the identifying of separate healthcare competences where blockchain might contribute substantially. The subject of this study is in a revolutionary state, with the use of blockchain in healthcare sector emerging as a beacon of hope day by day.

6. Major Application Areas of Blockchain in Healthcare Systems

The following section will discuss the key fields of healthcare system where blockchain is beneficial, such as health information management which includes healthcare record sharing, healthcare image sharing and healthcare log management. Figure 9 illustrates the application areas of blockchain in healthcare systems.

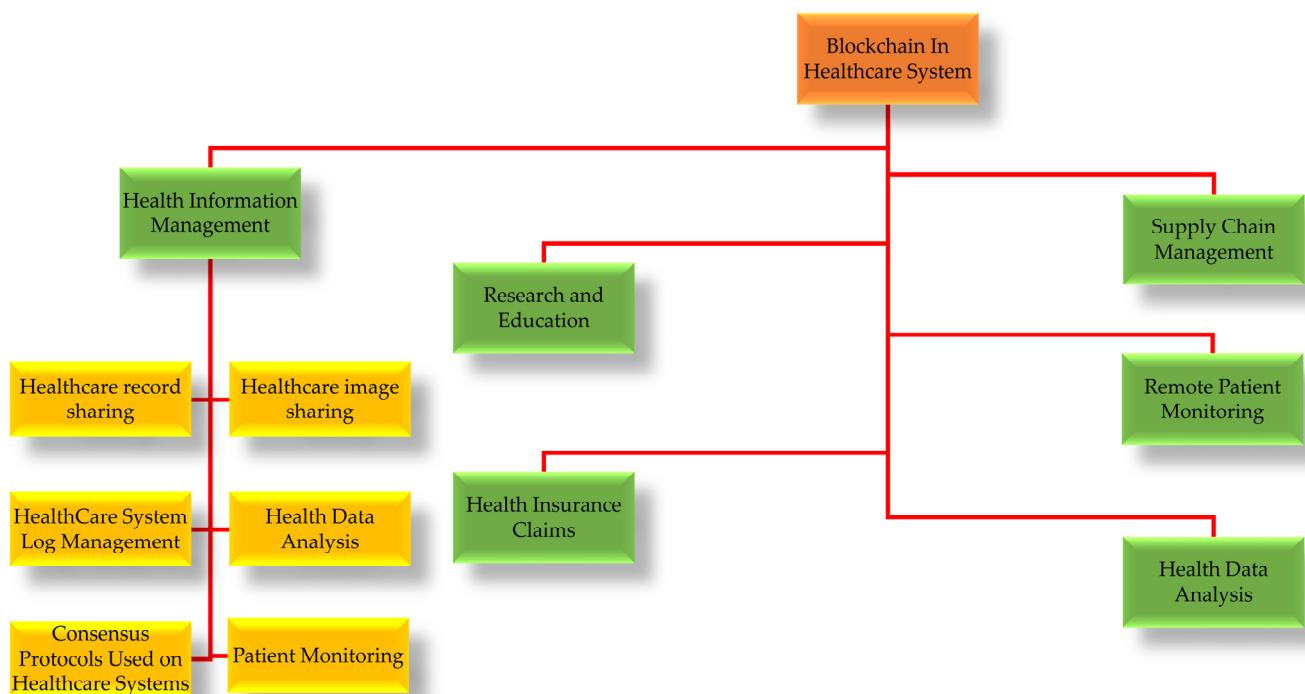


Figure 9. Application areas of Blockchain in Healthcare systems.

6.1. Health Information Management

This segment will investigate the ways in which blockchain can be utilized in the realm of medicine, including healthcare information management and the handling of sensitive patient data.

Blockchain has social significance in the field of healthcare because its progressive use can improve the quality of life. Following the same logic, computation can reduce some of the problems in this area. Informatics, for example, contributes to health record automation by ensuring more reliable data exchange, applications in other fields, and log management [92–94].

Managing healthcare data through medical records or in any other way has an immediate impact on the way in which the patient will be cared for. Collection of information can reduce the time required for treatment, allowing physicians to easily identify the patient's symptoms and make quick decisions [95].

In this segment, the management of information related to healthcare will be considered. This will look at the ways in which blockchain technology might aid in the

management and exchange of medical data, e.g., patient monitoring data originating from IoT devices.

6.1.1. Healthcare Record Sharing

One of the first blockchain-based healthcare systems involves the sharing of health information. This is difficult since it deals with the patient's personal information and is classified as sensitive data. Such a type of application of blockchain has been discussed in [92,94,96].

For exchanging electronic healthcare information, blockchain-based architectures are supposed to have many features. The workings of the classic system are discussed in [92]. This literature has been created by retrieving information from current papers [92,97–100].

MedRec has a shared architecture. It saves electronic healthcare data and adopts blockchain-based frameworks to save electronic healthcare data. MedRec aims to deal with problems such as interoperability, data access response time, and improved data quality for healthcare experiments [92].

The materials used in creating the architecture of MedRec are worth inspecting as they create a private P2P network (permitted by BlockChain). It also allows one to track and manage network state transitions.

Providing patients with a consulting agency along with the healthcare history of the given agency is one of the many features of the MedRec architecture. This allows patients to be informed about their health decisions.

They are also capable of allowing health data standardization as they are supple, and they also suggest various public data standards of various shapes.

A similar kind of architecture applies an interesting strategy for implementing the health information management process by providing better safety and a shared language to exchange information for research objectives [92]. It is also capable of conducting tests and evaluating users in different groups [92].

MedRec presents a feasible approach for sharing healthcare history with clinicians, patients, and hospitals, and it can be merged into healthcare. As a result, the anomalies in various hospital systems may be reduced by using registered data.

In [96], the topic of cloud computing is introduced, which could help create a new architectural design for sharing healthcare information via blockchain by providing a safer and more robust healthcare process used in medical practice. The author suggests a cloud-based architecture that embraces the blockchain data structure to connect node communications. Blockchain architecture utilizes intelligent contract concepts and transparent, unchangeable bookkeeping to supervise healthcare data sharing. In [96], the architecture of cloud junctions and blockchain concurrently is also pointed out to enhance management "access control" for the system. The author, for example, uses data collected from the Department of Radiation Oncology for testing. It specifies access control rules with two primary functions (patient and doctor). It also specifies transaction logic using intelligent contracts. These kinds of architectures have one objective for the future: to share radiology pictures and, if possible, test them on actual patients [96]. Recent papers linked to blockchain in healthcare discuss a network or system prototype. They also wish to develop a working system for testing with actual users.

Along with examining all of the components of the blockchain architecture for exchanging healthcare information with the use of cloud computing, it is also important to discuss other aspects such as data inspection. In [94], the authors discuss developing a solution based on blockchain for sharing records across health cloud service providers. The purpose of this solution is to ensure a better system for auditing and controlling record access, along with generating a query layer to establish a connection to the blockchain network while utilizing an activation set-off to execute the task through smart contracts.

There are four layers in the MedShare-based solution system. They are:

- (1) User layer: a graphical interface that will allow the user to access data.
- (2) Data query layer: a system architecture that manages and responds to query requests.

- (3) Database infrastructure: a layer constructed by a system database that only a few specialized organizations have access to.
- (4) Provenance and Data Structuring Layer: The adopted blockchain network structure, node authentication, smart contracts, and consensus protocol are all part of this layering process within the systems.

Medshare and similar kinds of solutions have one primary objective, and that is to facilitate the adoption of some characteristics of the healthcare system. Auditing, data provenance, and better security for the system might be included in these characteristics. Additionally, the solution enables the user privileges of management and cancellation of access and the possible establishment of a healthcare information repository that may be helpful for big data analysis. As a result, the system may be able to handle the increasing demand for data by using cloud processing.

It is essential to highlight the technologies used in creating these architectures. Typically, Python is the language used in implementations, and the Flask library is also used to build web pages in Python. This technology has been used because a wide variety of devices may be implemented in this environment. The database is another noteworthy technology here; a common example is SQLite2.

6.1.2. Healthcare Image Sharing

All kinds of data, along with pictures, can be used to describe healthcare information. Presently, some issues associated with exchanging healthcare records may appear in pictures [101]. An architecture working with similar kinds of information [102] has some definitions behind this concept. They want to present an architecture for image sharing based on this effort fundamentally. Patients can exchange their medical pictures in a secure and measured manner. The Radiological Society of North America (RSNA) designed a centralized network system that was established in a decentralized manner as the foundation for this architecture. The Image Share Network (ISN) was established to address the concerns identified by the RSNA networks, such as registering photos in repositories for research that can be safely examined. Photos can be viewed if the owner provides permission [102].

The architecture of [102] was constructed as a set of nodes forming a chord-type P2P network where every node represents an entity in the healthcare system specified by it. The network consists of four parts: (1) health, which provides read-only access to the images specified by the patient owner; (2) the image center, which acts as an intermediary node for accessing images; (3) personal healthcare records, which represent the patient's healthcare records and all other types of records related to the patient in a hospital or other setting; and (4) the patient, who has full access to their images and can choose who to share them with. The notion applied in the verification procedure is the primary objective of the architecture for picture sharing. The consensus algorithm, proof-of-stake, carries out the process as it benefits the participants with a marginal load. Private and public cryptographic key concepts are used for secure transfers. Simply put, the architecture presented can aid health systems by creating a secure and dependable environment using blockchain technology.

However, it has shortcomings, most notably in terms of the privacy of pictures, which is sensitive information. The authors wish that future researchers would be more cautious in this area [102]. To summarize, the solution described in [102] may be beneficial since it eliminates the use of a middleman and allows patients to control the distribution of their information and keys. The architecture of [102] could be compared to the work of [103], which provides a structure for the exchange of patient-oriented photos (i.e., owners manage the sharing of their photos).

In any case, the network is dependent on a central unit that transmits data to the network's various nodes. Attacks or server failures on the central server may jeopardize the network's performance.

6.1.3. HealthCare System Log Management

The concept of log management is essential for a computational system because logs allow historical data to be created to support intrusion detection, error analysis, and other services [104]. This type of administration is required to provide more user control when patient data is accessed in the healthcare system [93].

Nevertheless, while the logs created by the traditional methods that we utilize nowadays are facing a threat of being modified, a technological system is needed to resolve the problem, and blockchain can provide this. The blockchain's immutability features can assure that stored data (e.g., logs) are not altered in the ledger. These ideas in the healthcare environment were explored by the authors of [105].

Blockchain-based method can be employed to manage logs generated by information accessibility. The technique that has been implemented also aims at auditing control, standardizing data, and smooth and straightforward sharing by using a permitted blockchain framework.

The logging process for security audits is a little bit complicated since the amalgamation of collected data is not always useful or may lack significant information pieces [93,105]. The authors of [105] explored a log control solution called AuditChain, which is primarily a program that meets interoperability concerns while allowing the sharing of electronic health information. The following components are deployed in this method: the Hyperledger fabric and the IBM framework, which assist in the blockchain-based construction of applications. The application is accessible through a user interface, but this requires the usage of a web service that is built on Node.js. This is why an application was developed to assist with audit log management and also provide the authors (i.e., doctors, nurses, and patients) with multiple access controls. It is worth noting that AuditChain concentrates on the administration of records of personal health, and every patient may access and manage their own data [105]. AuditChain logs are stored in the ledger to enable replication and distribution to network nodes. However, the concept of smart contracts, along with the concept of the ledger, are required to describe the transaction logic. In the Hyperledger Fabric framework, a similar kind of contract is known as Chaincode [105]. When dealing with such a blockchain-based framework, the AuditChain encrypts data related to the transaction through asymmetric encryption using a set of keys. Users who have authorized access to the blockchain network receive a virtual token in the JavaScript Object Notation (JSON) format, even if the blockchain network encounters a security breach. It will be used as the user's transaction's digital signature.

Nevertheless, there are a few downsides to using AuditChain, such as the inability to locate logs relevant to a particular user. Furthermore, it is expected to write the query script before performing the operation, which makes it a less notable method. Another important point is that the trials performed on the scheme were not conducted in the real world. Therefore, the applied matrix may not be the most suitable for implementation in a real-world context [105].

6.1.4. Industry-Specific Approaches

The preceding sections evaluated some policies for electronic health record management. Due to the growing popularity of the blockchain concept, it is essential to examine certain applications that are particularly aimed at companies. Company strategies typically include strategies aimed at resolving specific market-related issues and increasing profitability.

Researchers in [106,107] are developing two blockchain-based techniques in the healthcare ecosystem industry. Additionally, throughout our study, we came across a survey on strategies targeted at companies using the Sandgaard and Wishstar [107] approach, which is geared toward the healthcare sector. The first method to discuss is the work conducted in [107] titled Medicalchain. It was built with the assistance of a Hyperledger Fabric-based permissioned blockchain. Patients may utilize access controls for all of their data and manage healthcare information in a customized manner using this application.

MedicalChain makes information accessible through tokens and supports access control by identifying important individuals such as patients, physicians, and research teams.

Medicalchain can be distinguished from other methods described in the study in many ways. One of them is the presence of a repository for healthcare data. For instance, research groups may use this store to exchange data for monetary assets that can be used across the network. When a patient provides data to the network, they are rewarded with coins that may be spent in the system; the cryptocurrency in this system is called Medtoken. Furthermore, an integrated blockchain network allows data from a patient's wearable devices to be recorded. They can be used to monitor alcohol intake, physical activity, blood pressure, and other factors that could aid physicians in diagnosing patients [106].

In essence, the Medicalchain system has the capacity to be very beneficial, and it provides significant prospects for healthcare systems. It does, however, have significant drawbacks in that the information-sharing procedure is bureaucratic and requires payment to obtain data from the structure. Another constraint relates to Medtoken, since its usage is system-specific. Moreover, every Medtoken costs USD 0.25. It should be noted that the project is currently in beta testing mode and that the modules contain some bugs [106].

Considering industrial applications, attention should be focused on Sandgaard and Wishstar's work [107], which proposes a blockchain-based system for electronic health data management. Thus, it intends to increase transparency and safety while developing healthcare apps. Medchain, as the technology is known, aids in the management of electronic health data in two crucial aspects: security and the interoperability of the systems that use it.

Medchain employs a modular approach in its architectural applications because certain layers have been attached to it. The standard data layer (a chain for protecting health records) is one of the crucial layers of the tool because it stands as the baseline for all others. This layer enables additional software to be linked in to use its functionalities in the future. The standard data layer also supports distributed feature (DApp) applications that aid patients in accessing their healthcare files. These are derived from a user interface application that can communicate with DApp [107].

The primary goal of some papers [108] is to propose a framework such as Clinicoing [109], Medibloc [110], and Medx [111] that would ensure the safety and confidentiality of patient information when blockchain technology is used in medical management.

Medchain has the characteristics of Medicalchain since it operates similarly on the inside of a system that consists of different types of tokens, such as the following:

- (1) MedCoin as an external token that can be used in exchange.
- (2) An internal token that would have the capability to generate a block hash to provide dispersed information located in any place in the system to the owner of the data.

As a service, one more characteristic of Medchain is related to the aims of the structure of the network: support of the integration of any electronic record system with the blockchain and ensuring that its users enjoy superior safety, dependability, and advantages [107].

A practical use of blockchain in healthcare is the GovTech initiative from Estonia, which began in 2011 and has contributed to the governmental process by bringing together emerging technologies to solve problems. Similarly, blockchain technology contributes to the security and sustainability of government healthcare systems. According to the study by Heston [112], the use case of blockchain in healthcare presents certain advantages when implemented in this setting, e.g., for the preservation and management of healthcare data. Blockchain technology provides safety, immutability, and expandability without requiring a third party. Additionally, this technology may enhance audibility through the use of immutable logs, provide privacy for healthcare data, and possibly save on healthcare expenditures. Another problem is Estonia's difficulties in deploying this technology, such as its compatibility with its users (patients, doctors, and healthcare professionals), which encourages it to adopt the process along with blockchain technology. Briefly, the blockchain in Estonia has the potential to significantly enhance medical treatment and the standard of

living for consumers of the healthcare system while simultaneously ensuring the privacy of patient data [112].

6.1.5. Consensus Protocols Used on Healthcare Systems

The consensus rules are a dominant framework for managing the transaction ambiance in blockchain networks. Some specifically defined algorithms help to coordinate and validate the transition protocols. For the most part, they assist in affirming nodes to reach a proposed system, but there could be a chance that the transaction which they pass to the network system may be born a bitter sprout. Therefore, it can help to reject fake transactions on the network [113].

In this instance, IBM could be mentioned as an example. It has a platform called Hyperledger Fabric that sometimes works in the context of blockchain in healthcare systems [114]. In this research-based exploration, it was shown that two well-known approaches are widely adopted in healthcare system protocols. One is proof-of-work, and the other is PBFT (practical Byzantine fault tolerance). Proof-of-work gained its popularity because it first appeared in various sectors. PBFT is popular for its low-latency network and also for the basic stage of the IBM Hyperledger, which is related to the blockchain network. In the industry, two well-known protocols are called proof of accessibility and proof of time and space. The first one is used for the types of algorithms that guarantee access to data. If, by any chance, a node gets canceled out of the system, the system can still operate. The time-and-space-proof protocol checks whether data has been saved and periodically requests the time. These demands examine the purity of storage of healthcare records when nodes participating in such a system receive a wage in Medcoins [107].

In addition, the agreed rules presented are searched in various areas such as IoT and the supply chain or supply chain system. IoT's "light compliance" protocol is required because of devices with small amounts of hardware, for example, PBFT, modified POS, the Stellar Consensus Protocol (SCP), and others [115,116].

Concerning the supply chain, the alternative to the rules and regulations places trust in the applications. However, here, we are just focusing on healthcare system-based applications.

6.1.6. Patient Monitoring

In this section, the aim is to carry out some analysis of rules, tests, and studies that can help a patient to monitor their condition with their sensor. This section also investigates the improvement of data quality and the restrictions on the healthcare system. A special attention is also focused on various energy reduction methods.

As IoT systems and sensors are used in a variety of settings, including clinics, hospitals, and other medical facilities, it is critical to strengthen their security [117].

The sensors may resemble new wristlets or devices that may be inserted into patients or hospitals. Blockchain technology helps to moderate the security system of usable devices because sensitive personal information is created when a patient is under monitoring. At that point, these sensors are generating the personal data of a patient. Some rules and regulations must be followed for the preservation of a patient's personal information, as they have been followed by many countries in their hospital management systems for a long time. For example, we can include rules from various countries, such as the Lei Geral de Proteção a Dados (LGPD) in Brazil [118], the General Data Protection Regulation (GDPR) in Europe [119], and HIPAA in the United States [120]. These rules ensure that proposed systems guarantee the confidentiality and privacy of patient information. Many technologies have arisen to modify and empower conventional systems. For example, this technology is IoT, which consists of networks of sensors and wearable devices. These advances are also being made in medicine, which could benefit from this system in areas such as the use of wireless body area networks (WBANs). The main idea of this principle is to apply implantable or wearable sensor networks to conduct the desired task. The sensor has a central unit where the data are transferred [121].

Figure 10 shows the WBAN network structure simplification for a patient counseling system with a blockchain network [122].

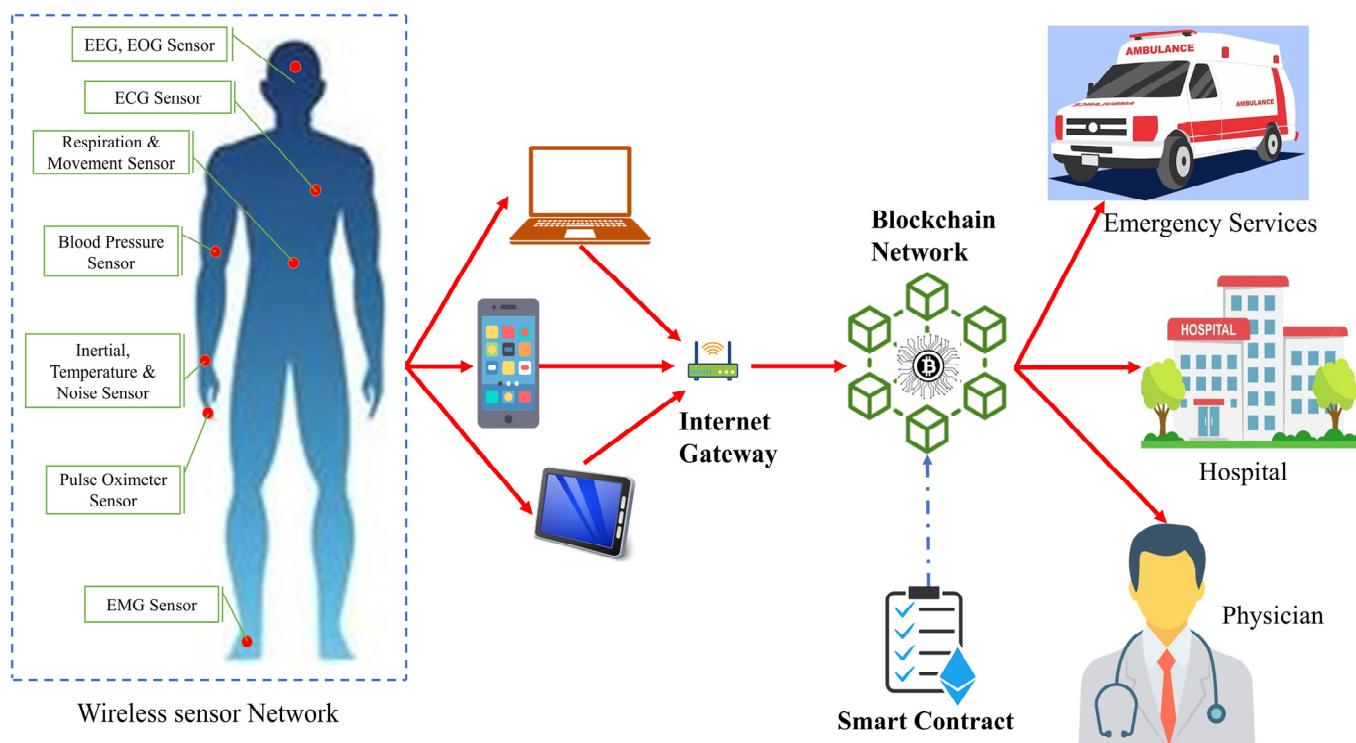


Figure 10. A system of Wireless Body Area Networks (WBANs).

In Figure 10, a patient is continuing elemental exercise, and at that time, if a doctor wants to measure the heart rate using sensors that are already installed on the patient's body, the sensor will send a gateway packet to the device. Then, the package proceeds to the blockchain network and interacts with modern devices to store the data. Stored data are sent to the hospital, where physicians can examine them, and the data remain secure in the blockchain system.

Health monitoring of a patient is an important issue in the healthcare system, as a patient is constantly undergoing professional follow-up treatment. Therefore, the required features of WBANS and their rules, such as wearable device technology and gateways, should enhance the attributes of the healthcare system.

Next, the capability to share the information of a patient on the channel has some limitations regarding reliability, efficiency, and consistency [123]. Hopefully, other new technologies will overcome these situations. One example is blockchain, as it is easy to alternate the report between the nodes, and the concepts of data privacy and immutability are very clear. In this way, blockchain technology can provide the highest level of security for the disposal of information. So, emerging from this feature, blockchain may be a reliable process for monitoring patient healthcare.

In [124], the authors asserted that a blockchain-based network was introduced for sharing healthcare information that would be obtained from sensors. This provides all of the advantages of blockchain technology. However, when the information supplied by the sensor is integrated, such as the heartbeat detected by a cardiac monitor, the patient will be able to handle it [124].

Some authors have proposed sharing the repository information which is blockchain-based. This sharing of proposed information helps in various fields of the healthcare research system. The researcher-generated data may bring some benefits to improving patient healthcare and may also accelerate the treatment system of a diagnosis center for various diseases [124]. An example of the system is provided in [125], where the technology

is used in the blockchain system for patient monitoring purposes. Here, the authors research indirect monitoring for a patient with a personal sensor network. It is also shown that this technology can transfer generated data to the blockchain system at different levels with this suggested structure. The use of this technology has the advantage of reducing communication costs, and when it sends the records, there is no need to seek help from any other third party, even in the transpiration and constancy of the healthcare system.

In [125], an architectural design that contains two layers is proposed: (i) one is flow and storage controls of the data; (ii) the second one is a central healthcare data unit. The proposed methods work with the patient's own sensor network, where generated data are transferred to the healthcare system via a smart device. The generated data are transferred to the server, which acts as an agent for the patient. It also works for data control, mining, and security management on the system.

The authors of [125] discuss the test and measure of architectural design in a variety of contexts, including man-in-the-middle assaults, denial-of-service attacks, and the implications for patient privacy. Prior to these experiments, several industries used various types of selection algorithms.

Many parameters had to be determined before the testing could be carried out, beginning with the mining and mining selection algorithms. This analysis showed that processors are used at 25% and memory needs are at 95 MB, but before that, the network needed three miners. On the other hand, safety test subjects were selected based on the aforementioned assault and were likened to the work of other authors [128,129].

The network's physical characteristics were also examined, such as processing time, overhead, and throughput in kbps (kilobytes per second). In this test, it was determined that processing and overhead costs were lower than in previous tests such as baseline. The result also showed that this system has a 45% transfer rate on the network within 26 nodes, which is lower than that of the previous bassline system [125].

6.1.7. Discussion

Here, we are examining some concepts employed to manage healthcare information using blockchain technology. As a result, it can now use some rules and regulations to control network transaction processes. On the basis of this knowledge, it can govern the process of remotely controlling principles such as electronic health records, greater security, data immutability, and privacy.

Basic protocols involved in the healthcare system's network trust-building process are sensory protocols, such as proof-of-work, proof-of-stack, and PBFT. Furthermore, the performance of blockchain-based applications is used. There are some studies that rely on hyper-laser contexture structures that are used for the PBFT sense quantum protocol.

On the other hand, in this section, some factors are discussed, such as the expectation of distributing healthcare documents and images, guiding healthcare application logs, and leading healthcare reports for industry-wide bargaining. Here, every point carries some benefits and helps the healthcare environment by discussing problems to determine the solution path.

Finally, some of the rules were discussed and analyzed in some of the research that examines the treatment of patients when observations are made with the help of personal sensors. This research also examines the skill and safety of data moving as well as measures the reduction in energy costs.

It should be noted that while blockchain is a relatively new notion in computing, it can be used to improve dependability and monitor patients using sensors with less technology.

Furthermore, as many sensory protocols are evolving, they can be used on resource-limited devices (e.g., IoT), including lightweight compliance protocols such as PBFT and SCP [130].

6.2. Supply Chain Management

Blockchain is used in health supply chain management, in the pharmaceutical sector in particular. Patients can be severely harmed if substandard drugs are supplied. Although this problem is common in the pharmaceutical industry, blockchain technology presents the possibility to solve it [131–135].

Some industries are working on a way to use the blockchain to detect prescription medicine fraud, according to Engelhardt, who conducted a study on this topic. These industries are HealthChainRx, Scalamed, and Nuco [136]. The blockchain network records every deal related to the prescription of medicine for all stakeholders who are connected to it, such as the distributor, patient, manufacturer, physician, and pharmacist. It can detect any change in the prescription. The developers of Hyperledger Fabric created a counterfeit drug project to take steps against drug counterfeiters [137].

However, [138] is the only article in this review that discusses the use of blockchain applications in the drug supply chain. One of the startups using the blockchain is Modum.io AG, which makes pharmaceutical products accessible to everyone when it records the temperature and has the ability to keep its information unchanged using the blockchain. When the products are transported, the temperature can be controlled according to the required level. Mackey and Nayyar have received many examples of prototypes from the gray literature and related research on the use of blockchain in pharmaceutical supply chain management [139]. It refers to the players in the industry who may have used many business types' blockchain-based products to fight counterfeit drug distribution. However, there are still a small number of academic publications available in the trade. Figure 11 shows the supply chain management system in blockchain.

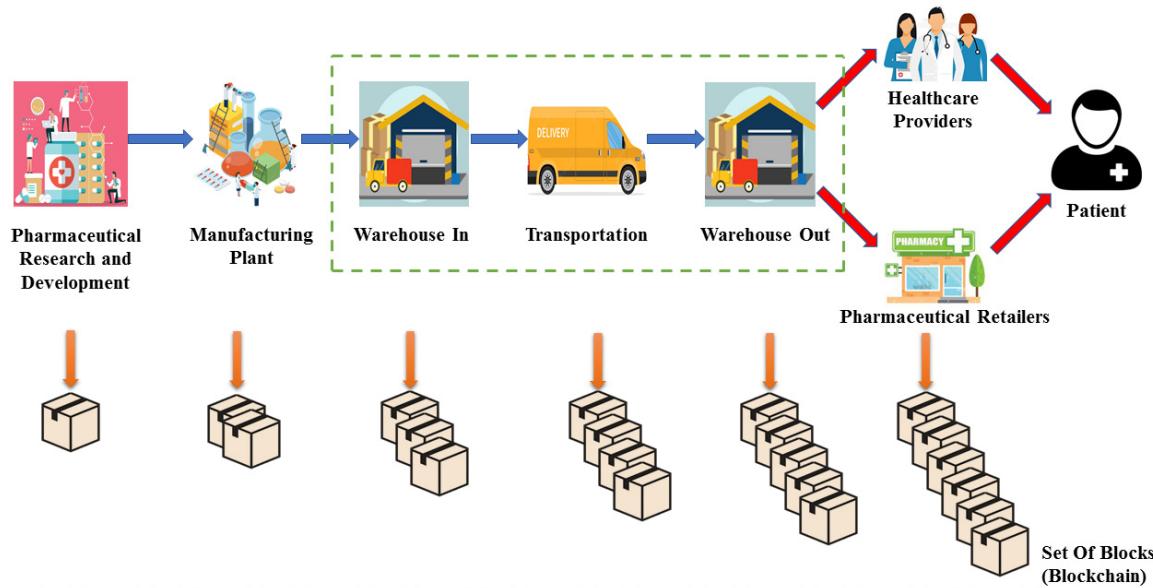


Figure 11. Supply Chain Management in Blockchain.

In this figure, first, during the discovery of new drugs, a block is created where the data from clinical trials are stored. Second, for the test prototype, the patent is sent to the manufacturing plant. In the third stage, the drugs are stored in warehouses at the end of production. In the fourth step, the blockchain collects all the information used in transportation. In the fifth step, the medicines are sent from the warehouse to various healthcare centers or pharmacies. In the sixth step, all the information from the healthcare centers is stored through blockchain to prevent counterfeiting. In the seventh step, all the information about the retailer is saved. Finally, by collecting data from the blockchain supply chain, patients will be able to verify the veracity of the process [188].

6.3. Research and Education

There are two good uses for blockchain, one in education and the other in biomedical research. In the case of blockchain clinical trials, the data help to dispel falsehoods and eliminate undesirable results in research [135,140–142]. The blockchain creates an easy way for patients to allow their data to be used for testing in a clinic or hospital, as the anonymity system here encodes data [133].

The transparent and universal nature of the blockchain makes it easy to conduct research using blockchain-dependent information. For these reasons, the blockchain has the potential to revolutionize biomedical research [136,143].

The blockchain also creates the possibility of revolutionizing the peer-review system for publishing clinical research, dependent on its decentralized, unchanging, and transparent features [143]. Blockchain introduces another powerful application of healthcare profession education (HPE), where a case has been created to design an HPE method using blockchain that provides quality and qualification-based certification services without relying on any third party [144].

In [145], evidence for the adoption of clinical trials utilizing blockchain technologies with traceability is presented.

Authors of [146] show that it is possible to deal more smartly with and also improve data movement on the Ethereum blockchain platform with clinical trials.

The Ethereum platform for biomedical databases proposed a notarized documentation implementation on the blockchain system [147].

6.4. Remote Patient Monitoring

In this segment, we discuss the ways in which blockchain helps with remote patient monitoring. Remote patient monitoring is the gathering of biomedical information using a mobile device or body area sensor, and the patient's condition can be monitored remotely from outside the hospital.

Blockchain can be used to retrieve, share, and store biomedical data collected remotely [148–150]. Figure 12 shows the remote patient monitoring system.

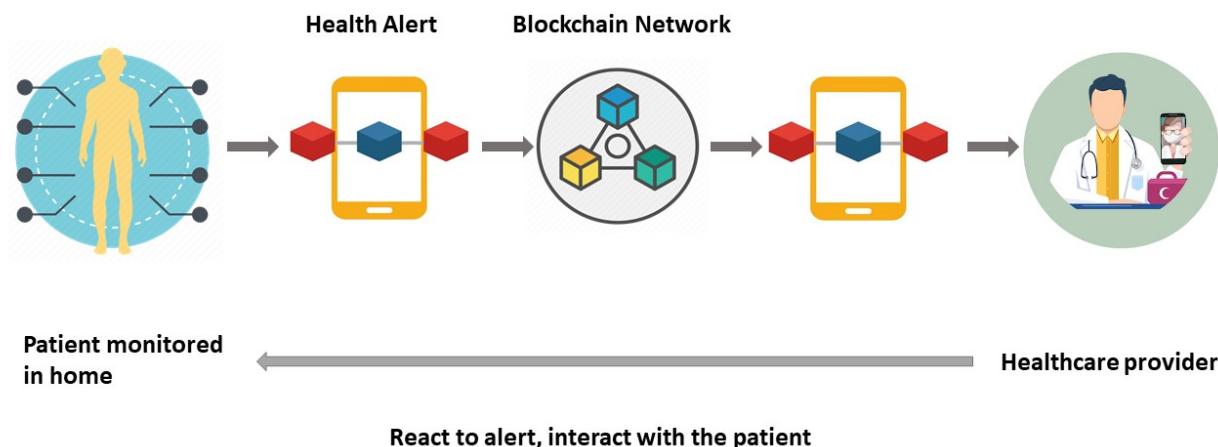


Figure 12. Remote Patient Monitoring System.

Authors of [151] demonstrate that the Ethereum blockchain can be used to facilitate real-time patient tracking in a secure environment. A Hyperledger-based implementation is presented by Liang et al. [152]. The research discusses the way in which blockchain enables data sharing and collection among stakeholders in healthcare. Blockchain is also used in mobile-enabled assistive devices for monitoring patients with diabetes [153]. The data transmitting process using smartphone devices is also possible on the Hyperledger Fabric application where the blockchain system is presented [154].

A patient centric agent (PCA) is one kind of platform where data security works as an end-to-end node and offers the highest privacy for continuous patient monitoring

criteria [155]. In [156], the writer suggest using practical swarm optimization (PSO) to take advantage of selection and feature optimization in blockchain, which may be used by smartphones for medical data synchronization.

6.5. Health Insurance Claims

In the case of health insurance claims, help can be obtained from the blockchain because of its transparency, decentralization, and immutability [133]. Insurance claims processing in the healthcare system is a committed area for the implementation of blockchain. This has been mentioned in numerous papers, including [131,133,143,157,158]. However, we do not see many examples of prototype implementations of these systems. The good news is that there is a good example of this, MIStore, which has been extended to the Ethereum blockchain platform, as can be seen in [51]. A company called Pokitdok expressed interest in working with Intel to create a blockchain-based method that would handle healthcare insurance claims [136].

6.6. Health Data Analysis

Blockchain provides an opportunity for all emerging technologies to harness their power, e.g., deep learning to predict healthcare data and avoid mistakes in medicine [160]. The use of blockchain is discussed in [63,133,143], which provide a roadmap on ways to realize this. To classify arrhythmias, blockchain is used in deep learning [161].

7. Blockchain-Based Solutions in Existing Healthcare Systems

This section covers the solutions suggested in past research based on different technological challenges. Confidentiality, authenticity, scalability, privacy, legitimacy, trustworthiness, non-repudiation, traceability, and audibility are among the current set of applicable healthcare system security objectives that must be addressed. Prior research has attempted to address all of these security concerns, whereas some has focused on a specific area of the medical data system's security requirements. Therefore, solutions of past research are categorized based on their contributions to the achievement of security objectives. Figures 13 and 14 represent these ideas which will be further explained in the following sections.

7.1. Proposed Solutions for the Safety of Medical Data

Prior research has suggested that stacking blockchain layers on top of a traditional system can increase the security value of current medical systems when used in combination with cryptographic approaches. Figure 13 illustrates this method of multiple layering. By using the fundamental features of blockchain, studies [162–165] changed the centralized structure of EHR network communication among healthcare providers into a decentralized network, consequently providing many advantages and addressing security concerns. The decentralized EHR network has reduced third-party reliance, improving the infrastructural health management system, storage management of personal information, advanced data access management, and preservation of safety and confidentiality. Researchers in [166] have introduced a new cryptosystem based on the features of existing cryptosystems (i.e., attribute-based encryption (ABE) and identity-based encryption (IBE)) as well as blockchain technology that assures secrecy, authentication, and medical information integrity and allows complete control of access to cloud-backed medical data. In studies [167–172], the consent function in blockchain was optimized, in which the consensus algorithm governs the access, storage, and distribution of medical data inside an EHR network. The EHR system is in charge of any decision that must be approved by all network members. As a consequence, the network gains a great deal of certainty prior to allowing data to be modified.

This functionality provides an additional layer of certainty to the healthcare information repository network, making it less liable to single point of failure attacks and deterring ransomware and denial-of-service assaults. Researchers in [173] increased the security elements and decreased the intricacy of the existing EHR system by adding a

cipher controller to the blockchain and applying encryption techniques before network data are transferred or received. Every patient has a distinct identity and identifier within the blockchain system, prohibiting the illegal use of information and providing strong data protection. In [174], security and scalability limitations in the existing Health Information Exchange (HIE) system were addressed by adopting a new integrated ACP and consortium blockchain in order to boost diagnostic precision and treatment efficacy. Furthermore, researchers in [175] strengthened the security of insurance management methods by integrating blockchain and homomorphic encryption to ensure safe, decentralized patient information storage.

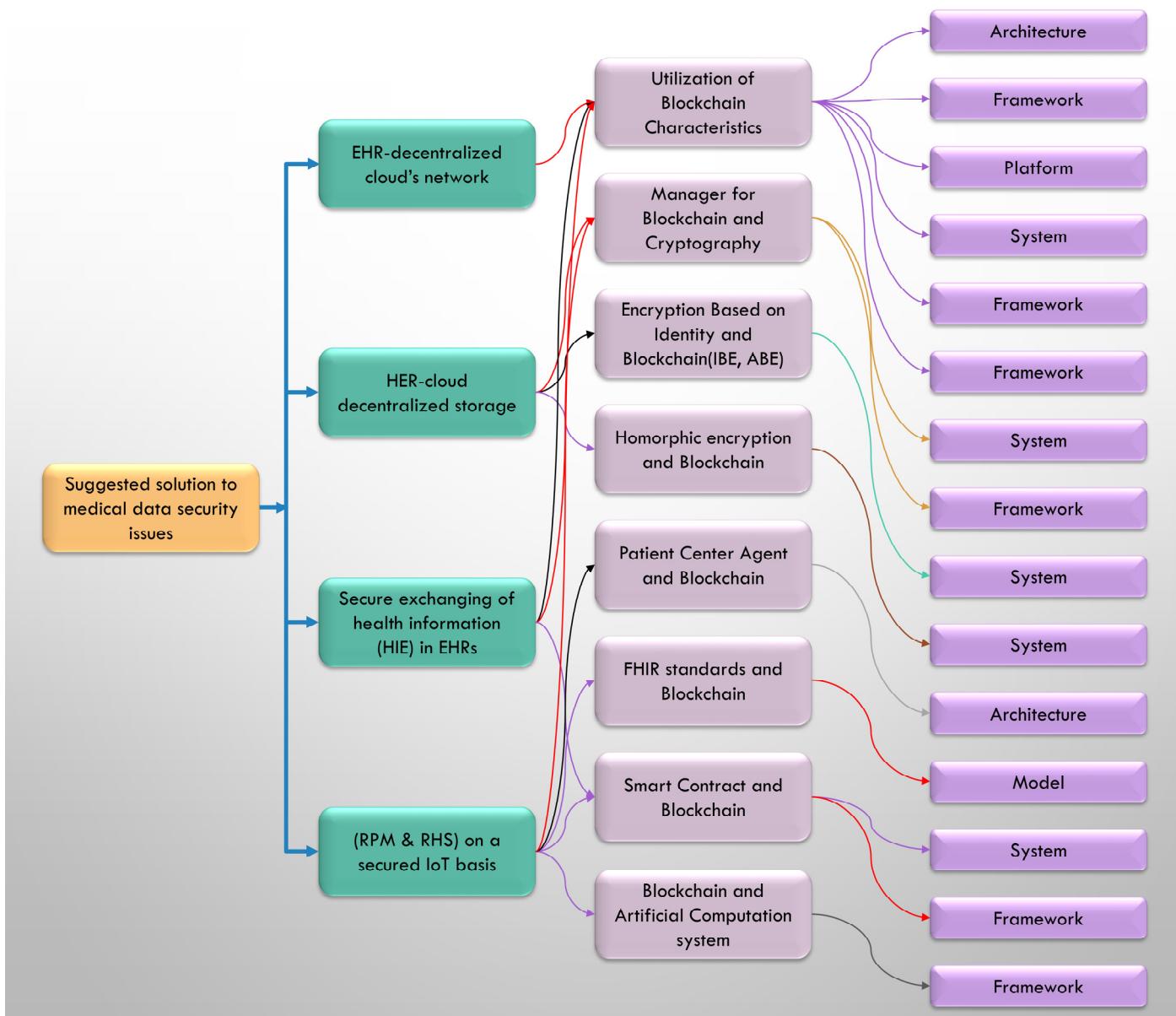


Figure 13. Classification of the Proposed Solutions for Medical Data Security Problems.

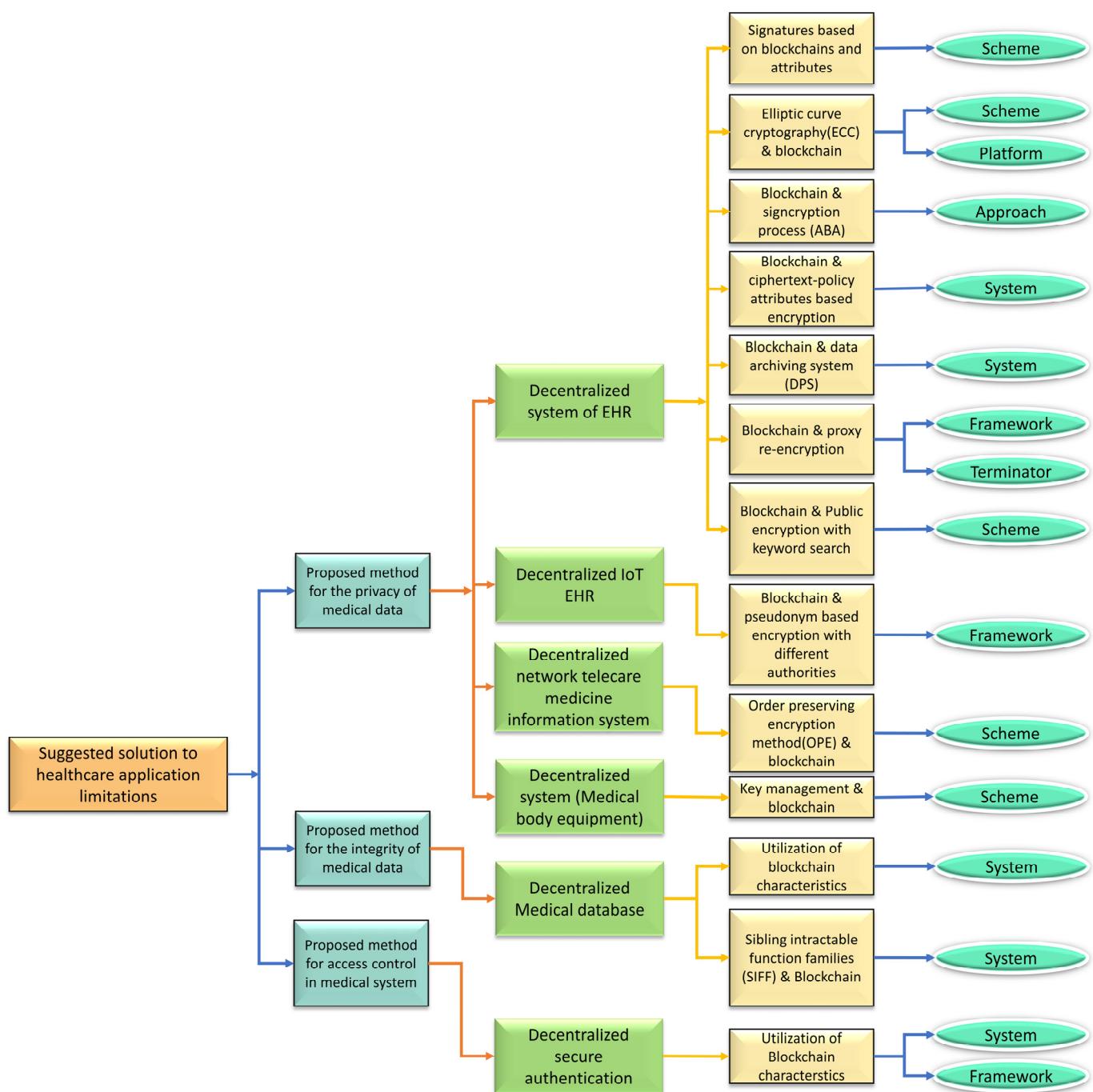


Figure 14. Classification of proposed privacy, integrity, and access control solutions.

Authors of [176] suggested a PCA (Principal Component Analysis) blockchain end-to-end architecture to address IoT RPMS (Remote Patient Monitoring System) security problems by generating vast volumes of data streams while ensuring patient anonymity. The privacy and security implications of data transmission and transaction recording over IoT-RPMS were examined by the authors of [60]. The updated architecture for IoT devices takes into account the benefits of blockchain distribution and many other network security and privacy characteristics in order to guarantee the safe transmission and analysis of massive amounts of data in RPM. The FHIR safety criterion is used in [81] and presents an IoT RPM Chain Model FHR in combination with the distribution characteristics of the blockchain to increase patient privacy and security via a cooperative healthcare decision. In [177], it was determined that deploying smart contracts in the blockchain network

benefited users by eliminating third parties and leveraging extra self-executing, immutable, self-verifying, and auto-enforcing features to manage device-generated data in IoT-RHS (Resource Host Monitor). To avoid security concerns such as DDoS, data breaches, hacking, and clinical remoteness, these components are linked and synchronized over a dispersed network of IoT devices owned and maintained by a variety of organizations.

7.2. Proposed Solutions for Resolving Privacy Issues with Medical Data

Significant efforts have been made to enhance the privacy of medical data for patients and healthcare providers by embedding a cryptographic approach into the decentralized EHR network or any other healthcare applications. Figure 14 illustrates the proposed privacy, integrity, and access control solutions that are described in this section. Authors of [178] attempted to build an effective technique based on ECC (Elliptic curve cryptography) on top of the current blockchain-based EHR system to ensure data accessibility and privacy preservation in the network. The researchers in [90] created an ECC technique to encrypt the back-and-forth exchange of medical data kept in the cloud, avoiding DDoS intrusions due to the blockchain network's pseudonymity.

In [179], a signcryption method (i.e., ABA) was used to safeguard the privacy of medical information sharing in decentralized EHRs, leading to better quality and cost savings associated with medical care. Using a consortium blockchain and ciphertext-policy attribute-based encryption, [180] demonstrated securing data-sharing privacy in a cloud-based EHR system (CP-ABE). Ciphertext Policy Attribute-Based Encryption (CP-ABE) provides excellent data confidentiality and allows data owners to exchange encrypted data with verified sludge storage users while preserving the access control system. In [70], patient privacy protection was addressed by including pseudonym-based encryption with different authorities (PBE-DA) into the multilayer protocol of a blockchain-based IoT-HER (Electronic Health Records) system. In [80], a bilinear keyword polynomial map was established that operates as a verification of conformance for the blockchain, which operates as a consensus technique, to protect and preserve the privacy of the EHR's keyword search protocol. In [49], the issue of keeping the medical information of a patient in a database was addressed by guaranteeing that their information is tamper-proof by utilizing the Ethereum blockchain's features.

A Data Preservation System (DPS) is a P2P network database that is accessible and distributed. It uses proof of primitivity as a consensus technique to preserve data on the blockchain forever. Every patient has severely limited access to EHRs through the blockchain system and cannot conveniently exchange such information with service providers or researchers. The researchers in [88] tackled these obstacles by offering an ABS-based system with several authorities in decentralized EHRs based on blockchain to assure patient confidentiality and interoperability. Using ABS for blockchain healthcare applications, [181] established double privacy preservation abilities in decentralized EHRs across diverse healthcare providers (e.g., clinics, hospitals). ABS in blockchain used for healthcare applications ensures that signer identity authentication remains private. Internal blockchain qualities have provided numerous advantages to EHRs. However, the transparent features may cause PHRs' privacy and confidentiality to be compromised. These issues were addressed in [67,182] by modeling the proxy re-encryption method on top of the blockchain application. This method distributes the task of re-encryption among several nodes. Following that, the EHR system's symmetric keys are segregated and work internally within the node. That is, confidential transactions retain the blockchain's data probity while enhancing privacy. The healthcare applications based on blockchain keep track of transactions that are available to the general public on the network and could be leaked. In [172], a tiered confidentiality sharing method was devised, tiering multiple times for patient whereabouts in the OPE-based TMIS to ensure the confidentiality of locations stored in the blockchain. In [183], critical maintenance systems were linked with blockchain technology to strengthen confidentiality in the medical field, which contains sensitive data.

7.3. Proposed Solutions for Problems with Medical Data Integrity

A system was suggested by the authors of [184] to solve the problem of medical data confidentiality and integrity in a centralized local database by converting it into a decentralized database. Using the blockchain's distinctive characteristics, this method provides more security, anonymity, and reliability. Moreover, this development system produces a hashed copy of the stored medical data to guarantee the integrity of the data. Following that, copies of the data may be provided to organizations desiring to access it (e.g., medical research institutions) to ensure its integrity while evading the threat of an database administrator with bad intentions. As a result, when entities seek access to patient medical data, smart contracts automatically carry out the process. By storing medical information in a decentralized database, implementing an authentication mechanism, and encrypting patient records with a symmetric key, [54] achieved authenticity, scalability, and security in managing the medical data. The integrity aspect of medical data was verified by genuine participants. Data may be stored on a Hyperledger Fabric blockchain, making it impossible for an attacker to change or delete data.

7.4. Proposed Solutions to the Medical System's Access Control Issues

The authors of [185] addressed the issue of centralized authentication by establishing a safe, decentralized authentication provider to protect the system from specific security attacks that occur when patient data are transferred between providers.

The proposed solution addresses authentication and authorization problems in existing EHR healthcare systems that are associated with the transfer of sensitive information among multiple healthcare service providers.

Remarkably, blockchain could be used as a form of authentication. In [59], using IoT-RPM to authenticate and securely communicate with saved devices created by healthcare systems using a blockchain-based mechanism was suggested. Since no one can physically remove information, implementing a blockchain system may enable users' identities and authorization protection against such dangers.

7.5. Proposed Solutions to Interoperability Issues with Medical Data

The EHR blockchain was coupled with AI in [186] to enhance medical data secrecy, security, and interactivity. The suggested solution addresses the medical system's issues with interoperability and medical data exchange across various healthcare service providers. The use of blockchain transactions enables collaboration across many EHR stakeholders while also preventing data fragmentation. In an unreliable cloud platform context, Ref. [94] utilized blockchain characteristics to address the issue of compromised patient confidentiality in medical data exchange interoperability between medical big data providers. As the consensus mechanism regulates the distribution and synchronization of data across various EHR providers, the use of blockchain assures efficient data exchange and zero mistakes. In [65], the problem of communal clinical decision-making being notably safe, protected, and accessible in sharing data was solved by using the Fast Healthcare Interoperability Resources (FHIR) of the HL7 standard and blockchain. This combination successfully enhanced information sharing and resulted in better treatment choices.

The authors of [102] concentrated on the subject of medical image data exchange in the EHR by creating a system for image sharing among various domains that uses a blockchain as a distributed database to create several radiological studies with patient-defined access rights.

7.6. Proposed Solutions to Issues Associated with Handling Large Amounts of Patient Data

To address the issue of compromised patient confidentiality in the interoperability of medical data exchange across healthcare providers, the authors of [94] used blockchain. In [71], researchers used a novel blockchain-based architecture known as the Healthcare Data Gateway (HDG) to manage and exchange patient data efficiently and safely while respecting patient privacy. The development of the architecture solves the problem associated

with healthcare systems regarding collecting, storing, and analyzing personal healthcare data without infringing on privacy and ensures that data are owned and controlled by the patient rather than dispersed across different healthcare providers. Authors of [83] proposed an OmniPHR blockchain-based architecture for integrating PHR between patients and healthcare providers in order to address issues associated with patients' dispersed data records in terms of maintaining and retrieving current and duplicate data.

A new architecture for a decentralized health data ecosystem is suggested in [187] based on blockchain technology that can incorporate massive quantities of clinical data while maintaining anonymity. Medical data providers in an untrustworthy cloud service environment will benefit from the architecture designed to guarantee the quality of medical data in terms of complex analysis, diagnosis, and prediction.

In [94], blockchain technology was utilized in order to address the problem of vulnerable patient privacy and security in medical data sharing across healthcare providers. In [71], a distinctive blockchain-based model was created, the Healthcare Data Gateway (HDG), to effectively and securely store and exchange medical data while maintaining patient confidentiality. The architecture tackles the challenge of obtaining, preserving, and analyzing private health information without infringing on confidentiality, and guarantees that information is owned and maintained by the patient instead of being scattered among multiple healthcare service providers.

8. Discussion

This section discusses the limitations of blockchain in healthcare as well as challenges associated with this method. It also sheds light on the future research scopes and direction of this sector.

8.1. Limitations:

While acknowledging the limitations, previous research indicates that there are technological difficulties. The creation of novel algorithms, protocols, and proofs of concept for applying blockchain in healthcare has been the subject of these review studies. Assumptions, constraints, performance, ethics, and protection are the four categories we have classified for the current constraints based on our research.

8.1.1. Performance

Some research has shown that the essence of artifice direction, which is built for acceptance of the blockchain system in healthcare, may simulate the performance of this proposed structure [63,74,80]. For example, high appeasement measurement may cause the inherent stability of the structure and also the working process. Its design means there may be structures and changes for the documentary. Users rely on manuals, which can be efficient in structure and functionality [87]. The authors of [63] report that the mentioned structure for detecting chaos may be inferior in some cases if it does not detect any labeled dataset. It can be affected by the problem, which can be measured by the performance and scalability of this proposed structure, so the requirement is to continue updating.

Issues such as the necessity for ongoing upgrades by use can also impair a structure's scalability and execution efficiency, framework [46], a calculated load of sensor data [56], the amount of computational load disk space on the sensor data keyword, as well as the size of the network set-up needed for blockchains which are used in this system, such as Ethereum [80,85].

Similarly, researchers in [67] point out that the inclusion of particular features, such as managing global smart contracts, is improved. The structure can be offset if the performance cost becomes too high. Some studies indicate that working process challenges are engaged to improve the nodes of this proposed structure. For instance, uncertainty about the functionality of a structure may be attached to the number of nodes, delays between nodes, or both [73].

8.1.2. Assumptions

The workable ability and competence of this proposed structure compared with the earlier conjecture based on the literature is limited. These assumptions can also influence the proper evaluation of the performance of a structure. For example, patients can use their smartphones to receive and store medical-related information from sensors [77]. However, patients do not need to store all the medical data information to verify whether a valid owner has submitted genuine data or not. Similar terms have been discussed in [83], which states that those who admit they cannot verify the similarity or authenticity of the person or device servicing medical resources face a remarkable limitation. In other research, in [76], a structure for preserving data security where the data storage system is decentralized on the blockchain system is proposed, and based on their structure, it can be assumed that storage data would have proper corroboration on the blockchain system.

8.1.3. Constraints

Researchers have acknowledged the limitations of previous studies, which can be divided into four levels. These marked dimensions expose that such limitations exceed empirical limits.

In relation to the cost of upgrading and extending blockchain-based structures, data exploration and framework components, judgment, and some social spectacles are also involved (such as trust in the government, the technical infrastructure of the country). These are discussed further in the following section.

- Costs: Other costs labeled as limitations in the current study involved linear protocol costs, which depended on the characteristics of the respective organization. For example, patients create operational overhead and assessments may be delayed because of applicants' greater involvement in the apps [87,88]. The transaction and execution costs are created for the size of the string length and input size [90]. Searching time is also a cost-discussed issue as patients need to search for global smart contracts from storage data, so execution time should be short [57,76].
- Data and analysis: Much research has been conducted on data limitations, such as the lack of representation of specimen data. For data-driven simulations and tests, training data is not readily available [47]. Other studies have been limited by the inferiority of testing data [85]. Such limitations may fall on the completion or commencement of rule testing related to authentication within the organization [55]. It may also be affected by the performance testing of a development structure. For example, if the proposed structure presented in [49] is affected by a small amount of dataset, then it not only misuses the space, but also damages the recognition technique of multimedia images.
- Platform and framework elements: The blockchain platform on some elements of the advanced structure can act as an obligation for its improvement. Many previous reports have limitations, including the need for a gateway level for Tangle to receive a direct connection with the sensor [66]. This limited storage, however, is provided by a fog layer as well as compatibility with semantic inter-operative functionality and inheritance systems [65]. Failure to prioritize relevant entities can lead to complications, especially in emergencies, leading to conflicts in decision-making [48]. In addition, it is necessary to ensure that users will receive the full incentive when they share data [52]. Several studies have reported specific limitations for updated algorithms, such as the limitation of an advanced scheme of PSN-dependent blockchain for healthcare [56] and the limitation of another method such as the Optimized Masked Authenticated Messaging (MAM) module library [81].
- Societal environment: A very small amount of research has been conducted on the topic of the societal environment of blockchain healthcare system structure. For example, there would be a probability of creating collusion for information fraud [61] or it may be limited due to inability to monitor clinical abuses [65,79] acknowledged by their created architecture, which will depend on the user's nationwide access to the

internet connection. One more example is the exclusion of refugees from a country's healthcare system [57,79].

8.1.4. Ethics and Security

Our review further proposed that users' anxiety regarding ethical and secure data use could be an important limitation on the blockchain healthcare system. Some limitations are related to technical issues. For example, security systems on individual nodes [59], cryptographic elements in the structure security problems [54], and data privacy maintained when the request is complete to count [71]. However, some research has also been conducted for data sharing concerning social [61] and governmental trust-building [79]. Some concerns have also been raised about the maintenance of the security system from the user perspective, such as the mismanagement of a user's authorized data as a personal key [81].

8.2. Challenges

When properly implemented, blockchain technology can provide a reliable solution to certain healthcare application limitations such as data protection, confidentiality, reliability, sharing, interoperability, usability, and instantaneous medical data updates.

However, blockchain technology is not without its downsides. Regardless of the advantages of blockchain technology, its expansion and use in healthcare applications have created significant research challenges that require further exploration. The challenges of blockchain technology are investigated and identified in this section. The categorization of these issues is depicted in Figure 15.

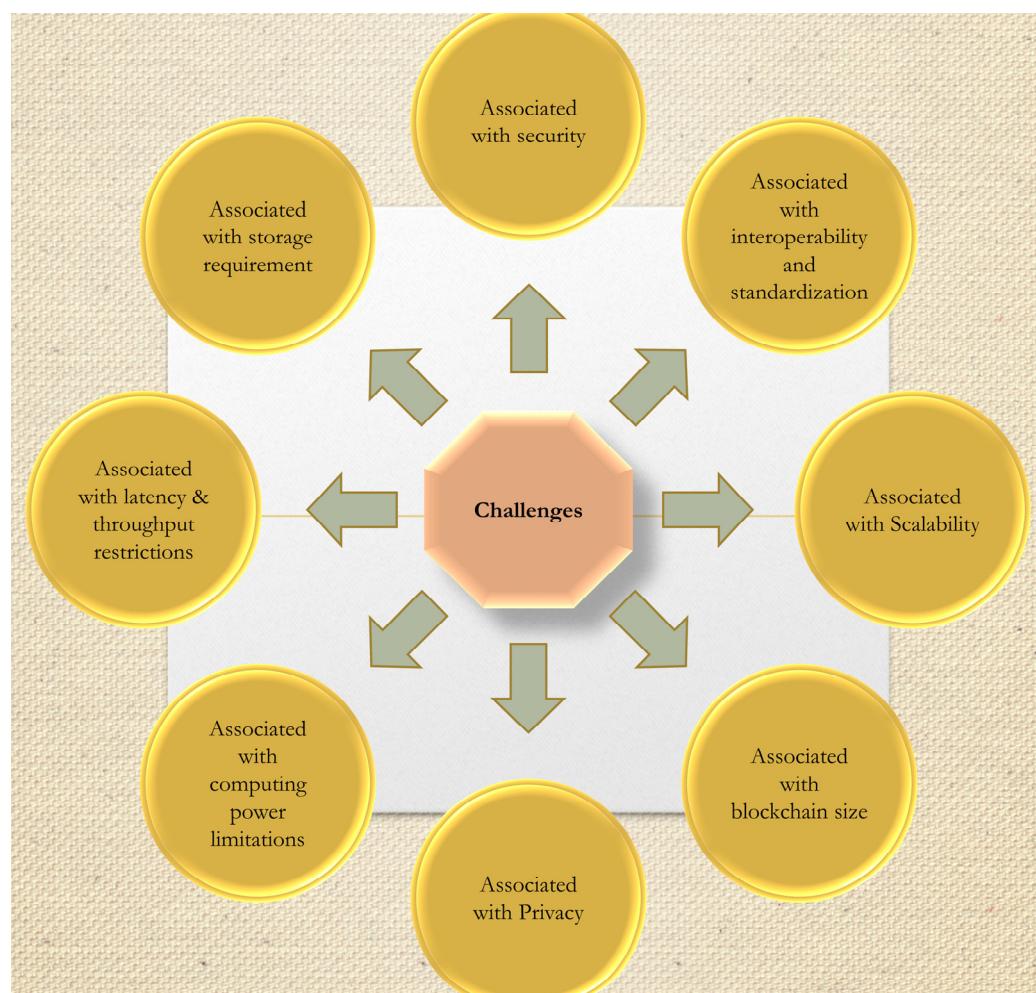


Figure 15. Categorizations of Difficulties in Implementing Blockchain Technology in Healthcare Applications.

8.2.1. Challenges Associated with Security

There are numerous security flaws in the architecture and application of blockchain technology. Security flaws in blockchain are frequently caused by issues with the consensus process that is used to validate and verify transactions. Security flaws include DDoS, transaction malleability, difficulty climbing, eclipse, Sybil, 51 percent, block rejecting, greedy mining, block holding, and double-spending attacks. The distributed blockchain system's consensus process algorithms do not overcome these security flaws. Theoretical considerations alone cannot resolve threats due to the high cost of the resources necessary [189,190]. The importance of consensus methods in overcoming these security concerns is limited. That is, an ideal solution should include a protocol with countermeasures that will prevent these assaults.

Malicious software can exploit security holes in the blockchain in order to create decentralized apps. These malicious attacks use security flaws in smart contract implementation to commit more severe crimes such as identity theft and data theft [191,192]. The use of blockchain creates another potential flaw (i.e., pseudo-anonymity), wherein the stream of transactions could be tracked in order to obtain actual identities or other relevant information [42] due to the public nature of the blockchain network.

8.2.2. Challenges Associated with Interoperability and Standardization

Interoperability in healthcare applications is hampered by the absence of information gathering, sharing, and analysis mechanisms. Conventional EHR solutions rely on centralized local databases and offline structures, while blockchain technology is decentralized and cloud-based.

As a result, reorienting healthcare systems toward this approach and utilizing blockchain technology would necessitate the establishment of an effective EHR system capable of supporting cooperation and interchange between the scientific and medical communities [165,166]. In order to shift EHR data to blockchain technology, there are several technological obstacles to be overcome. The present healthcare databases are not distributed, making them difficult to integrate or extend [90].

8.2.3. Challenges Associated with Scalability

Due to the rising number of system users, the blockchain system offers additional scaling problems in terms of improving overhead or processing capabilities in IoMT (Internet of Medical Things) devices.

This sort of difficulty might result in increased computing needs for the whole blockchain system. This scenario becomes more complicated when multiple sensors or smart devices are present, since the processing capabilities of these devices are less than those of a typical computer. The blockchain network's IoT devices are expensive as well as requiring a large overhead bandwidth, resulting in data latency and hefty processing power. Such devices often lack the processing capacity to utilize blockchain features, resulting in substandard or perhaps exorbitant performance and prohibiting them from operating either their native or blockchain applications [192] simultaneously.

8.2.4. Challenges Associated with Storage Requirement

A blockchain requires a lot of storage to keep track of the network's transactions, which might be an issue for constrained nodes that transmit information to the network. Blockchain can guarantee that stored and distributed EHR data is neither modified, forgeable, or traceable, but it may also potentially display highly distributed EHR data storage needs [181,193].

8.2.5. Challenges Associated with Computing Power Limitations

Blockchain data for IoMT devices is typically computationally constrained, precluding the adoption of cryptographic methods [60]. Cryptosystems in resource-constrained devices that maintain sensors and control security are severely restricted concerning memory and

processing capacity throughout many health-related applications. That also means they face contemporary, secure public key cryptography systems. A vast proportion of blockchains deploy ECC-based public critical cryptographic systems, which already have performance and security concerns, complicating the overall process of selecting suitable cryptographic methods. Blockchain cryptographic systems should be conscious of the post-quantum computing danger and seek out energy-efficient quantum-safe techniques to maintain data security for an extended period.

8.2.6. Challenges Associated with Blockchain Size

Blockchains continue to expand in size as each device performs transactions, including IoT-RPM [59] and EHR [70], necessitating the employment of more powerful miners. Because of their resource limitations, typical IoMT devices cannot support relatively small-scale blockchains. As a result, compression methods in the blockchain should be compared to alternative ways, such as mini-blockchains [60,81].

8.2.7. Challenges Associated with Latency and Throughput Restrictions

Almost all blockchain systems require some time to establish confirmed transactions and consensus. That might aggravate embedding blockchains into healthcare applications, which must respond to actions and information received simultaneously. Transaction latency represents the time a blockchain requires to process a transaction. For instance, the bitcoin blockchain's latency is ten minutes, which means ten minutes are required to confirm any transaction on the network. Although each transaction involves the addition of five to seven blocks to the chain prior to confirmation, it is indeed necessary to delay for approximately one hour before validating every transaction. In comparison, conventional database systems require just a few seconds to validate a transaction [94]. RPM [59,60,81] and EHR [70] are IoT-based blockchain that generally expects systems to process massive numbers of transactions every second.

8.2.8. Challenges Associated with Privacy

The existing secure communication architectures for EHRs are insensitive to the privacy of users or patients, as evidenced by the interchange systems releasing all information without the owners' approval or noise in the data requester description. Nevertheless, if existing EHR programs are developed based on blockchain, the requester needs reliable patient data in order to provide individualized services. The primary issue in ensuring the protection of patient data privacy is creating a foundation for data privacy and confidentiality on an EHR based on blockchain. This functionality makes it much more challenging to determine the precise patient using their actual account number. In any comparable framework, problems in the management of patients' private data should be rectified.

To begin with, patients should be able to quickly and effectively share their data since implementing blockchain-based frameworks inside the EHR requires a considerable amount of processing power and consumes a prolonged time when completing an operation. Additionally, adding an extra node to the blockchain network that new patients necessitate provides several additional steps to confirm that the patient is reliable and trustworthy [80,173].

8.3. Future Research Directions

According to the SLR, a summary of the thematic issues has been compiled that will draw the attention of future scholars. This next section will elaborate further on this topic.

8.3.1. Adoption of a Comprehensive Approach

This is important to develop a resolution to workarounds and system security, interoperability, as shown by the researchers in [90], as well as access management [76]. A complete and thorough perspective is needed for better understanding of blockchain. This is necessary in order to establish complete, legally, and ethically acceptable [68,69]

electronic healthcare ecosystems with solid data administration and authentication procedures [74]. Along with that, we argue for the importance of checking blockchain-based e-healthcare ecosystems in intra- and international and institutional environments as a way of developing context-specific, tailored healthcare solutions in liaison with organizations inside the healthcare ecosystem, such as medical research organizations [47].

8.3.2. Optimization of the Architecture

Researchers may work on ensuring that proposed or tested designs improve in performance and efficiency to accommodate the increasing volume of transactions that may be projected with further implementation of blockchain systems in healthcare operations in the coming years [55]. This could be accomplished by addressing network latency [87], throughput [66], and resources [194].

8.3.3. Data Security and Legal Compliance

Managing data along with patients' privacy and legal difficulties will be an essential topic for future study [59,68,69]. These issues could well be solved by implementing blockchain protocols for handling medical information verified through smart contracts and complying with data and personal privacy standards such as HIPAA (Health Insurance Portability and Accountability Act) [59,195,196].

8.3.4. Integration with Various Technologies

The deployment of blockchain technology in healthcare may benefit from better integrating the technology with business processes to boost functionality. For example, intellectuals could concentrate further on integrating edge computing, machine learning (ML) [196], and artificial intelligence (AI) into healthcare ecosystems based on blockchain in order to significantly improve analytic models for personally tailored patient care and diagnostics [52,63,75]. Furthermore, research may concentrate on enhancing service quality by incorporating more IoT-based sensors to increase service and data ease of access, remote patient monitoring, and emergency response services.

Moreover, we recommend two other prospective approaches for future researchers to examine in order to expand the existing breadth of intellectual limits on this subject. First, we propose that the outcomes of blockchain implementation in healthcare be investigated in much more specific yet similar areas such as patient's digital rights maintenance [197], drug prescription administration [91], and prescription fraud prevention [72].

Finally, exploration could be conducted to determine the implications of blockchain implementation across healthcare valuation and supply chains. This could assist researchers in better understanding the patient-related interoperability difficulties and perhaps enable them to build standardized procedures intended for employing blockchain-based systems in the process of conducting research.

9. Conclusions

This research aimed to conduct a thorough review, survey, and categorization of relevant research papers on blockchain and their integration into various healthcare applications where certain literary patterns may be detected. This paper presented the bibliometric and functional distribution of 144 research papers on blockchain in healthcare. We evaluated the distribution of blockchain platforms and the various kinds of blockchain techniques used or proposed in the examined papers. The blockchain platform allows the development of decentralized applications where the pattern of data transfers is uncontrollable by any third-party organization. The data transactions of the entities are kept in a decentralized database in a verifiable, secure, immutable, and transparent way, along with a timestamp and other pertinent information.

Additionally, blockchain technology has a variety of potential applications in healthcare, including data sharing, log management, medication, biomedical research and teaching, remote patient monitoring, and health data analytics. Even though blockchain adds

many valuable features to healthcare applications, it has some drawbacks. We also analyzed the proposed solution in the reviewed papers for these drawbacks. Despite the considerable interest in blockchain technology, we discovered that its effect on healthcare applications is mostly in the documentation phase. There is yet to be a significant amount of study conducted in this area, as well as healthcare applications built on blockchain.

Author Contributions: Conceptualization, P.K.G.; A.C.; M.H.; K.R.; A.H.S.; methodology, P.K.G.; A.C.; M.H.; investigation, K.R.; A.H.S.; writing—original draft preparation, P.K.G.; A.C.; M.H.; writing—review and editing, K.R.; A.H.S.; supervision, K.R.; A.H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work did not receive any funding to report.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors do not have any conflicts of interest to declare.

References

- McClean, S.; Gillespie, J.; Garg, L.; Barton, M.; Scotney, B.; Kullerton, K. Using phase-type models to cost stroke patient care across health, social and community services. *Eur. J. Oper. Res.* **2014**, *236*, 190–199. [[CrossRef](#)]
- Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. *IEEE Trans. Eng. Manag.* **2023**, *70*, 353–368. [[CrossRef](#)]
- Xing, W.; Bei, Y. Medical Health Big Data Classification Based on KNN Classification Algorithm. *IEEE Access* **2020**, *8*, 28808–28819. [[CrossRef](#)]
- Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BloMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. *IEEE Access* **2022**, *10*, 78887–78898. [[CrossRef](#)]
- Quadery, S.E.U.; Hasan, M.; Khan, M.M. Consumer side economic perception of telemedicine during COVID-19 era: A survey on Bangladesh's perspective. *Inform. Med. Unlocked* **2021**, *27*, 100797. [[CrossRef](#)] [[PubMed](#)]
- Tomlinson, M.; Rotheram-Borus, M.J.; Swartz, L.; Tsai, A.C. Scaling up mhealth: Where is the evidence. *PLoS Med.* **2013**, *10*, e1001382. [[CrossRef](#)]
- Chanda, J.N.; Chowdhury, I.A.; Peyaru, M.; Barua, S.; Islam, M.; Hasan, M. Healthcare Monitoring System for Dedicated COVID-19 Hospitals or Isolation Centers. In Proceedings of the 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India, 24–25 October 2021; pp. 405–410.
- Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for Public Services: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 13904–13921. [[CrossRef](#)]
- Jabeen, F.; Hamid, Z.; Akhunzada, A.; Abdul, W.; Ghouzali, S. Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues. *IEEE Access* **2018**, *6*, 17246–17263. [[CrossRef](#)]
- Ghayvat, H.; Pandya, S.; Bhattacharya, P.; Zuhair, M.; Rashid, M.; Hakak, S.; Dev, K. CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1937–1948. [[CrossRef](#)]
- Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [[CrossRef](#)]
- 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](#)]
- Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access* **2021**, *9*, 37397–37409. [[CrossRef](#)]
- Shynu, P.G.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. *IEEE Access* **2021**, *9*, 45706–45720. [[CrossRef](#)]
- Sun, Z.H.; Chen, Z.; Cao, S.; Ming, X. Potential Requirements and Opportunities of Blockchain-Based Industrial IoT in Supply Chain: A Survey. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 1469–1483. [[CrossRef](#)]
- Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [[CrossRef](#)]
- Liu, Q.; Liu, Y.; Luo, M.; He, D.; Wang, H.; Choo, K.-K.R.C. The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities. *IEEE Syst. J.* **2022**, *16*, 5741–5752. [[CrossRef](#)]
- Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927. [[CrossRef](#)]
- Ahmed, I.; Mousa, A. Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 229–236. [[CrossRef](#)]

20. Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2022**, *27*, 760–776. [[CrossRef](#)]
21. Chinaei, M.H.; Gharakheili, H.H.; Sivaraman, V. Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract. *IEEE Internet Things J.* **2021**, *8*, 10117–10130. [[CrossRef](#)]
22. 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](#)]
23. Li, P.; Xu, C.; Jin, H.; Hu, C.; Luo, Y.; Cao, Y.; Mathew, J.; Ma, Y. ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains. *IEEE Syst. J.* **2020**, *14*, 2042–2053. [[CrossRef](#)]
24. Qahtan, S.; Sharif, K.Y.; Zaidan, A.A.; Alsattar, H.A.; Albahri, O.S.; Zaidan, B.B.; Zulzalil, H.; Osman, M.H.; Alamoodi, A.H.; Mohammed, R.T. Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6415–6423. [[CrossRef](#)]
25. Kapadiya, K.; Patel, U.; Gupta, R.; Alshehri, M.D.; Tanwar, S.; Sharma, G.; Bokoro, P.N. Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. *IEEE Access* **2022**, *10*, 79606–79627. [[CrossRef](#)]
26. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.N.; Shorfuzzaman, M. Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8065–8073. [[CrossRef](#)]
27. Saini, A.; Wijaya, D.; Kaur, N.; Xiang, Y.; Gao, L. LSP: Lightweight Smart-Contract-Based Transaction Prioritization Scheme for Smart Healthcare. *IEEE Internet Things J.* **2022**, *9*, 14005–14017. [[CrossRef](#)]
28. Singh, A.P.; Pradhan, N.R.; Luhach, A.K.; Agnihotri, S.; Jhanjhi, N.Z.; Verma, S.; Ghosh, U.; Roy, D.S. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5779–5789. [[CrossRef](#)]
29. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [[CrossRef](#)]
30. Aujla, G.S.; Jindal, A. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 491–499. [[CrossRef](#)]
31. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2021**, *8*, 5914–5925. [[CrossRef](#)]
32. Akash, S.S.; Ferdous, M.S. A Blockchain Based System for Healthcare Digital Twin. *IEEE Access* **2022**, *10*, 50523–50547. [[CrossRef](#)]
33. Bansal, G.; Rajgopal, K.; Chamola, V.; Xiong, Z.; Niyato, D. Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare. *IEEE Access* **2022**, *10*, 119914–119946. [[CrossRef](#)]
34. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R.; Aledhari, M. Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2146–2156. [[CrossRef](#)] [[PubMed](#)]
35. Kumar, Y.; Nakamoto, S. Bitcoin 6.0: Military Grade e-Payment System. *SSRN Electron. J.* **2020**. [[CrossRef](#)]
36. Jolfaei, A.A.; Aghili, S.F.; Singelee, D. A Survey on Blockchain-Based IoMT Systems: Towards Scalability. *IEEE Access* **2021**, *9*, 148948–148975. [[CrossRef](#)]
37. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [[CrossRef](#)]
38. Anoica, A.; Levard, H. Quantitative Description of Internal Activity on the Ethereum Public Blockchain. In Proceedings of the 2018 9th IFIP international conference on New technologies, Mobility and security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
39. Feng, L.; Zhang, H.; Tsai, W.T.; Sun, S. System architecture for high-performance permissioned blockchains. *Front. Comput. Sci.* **2019**, *13*, 1151–1165. [[CrossRef](#)]
40. Khan, C.; Lewis, A.; Rutland, E.; Wan, C.; Rutter, K.; Thompson, C. A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer* **2017**, *50*, 29–37. [[CrossRef](#)]
41. King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security—CCS’16, Vienna, Austria, 24–28 October 2016; Volume 1918, pp. 1–27.
42. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [[CrossRef](#)]
43. Fahim, A.; Hasan, M.; Chowdhury, M.A. Smart parking systems: Comprehensive review based on various aspects. *Heliyon* **2021**, *7*, e07050. [[CrossRef](#)]
44. Hasan, M.; Biswas, P.; Bilash, M.T.I.; Dipto, M.A.Z. Smart Home Systems: Overview and Comparative Analysis. In Proceedings of the 2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, India, 22–23 November 2018; pp. 264–268.
45. Järvelin, K.; Vakkari, P. LIS research across 50 years: Content analysis of journal articles. *J. Doc.* **2021**, *78*, 65–88. [[CrossRef](#)]
46. Murthy, C.V.B.; Shri, M.L.; Kadry, S.; Lim, S. Blockchain based cloud computing: Architecture and research challenges. *IEEE Access* **2020**, *8*, 205190–205205. [[CrossRef](#)]
47. Acquah, M.A.; Chen, N.; Pan, J.S.; Yang, H.M.; Yan, B. Securing fingerprint template using blockchain and distributed storage system. *Symmetry* **2020**, *12*, 951. [[CrossRef](#)]
48. 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](#)]

49. Lee, T.F.; Li, H.Z.; Hsieh, Y.P. A blockchain-based medical data preservation scheme for telecare medical information systems. *Int. J. Inf. Secur.* **2021**, *20*, 589–601. [CrossRef]
50. Sang, Z.; Yang, K.; Zhang, R. A security technology of power relay using edge computing. *PLoS ONE* **2021**, *16*, e0253428. [CrossRef] [PubMed]
51. Zhou, L.; Wang, L.; Sun, Y. MIStore: A Blockchain-Based Medical Insurance Storage System. *J. Med. Syst.* **2018**, *42*, 149. [CrossRef]
52. Ejaz, M.; Kumar, T.; Kovacevic, I.; Ylianttila, M.; Harjula, E. Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications. *Sensors* **2021**, *21*, 2502. [CrossRef]
53. Suma, B.; Murali, G. Blockchain usage in the electronic health record system using attribute-based signature. *Int. J. Recent Technol. Eng.* **2019**, *8*, 993–997.
54. Natarajan, B.; Balaji, K. Medical Data Management Using Blockchain. *J. ISMAC* **2020**, *2*, 222–231.
55. Magyar, G. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In Proceedings of the 2017 IEEE 30th Neumann Colloquium (NC), Budapest, Hungary, 24–25 November 2017; pp. 135–140.
56. 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.
57. Islam, N.; Faheem, Y.; Din, I.U.; Talha, M.; Guizani, M.; Khalil, M. A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services. *Future Gener. Comput. Syst.* **2019**, *100*, 569–578. [CrossRef]
58. Fan, K.; Wang, S.; Ren, Y.; Yang, K.; Yan, Z.; Li, H.; Yang, Y. Blockchain-Based Secure Time Protection Scheme in IoT. *IEEE Internet Things J.* **2019**, *6*, 4671–4679. [CrossRef]
59. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.H. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef] [PubMed]
60. Mohammed, R.; Alubady, R.; Sherbaz, A. Utilizing blockchain technology for IoT-based healthcare systems. *J. Phys. Conf. Ser.* **2021**, *1818*, 012111. [CrossRef]
61. Hirano, T.; Motohashi, T.; Okumura, K.; Takajo, K.; Kuroki, T.; Ichikawa, D.; Matsuoka, Y.; Ochi, E.; Ueno, T. Data validation and verification using blockchain in a clinical trial for breast cancer: Regulatory sandbox. *J. Med. Internet Res.* **2020**, *22*, e18938. [CrossRef]
62. Lee, S.J.; Cho, G.Y.; Ikeno, F.; Lee, T.R. BAQALC: Blockchain applied lossless efficient transmission of DNA sequencing data for next generation medical informatics. *Appl. Sci.* **2018**, *8*, 1471. [CrossRef]
63. Tagde, P.; Tagde, S.; Bhattacharya, T.; Tagde, P.; Chopra, H.; Akter, R.; Kaushik, D.; Rahman, M. Blockchain and artificial intelligence technology in e-Health. *Environ. Sci. Pollut. Res.* **2021**, *28*, 52810–52831. [CrossRef]
64. Noh, S.W.; Park, Y.; Sur, C.; Shin, S.U.; Rhee, K.H. Blockchain-Based User-Centric Records Management System. *Int. J. Control Autom.* **2017**, *10*, 133–144. [CrossRef]
65. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef]
66. Farahani, B.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [CrossRef]
67. Chenthara, 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] [PubMed]
68. Kuo, T.T.; Gabriel, R.A.; Ohno-Machado, L. Fair compute loads enabled by blockchain: Sharing models by alternating client and server roles. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 392–403. [CrossRef] [PubMed]
69. Hasselgren, A.; Rensaa, J.A.H.; Kralevska, K.; Gligoroski, D.; Faxvaag, A. Blockchain for increased trust in virtual health care: Proof-of-concept study. *J. Med. Internet Res.* **2021**, *23*, e28496. [CrossRef] [PubMed]
70. Hemalatha, P. Monitoring and Securing the Healthcare Data Harnessing IOT and Blockchain Technology. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 2554–2561.
71. 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]
72. Casado-Vara, R.; Corchado, J. Distributed e-health wide-world accounting ledger via blockchain. *J. Intell. Fuzzy Syst.* **2019**, *36*, 2381–2386. [CrossRef]
73. Hyla, T.; Pejaš, J. eHealth integrity model based on permissioned blockchain. *Future Internet* **2019**, *11*, 76. [CrossRef]
74. Guo, Y.; Li, Y.; Wang, F.; Wei, Y.; Rong, Z. Processes controlling sea surface temperature variability of ningaloo niño. *J. Clim.* **2020**, *33*, 4369–4389. [CrossRef]
75. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [CrossRef]
76. Shrestha, A.K.; Vassileva, J.; Deters, R. A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. *Front. Blockchain* **2020**, *3*, 497985. [CrossRef]
77. Bokefode, J.D.; Komarasamy, G. A remote patient monitoring system: Need, trends, challenges and opportunities. *Int. J. Sci. Technol. Res.* **2019**, *8*, 830–835.
78. CSwanaposri, C.; Bhatiasevi, V.; Thanakijksombat, T. Drivers of Blockchain Adoption in Financial and Supply Chain Enterprises. *Glob. Bus. Rev.* **2021**. [CrossRef]

79. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [CrossRef]
80. Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Comput. Mater. Contin.* **2020**, *65*, 87–107. [CrossRef]
81. PPandey, P.; Litoriya, R. Securing and authenticating healthcare records through blockchain technology. *Cryptologia* **2020**, *44*, 341–356. [CrossRef]
82. Nagasubramanian, G.; Sakthivel, R.K.; Patan, R.; Gandomi, A.H.; Sankayya, M.; Balusamy, B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput. Appl.* **2020**, *32*, 639–647. [CrossRef]
83. Roehrs, A.; da Costa, C.A.; Righi, R.R.; Mayer, A.H.; da Silva, V.F.; Goldim, J.R.; Schmidt, D.C. Integrating multiple blockchains to support distributed personal health records. *Health Inform. J.* **2021**, *27*, 14604582211007546. [CrossRef]
84. Ijaz, M.; Li, G.; Lin, L.; Cheikhrouhou, O.; Hamam, H.; Noor, A. Integration and applications of fog computing and cloud computing based on the internet of things for provision of healthcare services at home. *Electronics* **2021**, *10*, 1077. [CrossRef]
85. Chukwu, E.; Garg, L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access* **2020**, *8*, 21196–21214. [CrossRef]
86. Taralunga, D.D.; Florea, B.C. A blockchain-enabled framework for mhealth systems. *Sensors* **2021**, *21*, 2828. [CrossRef]
87. 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]
88. Fang, W.; Chen, W.; Zhang, W.; Pei, J.; Gao, W.; Wang, G. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 56. [CrossRef]
89. Ray, P.P.; Dash, D.; Salah, K.; Kumar, N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Syst. J.* **2021**, *15*, 85–94. [CrossRef]
90. Sivan, R.; Zukarnain, Z.A. Security and privacy in cloud-based e-health system. *Symmetry* **2021**, *13*, 742. [CrossRef]
91. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
92. Patane, R.; Nadar, A.; Dubey, V.; Nadar, C. Medical Data Access and Permission Management Using BlockChain. *JETIR Res. J.* **2019**, *6*, 655–658.
93. Praveen, G. The Impact of Blockchain on the Healthcare Environment. *J. Inform. Electr. Electron. Eng.* **2021**, *2*, 1–11. [CrossRef]
94. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
95. Yehualashet, D.E.; Seboka, B.T.; Tesfa, G.A.; Demeke, A.D.; Amede, E.S. Barriers to the adoption of electronic medical record system in ethiopia: A systematic review. *J. Multidiscip. Healthc.* **2021**, *14*, 2597–2603. [CrossRef]
96. Mayer, A.H.; da Costa, C.A.; Righi, R.D.R. Electronic health records in a Blockchain: A systematic review. *Health Inform. J.* **2020**, *26*, 1273–1288. [CrossRef]
97. Blocki, J.; Harsha, B.; Kang, S.; Lee, S.; Xing, L.; Zhou, S. Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2019; pp. 573–607.
98. Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; Dennis, M. MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange. *IEEE Internet Things J.* **2021**, *8*, 15762–15775. [CrossRef]
99. Yadav, S.; Rishi, R. A Systematic and Critical Analysis of the Developments in the Field of Intelligent Transportation System. *Adv. Dyn. Syst. Appl.* **2021**, *16*, 901–911. [CrossRef]
100. Hasan, H.R.; Salah, K.; Jayaraman, R.; Omar, M.; Yaqoob, I.; Pesic, S.; Taylor, T.; Boscovic, D. A Blockchain-Based Approach for the Creation of Digital Twins. *IEEE Access* **2020**, *8*, 34113–34126. [CrossRef]
101. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access* **2020**, *8*, 118433–118471. [CrossRef]
102. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]
103. Zhuang, Y.; Sheets, L.R.; Chen, Y.-W.; Shae, Z.-Y.; Tsai, J.J.P.; Shyu, C.-R. A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176. [CrossRef]
104. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
105. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput. Secur.* **2020**, *97*, 101966. [CrossRef]
106. da Fonseca Ribeiro, M.I.; Vasconcelos, A. MedBlock: Using blockchain in health healthcare application based on blockchain and smart contracts. In Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020), Online Streaming, 5–7 May 2020; Volume 1, pp. 156–164.
107. De Aguiar, E.J.; Faiçal, B.S.; Krishnamachari, B.; Ueyama, J. A Survey of Blockchain-Based Strategies for Healthcare. *ACM Comput. Surv.* **2020**, *53*, 27. [CrossRef]
108. Wang, Z.; Wang, L.; Chen, Q.; Lu, L.; Hong, J. A traditional Chinese medicine traceability system based on lightweight blockchain. *J. Med. Internet Res.* **2021**, *23*, e25946. [CrossRef]

109. Velmovitsky, P.E.; Souza, P.A.D.S.E.; Vaillancourt, H.; Donovska, T.; Teague, J.; Morita, P.P. A blockchain-based consent platform for active assisted living: Modeling study and conceptual framework. *J. Med. Internet Res.* **2020**, *22*, e20832. [[CrossRef](#)]
110. Tomlinson, B.; Boberg, J.; Cranefield, J.; Johnstone, D.; Luczak-Roesch, M.; Patterson, D.J.; Kapoor, S. Analyzing the sustainability of 28 ‘Blockchain for Good’ projects via affordances and constraints. *Inf. Technol. Dev.* **2021**, *27*, 439–469. [[CrossRef](#)]
111. Wang, Y.C.; Ganzorig, B.; Wu, C.C.; Iqbal, U.; Khan, H.A.A.; Hsieh, W.S.; Jian, W.S.; Li, Y.C.J. Patient satisfaction with dermatology teleconsultation by using MedX. *Comput. Methods Programs Biomed.* **2018**, *167*, 37–42. [[CrossRef](#)]
112. Salahuddin, M.A.; Al-Fuqaha, A.; Guizani, M.; Shuaib, K.; Sallabi, F. Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare. *Computer* **2017**, *50*, 74–79. [[CrossRef](#)]
113. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain consensus: An overview of alternative protocols. *Symmetry* **2021**, *13*, 1363. [[CrossRef](#)]
114. Cachin, C.; Schubert, S.; Vukolić, M. Non-determinism in Byzantine fault-tolerant replication. *Leibniz Int. Proc. Inform. LIPIcs* **2017**, *70*, 24.1–24.16.
115. Salimitari, M.; Chatterjee, M.; Fallah, Y.P. A survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet Things* **2020**, *11*, 100212. [[CrossRef](#)]
116. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [[CrossRef](#)]
117. Lee, Y.; Rathore, S.; Park, J.H.; Park, J.H. A blockchain-based smart home gateway architecture for preventing data forgery. *Hum. Cent. Comput. Inf. Sci.* **2020**, *10*, 9. [[CrossRef](#)]
118. de Oliveira Fornasier, M. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. *Rev. Investig. Const.* **2019**, *6*, 297–321.
119. Li, H.; Yu, L.; He, W. The Impact of GDPR on Global Technology Development. *J. Glob. Inf. Technol. Manag.* **2019**, *22*, 1–6. [[CrossRef](#)]
120. Vanderpool, D. HIPAA COMPLIANCE: A Common Sense Approach. *Innov. Clin. Neurosci.* **2019**, *16*, 38–41. [[PubMed](#)]
121. Hussain, S.Z.; Kumar, M. Secured Key Agreement Schemes in Wireless Body Area Network—A Review. *Indian J. Sci. Technol.* **2021**, *14*, 2005–2033. [[CrossRef](#)]
122. Salem, O.; Alsubhi, K.; Mehaoua, A.; Boutaba, R. Markov Models for Anomaly Detection in Wireless Body Area Networks for Secure Health Monitoring. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 526–540. [[CrossRef](#)]
123. Taiwo, O.; Ezugwu, A.E. Smart healthcare support for remote patient monitoring during COVID-19 quarantine. *Inform. Med. Unlocked* **2020**, *20*, 100428. [[CrossRef](#)] [[PubMed](#)]
124. Huang, G.; al Foysal, A. Blockchain in Healthcare. *Technol. Invest.* **2021**, *12*, 168–181. [[CrossRef](#)]
125. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access* **2018**, *6*, 32700–32726. [[CrossRef](#)]
126. Fatokun, T.; Nag, A.; Sharma, S. Towards a blockchain assisted patient owned system for electronic health records. *Electronics* **2021**, *10*, 580. [[CrossRef](#)]
127. Chang, S.E.; Chen, Y.C. Blockchain in health care innovation: Literature review and case study from a business ecosystem perspective. *J. Med. Internet Res.* **2020**, *22*, e19480. [[CrossRef](#)] [[PubMed](#)]
128. Gope, P.; Gheraibia, Y.; Kabir, S.; Sikdar, B. A Secure IoT-Based Modern Healthcare System with Fault-Tolerant Decision Making Process. *IEEE J. Biomed. Health Inform.* **2021**, *25*, 862–873. [[CrossRef](#)]
129. Alamri, B.; Crowley, K.; Richardson, I. Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review. *IEEE Access* **2022**, *10*, 59612–59629. [[CrossRef](#)]
130. Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [[CrossRef](#)]
131. Velmovitsky, P.E.; Bublitz, F.M.; Fadrique, L.X.; Morita, P.P. Blockchain applications in health care and public health: Increased transparency. *JMIR Med. Inform.* **2021**, *9*, e20713. [[CrossRef](#)]
132. Mettler, M.; Hsg, M.A. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 16–18.
133. Boulos, M.N.K.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*, 25. [[CrossRef](#)] [[PubMed](#)]
134. Johny, S.; Priyadharsini, C. Investigations on the Implementation of Blockchain Technology in Supplychain Network. In Proceedings of the 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 19–20 March 2021; pp. 1–6. [[CrossRef](#)]
135. Ahmad, R.W.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Ellahham, S.; Omar, M. The role of blockchain technology in telehealth and telemedicine. *Int. J. Med. Inform.* **2021**, *148*, 104399. [[CrossRef](#)] [[PubMed](#)]
136. Rejeb, A.; Treiblmaier, H.; Rejeb, K.; Zailani, S. Blockchain research in healthcare: A bibliometric review and current research trends. *J. Data Inf. Manag.* **2021**, *3*, 109–124. [[CrossRef](#)]
137. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Hyperledger Fabric Blockchain for Securing the Edge Internet of Things. *Sensors* **2021**, *21*, 359. [[CrossRef](#)]

138. Hellani, H.; Sliman, L.; Samhat, A.; Exposito, E. On Blockchain Integration with Supply Chain: Overview on Data Transparency. *Logistics* **2021**, *5*, 46. [\[CrossRef\]](#)
139. Mackey, T.K.; Nayyar, G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opin. Drug Saf.* **2017**, *16*, 587–602. [\[CrossRef\]](#)
140. Mann, S.P.; Savulescu, J.; Ravaud, P.; Benchoufi, M. Blockchain, consent and present for medical research. *J. Med. Ethic* **2020**, *47*, 244–250. [\[CrossRef\]](#)
141. Lee, H.A.; Kung, H.H.; Udayasankaran, J.G.; Kijasanayotin, B.; Marcelo, A.B.; Chao, L.R.; Hsu, C.Y. An architecture and management platform for blockchain-based personal health record exchange: Development and usability study. *J. Med. Internet Res.* **2020**, *22*, e16748. [\[CrossRef\]](#) [\[PubMed\]](#)
142. Hang, L.; Kim, B.; Kim, K.; Kim, D. A Permissioned Blockchain-Based Clinical Trial Service Platform to Improve Trial Data Transparency. *BioMed Res. Int.* **2021**, *2021*, 5554487. [\[CrossRef\]](#) [\[PubMed\]](#)
143. 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. [\[CrossRef\]](#) [\[PubMed\]](#)
144. Rensaa, J.A.H.; Gligoroski, D.; Kralevska, K.; Hasselgren, A.; Faxvaag, A. VerifyMed-A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept. In Proceedings of the 2nd International Electronics Communication Conference (IECC 20), Singapore, 8–10 July 2020; pp. 73–80.
145. Omar, I.A.; Jayaraman, R.; Salah, K.; Simsekler, M.C.E.; Yaqoob, I.; Ellahham, S. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Med. Res. Methodol.* **2020**, *20*, 224. [\[CrossRef\]](#)
146. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer Peer Netw. Appl.* **2021**, *14*, 2901–2925. [\[CrossRef\]](#)
147. Kleinaki, A.-S.; Mytis-Gkometh, P.; Drosatos, G.; Efraimidis, P.S.; Kaldoudi, E. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 288–297. [\[CrossRef\]](#)
148. Sharma, A.; Kaur, S.; Singh, M. A comprehensive review on blockchain and Internet of Things in healthcare. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4333. [\[CrossRef\]](#)
149. Zhang, J.; Xue, N.; Huang, X. A Secure System For Pervasive Social Network-Based Healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [\[CrossRef\]](#)
150. Weiss, M.; Botha, A.; Herselman, M.; Loots, G. Blockchain as an enabler for public mHealth solutions in South Africa. In Proceedings of the 2017 IST-Africa Week Conference, Windhoek, Namibia, 31 May–2 June 2017; pp. 1–8. [\[CrossRef\]](#)
151. Jabarulla, M.Y.; Lee, H.-N. Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications. *Healthcare* **2021**, *9*, 1019. [\[CrossRef\]](#)
152. 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. [\[CrossRef\]](#)
153. Rodriguez-León, C.; Villalonga, C.; Munoz-Torres, M.; Ruiz, J.R.; Banos, O. Mobile and wearable technology for the monitoring of diabetes-related parameters: Systematic review. *JMIR Mhealth Uhealth* **2021**, *9*, e25138. [\[CrossRef\]](#)
154. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR mHealth uHealth* **2017**, *5*, e111. [\[CrossRef\]](#) [\[PubMed\]](#)
155. Paganelli, A.I.; Velmovitsky, P.E.; Miranda, P.; Branco, A.; Alencar, P.; Cowan, D.; Endler, M.; Morita, P.P. A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home. *Internet Things* **2021**, *18*, 100399. [\[CrossRef\]](#)
156. Firdaus, A.; Anuar, N.B.; Ab Razak, M.F.; Hashem, I.A.T.; Bachok, S.; Sangaiah, A.K. Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management. *J. Med Syst.* **2018**, *42*, 112. [\[CrossRef\]](#) [\[PubMed\]](#)
157. Alkhateeb, Y.M. Blockchain Implications in the Management of Patient Complaints in Healthcare. *J. Inf. Secur.* **2021**, *12*, 212–223. [\[CrossRef\]](#)
158. Kamenivskyy, Y.; Palisetti, A.; Hamze, L.; Saberi, S. A Blockchain-Based Solution for COVID-19 Vaccine Distribution. *IEEE Eng. Manag. Rev.* **2022**, *50*, 43–53. [\[CrossRef\]](#)
159. Bhadoria, R.S.; Das, A.P.; Bashar, A.; Zikria, M. Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections. *Electronics* **2022**, *11*, 3359. [\[CrossRef\]](#)
160. Kasyap, H.; Tripathy, S. Privacy-preserving Decentralized Learning Framework for Healthcare System. *ACM Trans. Multimed. Comput. Commun. Appl.* **2021**, *17*, 1–24. [\[CrossRef\]](#)
161. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [\[CrossRef\]](#)
162. Ray, P.P.; Chowhan, B.; Kumar, N.; Almogren, A. BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. *IEEE Internet Things J.* **2021**, *8*, 10857–10872. [\[CrossRef\]](#)
163. Gadekallu, T.R.; Manoj, M.K.; Kumar, N.; Hakak, S.; Bhattacharya, S. Blockchain-Based Attack Detection on Machine Learning Algorithms for IoT-Based e-Health Applications. *IEEE Internet Things Mag.* **2021**, *4*, 30–33. [\[CrossRef\]](#)
164. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [\[CrossRef\]](#)
165. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, *42*, 156. [\[CrossRef\]](#) [\[PubMed\]](#)

166. Li, F.; Liu, K.; Zhang, L.; Huang, S.; Wu, Q. EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem. *IEEE Trans. Serv. Comput.* **2021**, *15*, 2755–2765. [CrossRef]
167. Jiang, S.; Jakobsen, K.; Bueie, J.; Li, J.; Haro, P.H. A Tertiary Review on Blockchain and Sustainability With Focus on Sustainable Development Goals. *IEEE Access* **2022**, *10*, 114975–115006. [CrossRef]
168. Sun, J.; Ren, L.; Wang, S.; Yao, X. A blockchain-based framework for electronic medical records sharing with fine-grained access control. *PLoS ONE* **2020**, *15*, e0239946. [CrossRef]
169. Kaur, J.; Rani, R.; Kalra, N. Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6369. [CrossRef]
170. Alabdulkarim, Y.; Alameer, A.; Almukaynizi, M.; Almaslukh, A. SPIN: A Blockchain-Based Framework for Sharing COVID-19 Pandemic Information across Nations. *Appl. Sci.* **2021**, *11*, 8767. [CrossRef]
171. Touloupou, M.; Themistocleous, M.; Iosif, E.; Christodoulou, K. A Systematic Literature Review Toward a Blockchain Benchmarking Framework. *IEEE Access* **2022**, *10*, 70630–70644. [CrossRef]
172. Wang, Q.; Xia, T.; Ren, Y.; Yuan, L.; Miao, G. A New Blockchain-Based Multi-Level Location Secure Sharing Scheme. *Appl. Sci.* **2021**, *11*, 2260. [CrossRef]
173. Huang, A.W.; Kandula, A.; Wang, X. A Differential-Privacy-Based Blockchain Architecture to Secure and Store Electronic Health Records. In Proceedings of the 3rd International Conference on Blockchain Technology, Shanghai, China, 26–28 March 2021; pp. 189–194.
174. Dauda, I.; Nuhu, B.; Abubakar, J.; Abdullahi, I.; Maliki, D. Blockchain Technology in Healthcare Systems: Applications, Methodology, Problems, and Current Trends. *J. Sci. Technol. Educ.* **2021**, *9*, 431–443.
175. Angeletti, F.; Chatzigiannakis, I.; Vitaletti, A. The role of blockchain and IoT in recruiting participants for digital clinical trials. In Proceedings of the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 21–23 September 2017; pp. 1–5. [CrossRef]
176. Ali, M.S.; Vecchio, M.; Putra, G.D.; Kanhere, S.S.; Antonelli, F. A Decentralized Peer-to-Peer Remote Health Monitoring System. *Sensors* **2020**, *20*, 1656. [CrossRef] [PubMed]
177. 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]
178. Hussien, H.; Yasin, S.; Udzir, N.; Ninggal, M. Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage. *Sensors* **2021**, *21*, 2462. [CrossRef] [PubMed]
179. Hasan, M.; Anik, M.H.; Islam, S. Microcontroller Based Smart Home System with Enhanced Appliance Switching Capacity. In Proceedings of the 2018 Fifth HCT Information Technology Trends (ITT), Dubai, United Arab Emirates, 28–29 November 2018; pp. 364–367.
180. Sharma, Y. A survey on privacy preserving methods of electronic medical record using blockchain. *J. Mech. Contin. Math. Sci.* **2020**, *15*, 32–47. [CrossRef]
181. Eltayieb, N.; Elhabob, R.; Hassan, A.; Li, F. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. *J. Syst. Arch.* **2019**, *102*, 101653. [CrossRef]
182. Rajput, A.; Li, Q.; Ahvanooey, M. A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition. *Healthcare* **2021**, *9*, 206. [CrossRef]
183. Panda, S.S.; Jena, D.; Mohanta, B.K.; RamasubbaReddy, S.; Daneshmand, M.; Gandomi, A.H. Authentication and Key Management in Distributed IoT Using Blockchain Technology. *IEEE Internet Things J.* **2021**, *8*, 12947–12954. [CrossRef]
184. Pawar, P.; Parolia, N.; Shinde, S.; Edoh, T.O.; Singh, M. eHealthChain—a blockchain-based personal health information management system. *Ann. Telecommun.* **2021**, *77*, 33–45. [CrossRef]
185. Javed, I.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K. Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare* **2021**, *9*, 712. [CrossRef]
186. Shinde, R.; Patil, S.; Kotecha, K.; Ruikar, K. Blockchain for Securing AI Applications and Open Innovations. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 189. [CrossRef]
187. Faisal, F.; Hasan, M.; Sabrin, S.; Hasan, Z.; Siddique, A.H. Voice Activated Portable Braille with Audio Feedback. In Proceedings of the 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 5–7 January 2021; pp. 418–423. [CrossRef]
188. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
189. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]
190. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2017**, *107*, 841–853. [CrossRef]
191. LeHoty, D.L. The greater scope of the economic security program. *Kyoto Daigaku Kokugakko Kiyo Bull. Stomatol. Kyoto Univ.* **1965**, *30*, 28–30.
192. 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]
193. Hasan, M.; Hosseini, J.; Hossain, M.; Zaman, H.U.; Islam, S. Design of a Scalable Low-Power 1-Bit Hybrid Full Adder for Fast Computation. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *67*, 1464–1468. [CrossRef]

194. Chowdhury, S.; Hasan, M. Design of an automatic gain control loop for high speed communication. *Int. J. Circuit Theory Appl.* **2022**, *51*, 47–66. [[CrossRef](#)]
195. Alla, S.; Soltanisehat, L.; Tatar, U.; Keskin, O. Blockchain technology in electronic healthcare systems. In Proceedings of the IISE Annual Conference and Expo 2018, Orlando, FL, USA, 19–22 May 2018; pp. 754–759.
196. Sultana, J.; Saha, B.; Khan, S.; Sanjida, T.M.; Hasan, M.; Khan, M.M. Identification and Classification of Melanoma Using Deep Learning Algorithm. In Proceedings of the 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Elec-tronics (ICDCECE), Ballari, India, 23–24 April 2022; pp. 1–6.
197. Abou Jaoude, J.; Saade, R.G. Blockchain Applications—Usage in Different Domains. *IEEE Access* **2019**, *7*, 45360–45381. [[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.