Blockchain application in healthcare system: A systematic review, synthesizing issues and future exploration

Artenie Andrada[1]

[1] Department of Computers and Information Technology University of Oradea, andradaartenie@gmail.com

Abstract. In recent years, the healthcare sector has witnessed a surge in interest surrounding blockchain technology, primarily due to its perceived capacity to ameliorate a wide spectrum of significant challenges encountered in electronic health record systems. This review offers a comprehensive and in-depth examination of the existing body of scholarly works addressing the application of blockchain technologies within the healthcare industry as well as the electronic healthcare system. Within this context, the study scrutinizes 30 scholarly articles that delve into the importance and constraints associated with leveraging blockchain solutions to enhance healthcare operations. The principal aim of this investigation is to illustrate the potential utility of blockchain technology, shedding light on the challenges it poses and identifying promising domains for future research initiatives within the healthcare sphere. The research undertaking begins with an extensive exploration of the foundational aspects of blockchain and its inherent features. Subsequently, the study transitions into a thorough literature review of the selected articles, with a focus on elucidating the prevailing research themes pertinent to blockchain-based healthcare systems. Following this, the investigation discerns the primary areas of application and outlines the solutions that blockchain technology offers to enhance healthcare systems. Lastly, the discussion section provides valuable insights into the limitations and challenges encountered in the utilization of blockchain in healthcare, while also suggesting potential directions for future research in this field.

1. Introduction

Blockchain applications find utility across a spectrum of industries, encompassing finance, healthcare, manufacturing, and education, capitalizing on the distinct array of properties offered by this technology. Blockchain technology (BT) proposes advantages in credibility, trustworthiness, organization, and transparency [1]. The unique amalgamation of traits, inclusive of decentralization, immutability, and transparency, positions blockchain technology (BT) as a promising enabler for diverse sectors [2]. Anticipations are held that this technology holds promise for constructive applications within academia and science.

One sector poised for substantial impact from blockchain is healthcare. In the realm of health informatics, scholars and practitioners continually grapple with the rapid expansion of research in this dynamic field. This article undertakes an extensive evaluation of recent studies exploring the incorporation of blockchain technology within the healthcare industry [3].

Blockchain technology was first introduced and applied in the context of the Bitcoin cryptocurrency in 2008. Electronic health records constitute a crucial element of the healthcare sector and its health information technology (HIT) frameworks, playing a vital role in contemporary life. Nevertheless, the gathering and exchange of medical data among different HIT systems present substantial security questioning because of the extensive and sensitive nature of the information. The storage of such data in a customary or traditional database is notably challenging and not a straightforward solution [4]. Formulated with a focus on security, blockchain technology holds the potential to tackle these security challenges. A pivotal characteristic of a blockchain is its decentralized and distributed nature, signifying that it lacks control from a singular entity and avoids a central point of vulnerability. This complexity makes it challenging for a lone entity to manipulate the data stored on the blockchain without obtaining consensus from the network. [4][5]

Blockchain technology possesses the capability to revolutionize the healthcare sector by positioning the patient as the focal point of the health system, enhancing the security, confidentiality, and interoperability of health data. This innovation has the potential to redefine health information exchange (HIE) by streamlining and fortifying electronic health records (EHRs). [5] EHRs, presented in a digital format, encapsulate a patient's health data, persisting throughout their lifetime, and are typically dispersed across various hospitals, clinics, and healthcare providers. These providers typically hold primary access to the records, impeding easy patient access to historical data. In instances where patients do gain access to their health records, their interaction with the data becomes fragmented, mirroring the inherent management structure of these records. [6]

Endorsing a mechanism conducive to sharing and trust, Blockchain emerges as a potential forthcoming resolution for data sharing, potentially facilitating cooperative decision-making in telemedicine and precision medicine. The primary scope of this review lies in a methodical examination of the existing literature, underscoring prior research endeavors related to Electronic Health Records (EHRs) and Blockchain. Within this comprehensive review, we investigate the utilization of a Blockchain framework in the healthcare domain, specifically focusing on the management of EHR storage and access.[6]

Nevertheless, it is crucial to acknowledge that no technology is entirely foolproof, and blockchains remain susceptible to potential attacks or other security breaches. The security of a blockchain is contingent on its implementation and usage. It is imperative to meticulously assess the security protocols in place for any given blockchain and adhere to best practices when engaging with and utilizing it. [7]

To succinctly encapsulate, the present study aims to conduct a comprehensive examination and evaluation of the current literature concerning the integration of Blockchain technology in the healthcare domain. Driven by a scholarly inquiry into plausible solutions for issues surrounding healthcare data, particularly those referring to storage and privacy, our objective is to detect challenges and address unresolved questions.

1.1. Motivation

In the traditional paradigm, cloud-based databases are employed by entities managing content to consolidate Electronic Health Records (EHRs), Electronic Medical Records (EMRs), clinical imagery, Personal Health Records (PHRs), and patient data, including details such as physician identification, physiological measurements, and information from home monitoring devices. It is pertinent to highlight that a centralized database is susceptible to cyber threats, thereby compromising the security and confidentiality of EHRs. [8] Simultaneously, challenges arise for stakeholders and healthcare providers in sharing health-related information due to incongruent standards and formats.

The complexity is exacerbated if a patient's EHR is erased from the hospital's database, resulting in an irreversible loss of the record. Hence, it is imperative for the current system to be resistant to tampering by unauthorized entities to preempt such occurrences. Additionally, a notable challenge presented by contemporary healthcare systems is the lack of complete autonomy for patients over their health records, as these records are managed by service providers [9]. With the escalating volume of

healthcare data, concerns regarding security and scalability have become . Figure 1 [10] provides an overview of the prevailing architectural framework for existing health records.

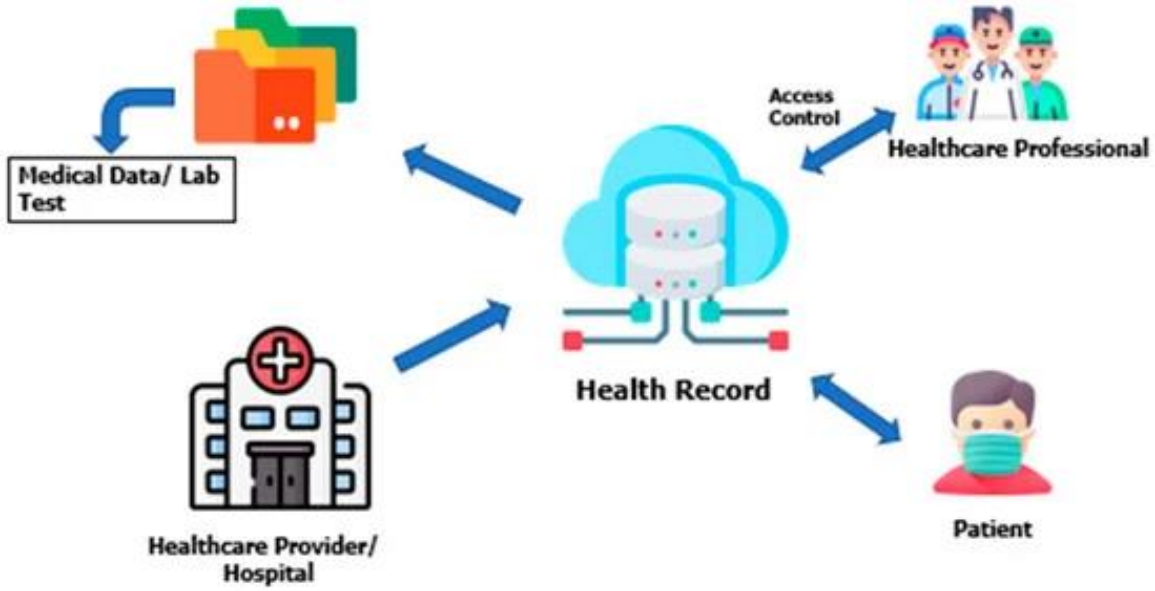


Figure 1. Overview of the current system [10]

As part of the research, several research questions (RQ) have been considered, these including:

1.1.1 What are the use cases of Blockchain in Healthcare?

The fundamental inquiry revolves around comprehending the various domains within healthcare where blockchain has demonstrated utility. Through a thorough examination of pertinent articles from scientific databases, we aim to pinpoint healthcare issues that blockchain can address. This process enables the identification of problems better suited for alternative solutions. Creating a map of blockchain's applicability in healthcare problem domains will assist researchers and practitioners in directing their attention to promising areas within the industry. The results of this question are presented in sections 2.7, 3 and 4 of this review.

1.1.2 Among the recognized use cases, what blockchain-based applications have materialized?

Numerous potential applications of blockchain in healthcare have been proposed in scholarly literature. However, not all these proposals have been translated into functional prototypes. Therefore, it is crucial to discern the extent of real-world implementations of blockchain-based healthcare applications concerning the identified use cases. This assessment will shed light on research gaps and the necessity to redirect focus towards these areas. The results of this question are presented in sections 2.7, 3 and 4 of this review.

1.1.3 What challenges and constraints are associated with blockchain-based applications?

This question aims to reveal the obstacles confronting the implementation of blockchain-based healthcare applications. Drawing insights from prototype applications, we seek to understand the limitations of this emerging technology in achieving its intended objectives in solving healthcare-related issues. The results of this question are presented in section 4 of this review.

1.1.4 How are current approaches addressing these challenges and limitations?

This research query delves into understanding the methodologies employed in the development of blockchain-based healthcare applications. By examining existing projects, we aim to provide guidance for future endeavors, minimizing the need for redundant efforts. Given the evolution of blockchain from its initial implementation in cryptocurrency to its adaptability in non-financial contexts,

this question explores contemporary trends in technical approaches and methodologies for healthcare applications. The results of this question are presented in section 5 and 6 of this review.

1.1.5 What research issues remain open, and what areas deserve future exploration?

The final question focuses on identifying ongoing research gaps and challenges in the field, guiding researchers towards addressing these issues in future endeavors. This strategic assessment enables a targeted approach, streamlining future research efforts to address identified gaps and challenges. The results of this question are presented in section 6 this review.

2. Materials and Methods

In this research, we conducted searches in the Scopus and Google Scholar databases using specific keywords like "Blockchain in healthcare," "healthcare system(s)," "healthcare record(s)", "healthcare and system and record(s)" and "healthcare and blockchain" to identify literature related to blockchain used in healthcare. By confining our inclusion criteria to influential review publications, this paper presents a succinct summary. Notably, we opted to use the term "Healthcare" instead of "Health care" in this study, as the former refers to an industry or system facilitating individual's access to necessary medical care, as supported by previous works. [25][33]

A thorough exploration of electronic repositories was undertaken to locate peer-reviewed articles released between 2018 and January 2024. This research opted for extensively utilized databases within information systems research, which encompass, as stated in Table 1, Google Scholar, Scopus, Web of Science, IEEE Xplore, Emerald, and the Elsevier ScienceDirect. Multiple databases were employed in this study to capitalize on available data and encompass all pertinent literature.

Table 1: Number of Articles retrieved from database.

Database	*Number of Articles*
Scopus	4813
IEEE Xplore	4
Web of Science	2513
Google Scholar	1020
Elsevier ScienceDirect	5304
Emerald	20
Total	13674

Moreover, as part of the inclusion and exclusion criteria, 5 groups of search terms were identified: "Electronic health record, EHR", "HER using blockchain", "EHR: electronic health record security in healthcare", "Interoperability, health information exchange" "Security, implications, challenges in EHR", to retrieve an exhaustive collection of relevant articles to identify literature related to Electronic Health Records (EHR). Table 2 identifies the number of results based on HER blockchain data synthesis.

Table 2: The number of results based on the new search in database for EHR data synthesis

Database	*Number of Articles*
Scopus	51
IEEE Xplore	4
Web of Science	35
Google Scholar	200
Elsevier ScienceDirect	9

Emerald	3
Total	302
Database	Number of Articles
Scopus	51
IEEE Xplore	4
Web of Science	35
Google Scholar	200

2.1 Inclusion and Exclusion Criteria

To ensure the quality and pertinence of the chosen articles, precise criteria for inclusion and exclusion were enforced. Only articles meeting the subsequent requirements were incorporated into this analysis: Written in the English language: Given English's predominant role in scholarly discourse, articles in English were scrutinized for thorough examination, thereby ensuring a comprehensive assessment of blockchain adoption factors. We refer to full-text articles with complete content, encompassing both open-access and subscription-based articles requiring access to academic libraries.
Empirical exploration: Just articles empirically delving into the factors shaping EHR blockchain technology adoption were considered. This criterion aimed at concentrating on studies offering empirical evidence and insights.
Published in reputable journals and conference proceedings: Articles featured in esteemed journals and conference papers were included to encompass a broad spectrum of research outputs.
Articles were excluded if they met any of the subsequent criteria:
Non-English content: Articles not in English were excluded due to linguistic constraints.
Lack of explicit attention to adoption determinants: Articles failing to specifically address factors influencing blockchain adoption in healthcare were omitted to maintain the relevance and focus of this review.

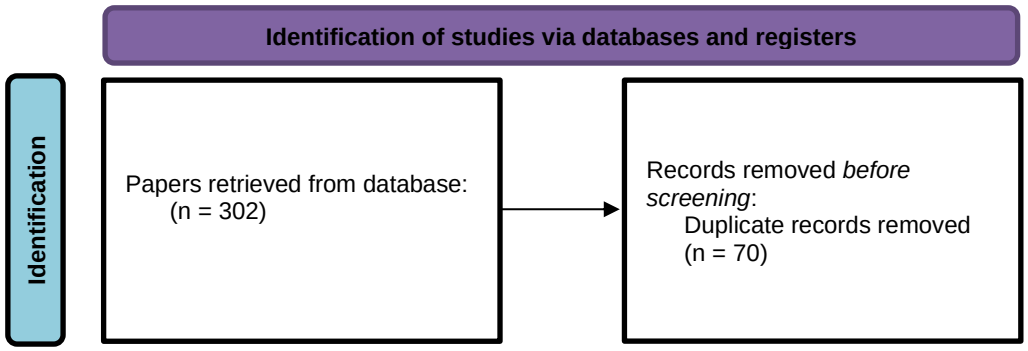
2.2. Screening and Selection

Elimination of precise duplicates was carried out by considering title and author information. Subsequently, a meticulous manual review was conducted to guarantee the absence of any overlooked duplicates. The remaining articles underwent a selection process for a comprehensive review of the full text, adhering to the predefined inclusion and exclusion criteria.

2.3. Data extraction and analysis

Information extraction from the selected articles was conducted to capture essential data, encompassing industry, and key insights concerning blockchain technology adoption in healtcare and the role of EHR and it's security overview in this industry.

To ensure the methodological integrity of our systematic review, we adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. In accordance with the PRISMA guidelines, Figure 2 illustrates the quantity of articles incorporated in this investigation.



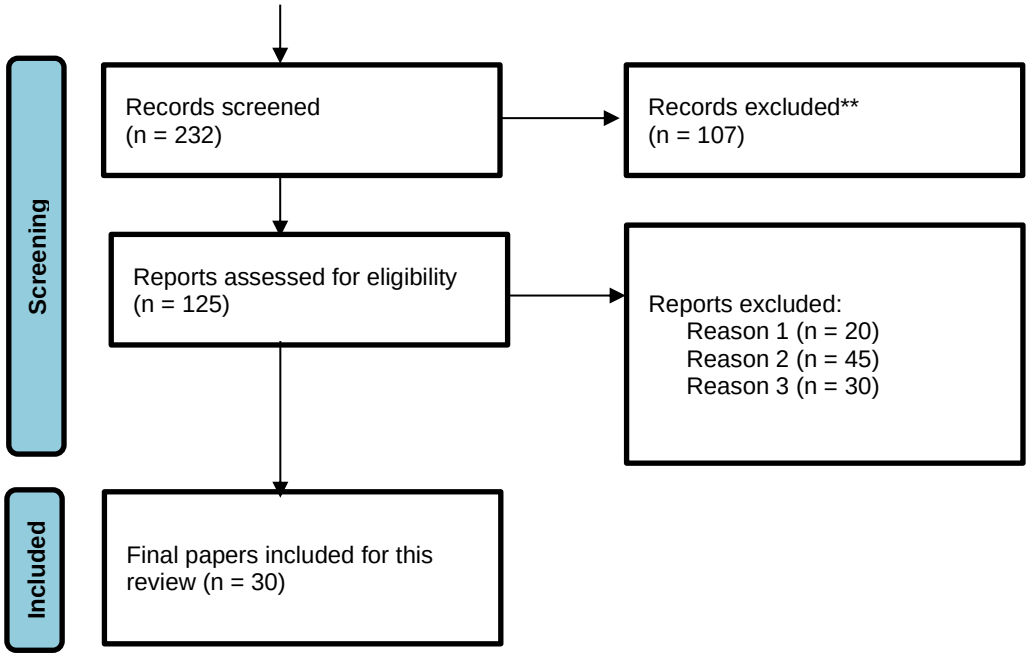


Figure 2: PRISMA flow chart for this study.

As depicted in Figure 2, out of 302 articles initially considered, 30 were ultimately included in this study. This reduction resulted from a meticulous screening and selection process guided by specific inclusion and exclusion criteria. Initially, 70 duplicate papers were eliminated, resulting in 232 unique papers. These papers underwent thorough screening, leading to the exclusion of 107 articles deemed irrelevant or failing to meet the criteria. Subsequently, the remaining 125 papers underwent further screening, with 95 being excluded due to lacking methodological rigor or relevance to the research objectives. For the study inclusion, 30 articles were identified as eligible after data extraction and synthesis, meeing all the criteria.

3. Background and concepts

In 2008, Satoshi Nakamoto introduced Bitcoin, a cryptocurrency built upon the principles outlined in the web white paper [11]. This cryptocurrency operates on open-source technology within a decentralized network, where all nodes are interconnected. These nodes can freely join or leave the network, subsequently receiving authentication through Proof of Work (PoW), also known as the blockchain [11]. Rejoining the network requires nodes to perform substantial computations, providing evidence of their authenticity. PoW serves to describe and validate the events that occurred during a node's absence from the network. To address potential Sybil attacks in cryptocurrency, PoW is employed across all network nodes to verify transactions.

The functionality of PoW is exemplified through the structure of Bitcoin blocks. The network comprises nodes, equivalent to participants, each possessing an identical ledger copy. [12] Transaction details, including sender and receiver information, transaction size, and hash values, are recorded in these blocks. Hash values serve to link the blocks, forming a chain of interconnected blocks, as depicted in Figure 5. The PoW consensus in Bitcoin determines the order in which blocks are linked. The chaining of bitcoins relies on hashing, where altering the hash value invalidates a block, necessitating recalculation for validation. While Bitcoin, as a public blockchain technology, excels in throughput, it

is vulnerable to security and privacy threats, making it unsuitable for healthcare systems where data privacy is crucial. [13].

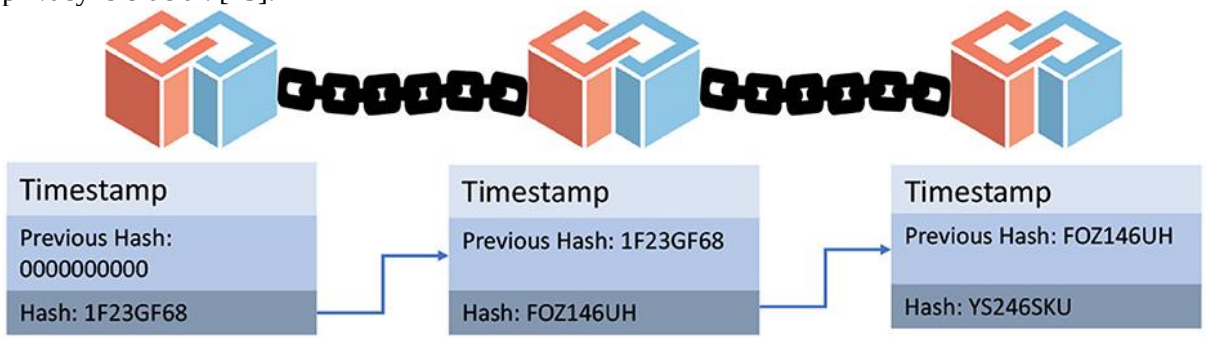


Figure 3. Depiction of blocks within a blockchain involves recording transaction specifics, such as sender and receiver details, transaction size, and hash value. A blockchain consists of a series of interconnected blocks, linked together through hash values. [14]

Blockchain is defined by its decentralized and immutable ledger, recording data and facilitating direct communication between entities without the need for a central, trusted middleman. The data is organized into blocks, forming sets of information that continuously expand. Once incorporated into the blockchain, these blocks are connected to preceding and succeeding blocks through cryptographic methods. All participants have the ability to read, write, and modify these data records or blocks in their original state. This structure enables decentralized transactions and data processing, contributing to the widespread adoption of blockchain for various purposes. Additionally, blockchain supports smart contracts, self-executing agreements that operate without reliance on a central authority. Currently, Ethereum serves as the blockchain platform that facilitates the execution of smart contracts. [13]

3.1. Blockchain Principles

A blockchain is a publicly accessible, decentralized, and distributed database overseen by numerous participants across interconnected nodes via a peer-to-peer (P2P) network. Functioning as a distributed ledger technology (DLT), blockchain allows users to digitally authenticate transactions without relying on a trusted third-party (TTP) authority [15]. Generally, blockchain offers a secure and self-governing consensus mechanism for progressively expanding the DLT while ensuring the immutability and indisputability of the data [16]. The key attributes of blockchain-DLT are illustrated in Figure 4:

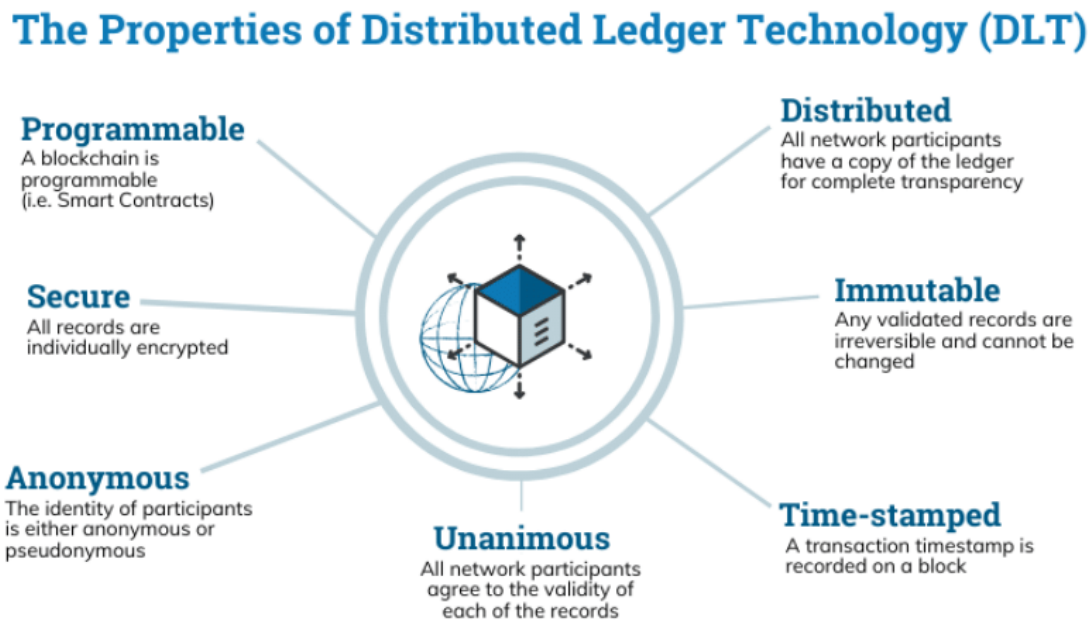


Figure 4: The properties of a distributed ledger technology(DLT) [17]

The extensive node storage in a distributed ledger poses significant difficulties in deleting information once it is added to the blockchain. Moreover, many blockchains leverage the advantageous feature of potential anonymity or pseudonymity. The interconnection of blocks in a blockchain, achieved by including the hash of the preceding block, provides traceability and transparency. The organization of transactions in blocks using a Merkle tree allows for independent verification from the root to each transaction. [18].

3.2. Types of blockchains

Blockchains exist in three primary forms: consortium, public, and private, each with distinct characteristics that determine user permissions for reading, writing, and accessing data. Public chains allow all users access to data, enabling anyone to contribute and modify the consensus and core software. Examples like Bitcoin and Ethereum fall into the public permissionless category. Consortium blockchains may seem somewhat centralized as only selected business groups can observe and participate in the consensus process. Private blockchains, though decentralized in structure, can be frequently perceived as centralized due to a limited number of nodes supervised by a central authority.[18][19][20] The definition and classification of blockchain types remain debatable, with no widespread agreement on defining characteristics and consensus procedures for labeling a technology as a "blockchain".[21] Various blockchain frameworks and platforms, such as Ethereum and Hyperledger, facilitate the development of decentralized applications (Dapps), allowing programmers to add new apps to existing blockchains and create new test nets using their protocols. [22]

3.3. Consensus algorithms

The crucial aspect of blockchain technology involves the process of validating data records on the decentralized ledger. This is achieved through a distributed consensus method that verifies the data entries. Various consensus techniques have been introduced and employed for this purpose, with the three most widely used ones outlined in Table 3 below:

Table 3: Comparison of consensus mechanisms.

Characteristics	PoW	PoS	PBFT
Management of nodes	Accessible	Accessible	Permissioned
Usage of energy	High	Medium	Low

Tolerated an adversary power	<25%	<51%	33.3%faulty
Example	Bitcoin	Ethereum	Hyperledger

Proof of Work (PoW): PoW stands as the consensus system most closely associated with the blockchain, notably in Bitcoin. This process verifies transactions and generates a new block for the blockchain. Miners engage in a competition during this process to be the first to complete the network transaction, receiving incentives for successfully confirming a new block. The significant electricity consumption in Bitcoin mining, currently comparable to that of a small nation, supports this concept. [24]

Proof of Stake (PoS): In PoS, the node chosen as an approving node is based on its stake in the blockchain, with an individual's balance in a particular currency representing their investment in cryptocurrencies. However, concerns arise about the potential for the "richest" node to unfairly benefit. To address this, various hybrid PoS systems have been introduced, where the approving node is selected through a combination of stake and randomization. Ethereum, the second-largest cryptocurrency, plans to transition from Proof of Work to Proof of Stake. [18]

Practical Byzantine Fault Tolerance (PBFT): PBFT relies on a Byzantine agreement mechanism as its underlying protocol. This consensus procedure is not suitable for public blockchains as every node in PBFT must be known to the network, imposing limitations on its application. The PBFT consensus process involves three distinct stages: pre-prepared, prepared, and commit. To progress through these stages, a node must receive two-thirds of the votes from other nodes. Hyperledger Fabric currently employs PBFT. [24] [25]

3.4. Smart contracts

Blockchain infrastructures such as Ethereum enable the functioning of smart contracts. These contracts are self-executing and contain clauses explicitly written into the source code. Smart contracts operate autonomously, devoid of any involvement from third parties or intermediaries, as they are automatically executed according to the predefined clauses. The healthcare industry appears to be a promising application for this feature, as it can be triggered by a blockchain transaction. [20]

3.5. Scalability

Scalability is a recognized challenge in blockchain, prompting a direct exploration of potential solutions [26]. The discussion below outlines the proposed solutions for addressing the scalability concern in blockchain:

3.5.1. Sharding

A widely used on-chain scaling method, sharding is a noteworthy solution to enhance blockchain adaptability. In this layer-1 scaling solution, sharding involves dividing data transactions into smaller, discrete groups, known as shards. These shards are processed concurrently by the network. Sharding allows data to be distributed among multiple nodes, ensuring data consistency. Shards, serving as the main chain's verification, maintain interconnectedness through cross-shard communication rules for exchanging locations, general states, and balances. [27]

3.5.2. Nested Blockchain

Functioning as a decentralized network foundation, nested blockchain utilizes the primary blockchain to establish boundaries for a larger network of secondary blockchains. This approach facilitates transactions through a network of interconnected secondary chains. Nested blockchain is identified as a promising layer-2 configuration to address blockchain scalability concerns. [28]

3.5.3. Consensus Mechanisms

Recognized blockchain entities like Bitcoin employ the Proof of Work consensus model, known for its robust security but relatively slow processing. To tackle scalability issues, many blockchain networks are exploring the Proof-of-Stake (POS) consensus mechanism. Unlike Proof of

Work, POS does not require miners to perform resource-intensive cryptographic computations. Instead, consensus is achieved through the selection of validators, determined by their organizational stakes. The adoption of POS consensus holds potential for enhancing decentralized security and addressing limitations in Ethereum networks. [29]

3.6. Significance of blockchain in healthcare industry

Healthcare is a challenge-driven field that heavily relies on people and data, and the sector's overall functioning hinges on essential aspects such as access to, updating, and trust in the information generated through its operations. [30] A classification of healthcare operations, including accident and emergency, health problem-solving, clinical decision-making, realization, and evaluation of knowledge-based care (Figure 5), underscores the importance of a diverse team of healthcare professionals equipped with the best knowledge, technologies, and skills to effectively treat patients. It is crucial for the healthcare industry to collaborate with educational institutions to provide students with access to patients and a training environment, enabling them to learn and develop their skill sets. In return, educational institutions contribute by supplying the industry with skilled personnel. [30]

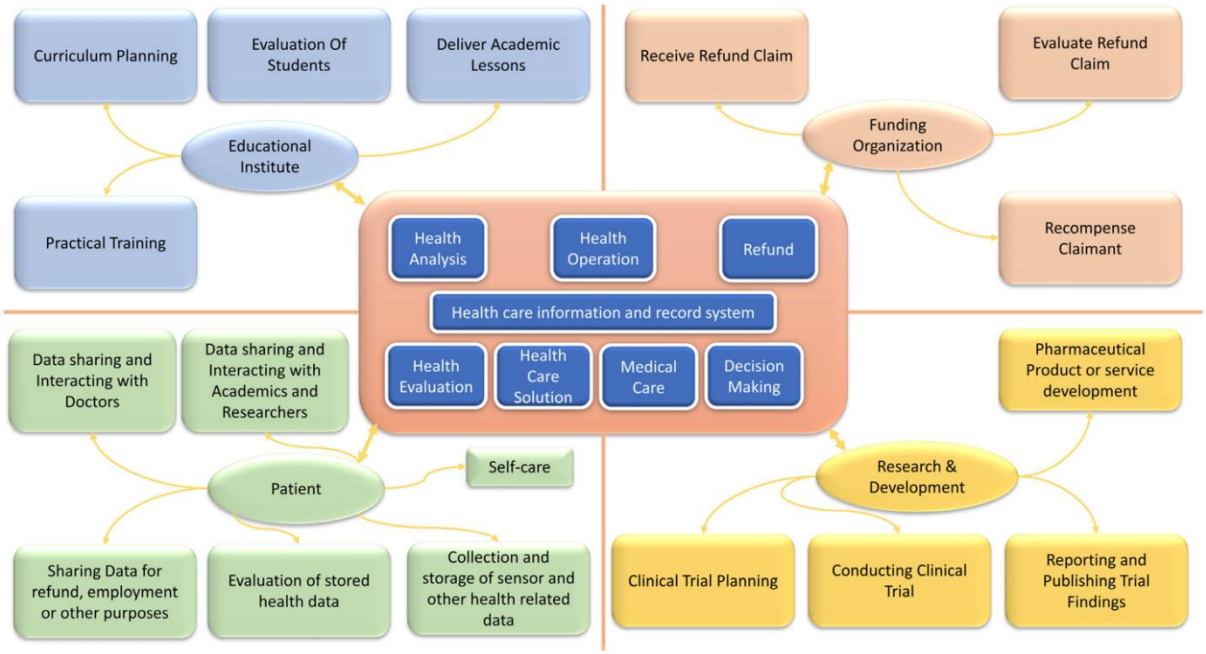


Figure 5: Map of the health sector. [30]

To accomplish this, there is a need for the exchange of consent, patient information, evidence, and handling payment processes, all of which fall under the responsibility of data exchange. It is a mandate for healthcare organizations to safeguard the information shared by patients. [31][32]

The healthcare sector encounters numerous challenges, including issues like data fragmentation, security, privacy concerns, and interoperability complications arising from the diverse standards employed in healthcare systems. Blockchain technology offers a potential solution by ensuring secure and impenetrable data storage through a distributed ledger system, facilitating secure data sharing to enhance interoperability, and protecting patient privacy through data encryption. Various technologies within the realm of blockchain, such as electronic health records (EHRs), health information exchanges (HIEs), and federated learning, address these challenges. However, it's crucial to acknowledge that while blockchain holds great promise, it is not a universal remedy, and the healthcare industry continues to explore various methods and technologies to meet its evolving demands. [31][32]

Collaboration between health institutions, research, and engineering organizations is vital for advancing research and technology. Health institutions play a role in providing access to experts, informants, test subjects, and samples for research purposes. They contribute to the design, planning, execution, and analysis of studies, participating in prospective clinical trials. In return, research and

engineering organizations offer the healthcare industry the latest information, practices, and technology. The operations of health institutions are closely intertwined with those of organizations involved in educating health professionals and conducting biomedical research and engineering. [31][32]

Efficient sharing of patient-related information, evidence, and reimbursement processes necessitates data exchange among different institutions. Protecting sensitive patient data entrusted to healthcare organizations is paramount. Ensuring patient privacy while sharing data within the healthcare network requires measures like access control, data origin preservation, maintaining data integrity, and enabling interoperability. Traditional access control mechanisms assume trust between data owners and the entities holding the data, which often manage access restrictions. To enhance individual and community health through collaborative data access, exchange, and utilization, seamless connectivity is required across various information systems, devices, or applications within and across organizational boundaries. [31][32]

Data provenance, encompasses the origins and historical records of data sources. This can increase transparency and trustworthiness in electronic health records (EHRs), rasing consumer assurance in EHR software. Data integrity, as defined by Courtney and Ware, involves maintaining data quality and meeting expected standards. This implies that adhering to or surpassing these standards directly affects the reliability of data. The need for real-world data from enterprises and research units is on the rise within healthcare institutions. At the same time, public confidence in healthcare organizations is diminishing due to incidents of unlawful data sharing, widely publicized breaches, and theft of private information. Another limitation is the existence of mispractices in the healthcare system that exploit the same level of trust, involving problems like fraudulent medications, deceptive personnel, and patient issues. Given this overall situation, a reevaluation and implementation of alternative strategies are crucial. [31][32].

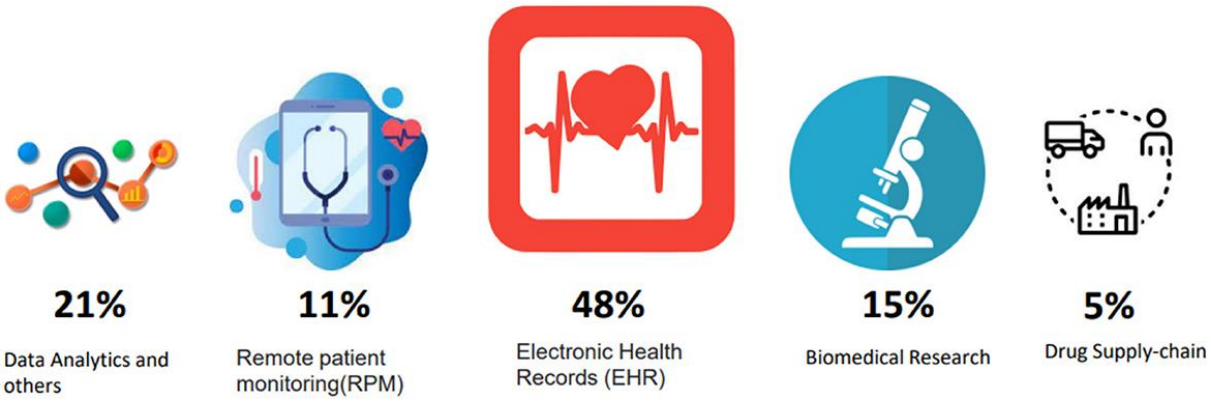


Figure 6. Emerging healthcare blockchain uses cases. [14]

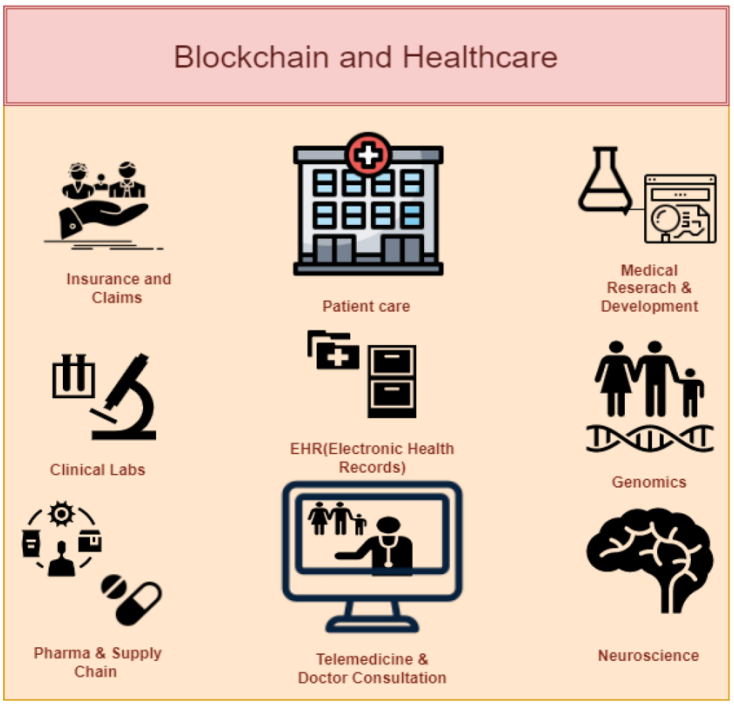


Figure 7. Blockchain adoption in healthcare. [51]

3.7. Applications of blockchain in healthcare

Blockchain technology holds the capacity to elevate the healthcare domain by placing the patient at the forefront of the system and augmenting the protection, integrity, and smooth transmission of health data. Essentially, the healthcare sector stands to undergo a significant metamorphosis with the widespread integration of blockchain, leading to overarching enhancements in safety, integrity, and transparency throughout all facets. Blockchain stands poised to revolutionize processes within this particular industry. It can fulfill a variety of functions, such as managing epidemics effectively and securely encrypting patient information. Ultimately, by facilitating secure data exchange among diverse healthcare systems with patient consent, blockchain has the potential to advance digital health (Figure 6). Figure 7 illustrates the influence of blockchain across different healthcare sectors and its inventive applications. A brief description of innovative BC use cases in healthcare is as presented below [14]:

3.7.1. Insurance and Claims

The utilization of blockchain technology offers potential benefits to health insurance and claims management through its transparency, decentralization, immutability, and auditability of records. Blockchain can be employed for processing claims, potentially enhancing the efficiency and security of the process. This software can securely store encrypted patient identifiers, health data, and provider claims on a blockchain shared by insurers and providers [52]. Nevertheless, there are very few instances of prototype implementations of such systems. A notable example is the MIStore (a medical insurance storage system based on blockchain) which is operational on the Ethereum blockchain platform [54]. Furthermore, [55] discusses a proposal by a company named Pokitdok, which intends to collaborate with Intel to develop a blockchain-driven system designed to make possible insurance claim resolution within the healthcare sector.

3.7.2. Health Data Analytics (HDA)

Blockchain also presents a distinct chance to leverage the capabilities of other emerging technologies like deep learning and transfer learning methodologies to achieve predictive analytics of healthcare data and progress research in the sector of precision medicine. This application of blockchain

is also referenced in [56] and [57], with [58] offering an extensive plan on its potential realization. Juneja and Marefat undertook experimental research wherein blockchain was incorporated into a deep-learning framework for arrhythmia classification.

3.7.3. Patient Care and Clinical Laboratories

Handling patient care and clinical laboratory records within Healthcare Management Systems (HMS) has posed challenges related to security, timeliness, privacy, and data sharing. Blockchain represents a fusion of disruptive technologies that can help address the various challenges inherent in current HMS. The healthcare industry stands to gain efficiency through the adoption and integration of blockchain applications. [53]

3.7.4. Medical Research and Development

Blockchain presents an intriguing application in biomedical research, education, and development. It can help prevent data manipulation and the suppression or omission of unfavorable outcomes in medical research. Blockchain facilitates easier patient authorization for the use of their data for research purposes. Blockchain streamlines the process for patients to authorize the use of their data in clinical trials due to the inherent anonymization encoded within the data [56]. Moreover, the immutability feature of blockchain ensures the integrity of data collected through blockchain for clinical studies. The transparent and publicly accessible nature of blockchain also facilitates the replication of research based on blockchain-derived data. These aspects collectively contribute to the anticipation that blockchain will revolutionize biomedical research. Blockchain has also been recognized for its potential to transform the peer-review process for clinical research publications, leveraging its decentralized, immutable, and transparent properties [57].

Another potential application of blockchain in Health Professions Education (HPE) is outlined in [59], where Funk et al. advocate for the use of blockchain to establish an HPE system characterized by value-based, competency-based principles, and offering credentialing services independently of third-party entities.

Nugent et al. discuss their research in [60], demonstrating how smart contracts on the Ethereum blockchain platform can enhance data transparency in clinical trials. Additionally, the Ethereum platform is utilized to deploy another blockchain-based solution proposed for notarizing documents extracted from biomedical databases.

3.7.5. Pharmaceuticals and Supply Chain

Another established application of blockchain technology is in pharmaceutical and supply chain management, particularly within the medication/drug sector. The distribution of counterfeit or inadequate medications can have severe consequences for patients. Faking poses a significant challenge in the pharmaceutical industry, but blockchain technology has been identified as having the potential to address this issue [61].

In his survey, Engelhardt highlights several companies exploring the utilization of blockchain technology to combat prescription drug fraud, including Nuco, HealthChainRx, and Scalamed [55]. The main concept involves recording every prescription drug-related transaction on a blockchain network, connecting all stakeholders such as manufacturers, distributors, doctors, patients, and pharmacists. This approach allows for the detection of any tampering or malicious alterations to prescriptions by any party involved.

Among the reviewed papers, only one presents an example implementation of a blockchain-based application for pharmaceutical supply chain management. Modum.io AG, a startup, employs blockchain to ensure data immutability while enabling public access to temperature records of pharmaceutical products during transportation. This facilitates verification of their compliance with quality control temperature requirements [62].

3.7.6. Neuroscience

Blockchain technology has been integrated into various neuroscience applications, including brain augmentation, brain simulation, and brain mapping. Digitizing and storing all brain-related data

necessitates a secure platform for data storage. The reliability and blockchain technology aid in the secure and precise storage of brain data [63].

3.7.7. Telemedicine and Doctor Consultation

Telemedicine holds significant promise for delivering real-time healthcare. However, the current telemedicine infrastructure faces challenges related to security, privacy, and interoperability, which hinder its suitability for widespread use in healthcare. Blockchain-based telemedicine systems have the potential to mitigate these challenges and could prove to be more efficient. [34]

3.7.8. Genomics

Human genomic projects are generating vast amounts of genomic data extensively utilized in biotechnology and clinical research. Consequently, there is a need for tools and technologies to process and analyze genomic data efficiently. Blockchain technology has emerged as a contemporary solution for securely storing and exchanging genomic data. The primary goal is to facilitate secure data exchange through privacy-preserving algorithms, simplifying compliance with ethical and legal obligations for both organizations and individuals. While many of these platforms are still in early stages of development, they offer promising solutions to governance issues related to genetic data sharing. Blockchain goes beyond being just a technological framework; it introduces a novel approach to managing open networks, leveraging decentralization, market dynamics, and consumer genetics. Blockchain solutions have the potential to automate data access control processes, enhancing transparency and availability of genetic data. The integration of smart contracts could further strengthen the enforcement of access agreements, drilling confidence among researchers and data owners that data usage will comply with specified terms and conditions.

Moreover, successful implementation of blockchain-driven solutions could reshape cultural norms surrounding data sharing, reducing the dominance of public and commercial genetic test providers in controlling the dissemination of genetic information. This shift would empower patients and individuals to play a more significant role in the data-sharing landscape. Blockchain technology can establish new shared resources that bridge the gap between market-driven dynamics and public resources. However, achieving this transformation requires substantial efforts in education, incentive design, ownership structure, and collaborative governance. The goal of blockchain-based platforms is to empower patients and citizens to have control over their data and participate in data sharing. Nevertheless, it is important to recognize that legal frameworks remain essential for the success of blockchain-based solutions. [65]

3.7.9. Remote Patient Monitoring (RPM)

In this section, we explore how blockchain technology facilitates remote patient monitoring (RPM), which entails gathering biomedical data through body area sensors (or IoT devices) and mobile devices to supervise patient status outside traditional healthcare surroundings like hospitals. Blockchain has been suggested as a solution for storing, sharing, and accessing remotely collected biomedical data [66].

In [67], Griggs et al. illustrate how smart contracts on the Ethereum blockchain platform can enable real-time patient monitoring applications, allowing for automated interventions in a secure environment. Liang et al. [68] introduce a Hyperledger-based implementation of blockchain-enabled data collection and sharing among healthcare stakeholders in a mobile healthcare setting. Similarly, blockchain technology is utilized to create SMEAD, a mobile-assisted device for monitoring diabetes patients. Another application example is outlined in [69], where mobile devices (smartphones) successfully transmit data to a blockchain-based application on Hyperledger Fabric. Ashraf Uddin et al. [70] have also devised a blockchain-based patient-centric agent (PCA) to ensure end-to-end data security and privacy in continuous remote patient monitoring applications. In [71], the authors propose utilizing practical swarm optimization (PSO) for root exploit detection and feature optimization in blockchain-based mobile device medical data management. Finally, Ji et al. propose BMPLS (Blockchain-based Multi-level Privacy-preserving Location Sharing), a scheme designed to achieve privacy-preserving location sharing in remote monitoring applications.

3.7.10. Electronic Medical Records (EMRs)

The predominant application of blockchain in healthcare revolves around the management of Electronic Health Records (EHR) or Electronic Medical Records (EMR), aimed at enhancing data security and reliability. This section initiates with a concise review of current literature pertaining to the utilization of Electronic Health Records (EHR) and blockchain technology. [77]

Prior to blockchain innovation, a significant constraint in EHR was the fragmentation of patients' information across various healthcare providers, with past data often inaccessible even within EHR systems [77]. Blockchain technology is widely regarded by researchers as a novel solution for storing patients' EHRs, ensuring the security of current data for an indefinite period and enabling retrieval at any time. Several prototypes based on blockchain have been developed by various companies, including MedRec, FHIRChain, MedBlock, MedShare, and others. In recent years, several prototypes of blockchain-based Healthcare Management Systems (HMS) have emerged. Table 4 provides a summary of the key application features of popular blockchain-based HMS:

Table 4: Summary of popular blockchain-based Healthcare Management Systems (HMS)

Blockchain-Based HMS	Summarized Application Features
MedRec [34]	MedRec, a collaborative effort between MIT Media Lab and Beth Israel Deaconess Medical Center, operates on the Ethereum blockchain platform. Its primary objective is to empower patients by granting them control over their information. This control extends to determining who has access to their data through finely-tailored access permissions managed on the blockchain.
Medicalchain [72]	Medicalchain has been created with a dual blockchain architecture. The initial blockchain manages access to health records and was constructed using Hyperledger Fabric. The second blockchain, built on Ethereum, utilizes the ERC20 token to govern platform administrators.
Ancile [73]	A blockchain-based framework built on the Ethereum blockchain leverages smart contracts to ensure efficient and secure access control, as well as non-repudiation of data. Enhanced cryptographic techniques are also employed to provide additional layers of security.
DPS [74]	A data preservation system built on Ethereum offers reliable data storage, ensuring the integrity of information while prioritizing security for critical healthcare data.
MedBlock [43]	MedBlock, utilizing a distributed ledger and a two-layer architecture featuring a block structure based on Merkle-Tree, enabled efficient access to Electronic Medical Records (EMRs) and facilitated EMR recovery [79]. The hybrid consensus system ensured EMR agreement without significant energy consumption or network congestion.
MedShare [75]	MedShare, designed to address the challenge of sharing large volumes of health data among big data stakeholders, offered data provenance, analysis, and control for shared health information in a cloud-based environment.
FHIRChain [76]	Another system was developed to meet the requirements of the Office of the National Coordinator for Health Information Technology (ONC) by embodying the HL7 Fast Healthcare Interoperability Resources (FHIR) standard for shared medical information. A decentralized application was created based on digital medical identity for remote cancer care.

Azaria et al. (2016) [34] introduced a framework known as MedRec, which employs blockchain for decentralizing health records. The proposed approach involves a public blockchain category that prompts researchers to mine new blocks in exchange for access to anonymized clinical data. The authors asserted that their architecture enhances the simplicity, security, and privacy of

healthcare records. Building upon the MedRec framework, Nchinda et al. (2019) extended its application by utilizing blockchain for the storage of consent contracts. In their research, providers could join the network, enabling them to grant access to their databases to patients and other entities using their credentials. [25]

Mikula and Jacobsen (2018) employed a unified blockchain with permissioned access to examine auditability. Their evaluation of the system indicated that the time required for mining to add a new block to the blockchain was approximately 2-3 minutes, with a block size of about 3.8 MB. In contrast, Haque et al. (2020) utilized two distinct blockchains to ensure security and data protection: one for storing solely EHRs and another for storing EHR solid files. Additionally, Haque et al. (2020) employed a secure hashing algorithm known as SHA-256 hash algorithm to generate a unique and irretrievable 256-bit or 32-byte hash for a specific medical record. Since there is no trusted central authority to oversee in a public blockchain-based approach, reaching consensus among untrusted nodes presents a significant challenge. Raikwar et al. (2019) offered an encryption strategy for sharing patient health records among interconnected networks, along with utilizing smart contracts to regulate access control and ensure interoperability among hospitals. [36] [37] [38]

Zhang et al. (2021) introduced a blockchain-based framework and executed Practical Byzantine Fault Tolerance (PBFT), a consensus mechanism facilitating information exchange among patients and researchers. In contrast to previous methods, PBFT requires less computational power and is adaptable to numerous other blockchain-based applications. The authors advocated for a consensus algorithm named Proof of Authenticity across the network, expecting clinics and healthcare centers to act as both miners and validators in adding blocks to the distributed ledger. The adoption of blockchain for managing healthcare data is a crucial area of study. While storing entire Electronic Health Records (EHRs) directly in the blockchain architecture amplifies computational load and capacity, various investigations and applications have opted for a hybrid storage design to address these challenges. This approach entails off-chain storage, where only reference data is stored on the blockchain, while the actual data is stored using an Interplanetary File System (IPFS), as proposed by Pilares et al. (2022). [39] [40]

Zhang et al. [41] explored the integration of blockchain technology into healthcare systems through various health-related scenarios, emphasizing a patient-centered approach to secure data exchange. They advocated for blockchain adoption across seven distinct domains, including clinical documentation, patient-managed cancer information, telemedicine services, patient authentication, and resolution of health insurance disputes. The authors directed their attention towards patients' health data to illustrate the relevance of blockchain in information sharing behaviors. Despite highlighting the advantages of employing blockchain in managing health records, there is limited existing literature providing a groundwork for its implementation in patient health data management. Homans et al. [42] developed a blockchain-based management information system for electronic health records to address concerns regarding security and privacy. They proposed a framework comprising six components: ledger, database, committer, "orderer," endorser, and client. Fan et al. did not delve into the concepts of privacy labor and digital currency, leaving them for future exploration. [41] [42]

Griggs et al., along with Fan et al. [43], expanded upon the research conducted by Fan et al., incorporating insights from Homans [42], by presenting a private blockchain to tackle privacy concerns associated with blockchain utilization. There are two types of blocks: public and private, each representing a comprehensive record of all completed and pending transactions. According to Griggs et al., employing a private blockchain could be a viable solution in healthcare management, particularly due to the significant security risks surrounding personal data. Privacy issues in EHR systems might lead to decreased rates of participation.

The study introduces the "PeNLP Parser," a tool developed to extract and visualize precise geographical information pertaining to maternal, neonatal, and pediatric healthcare from unstructured data. Utilizing Natural Language Processing (NLP) techniques, this application retrieves relevant data and geolocations from unstructured sources. By employing the PeNLP Parser, healthcare providers and researchers can efficiently access and visualize crucial geographic data, thereby enhancing their ability to make informed decisions and enhance maternal and child healthcare services. [44]

Patience et al. present an integrated ontology aimed at aiding decision-making in the Maternal, Newborn, and Child Health (MNCH) sector. Context awareness is a key feature of this ontology, allowing it to consider various situational factors when providing decision support. By leveraging this integrated ontology, which effectively analyzes and comprehends data pertinent to maternal, newborn, and child health, the study seeks to offer insightful analysis and recommendations to healthcare professionals and policymakers, thereby improving decision-making processes in MNCH. [45]

Sharma et al. [46] utilized soft systems methodology to provide qualitative evidence demonstrating that utilizing Electronic Health Records (EHRs) in conjunction with blockchain technology can enhance patient engagement and opt-in rates. They focused on the Primary Health Care (PHC) strategy, which comprises several individual EHRs intended for universal access to advance the healthcare system. They illustrated how their proposed blockchain-based approach could enhance patient and physician trust in medical record sharing, while also bolstering security and privacy in trustless PHC platforms.

Esmaeilzadeh et al. [47] considered the potential impacts of blockchain on Health Information Exchange (HIE), revealing that consumers are actively seeking comprehensive blockchain-based privacy protection mechanisms. Shahnaz et al. [48] presented a framework aimed at mitigating scalability issues in blockchain utilization to facilitate its adoption in Electronic Health Records (EHR) management. Blockchain-based healthcare systems present both advantages and disadvantages for patients and healthcare professionals, thereby offering new avenues for research. [49]

While blockchain technology's application in healthcare administration has been the subject of numerous studies, its precise role in healthcare systems remains unclear. To the best of the authors' knowledge, this study is the first to systematically examine the relationship between patients' willingness to share medical information and blockchain technology, with mediating effects. Additionally, the conceptual understanding of the role of external incentives and security/privacy in healthcare practitioner information systems is still lacking. [50]

4. Electronic Healthcare Records

In this section, we delve into how blockchain technology facilitates the management of electronic medical records (EMRs) in healthcare. EMRs, which are sometimes referred to interchangeably as electronic health records (EHRs) or personal health records (PHRs), involve the electronic creation, storage, and organization of patients' personal, medical, or health-related data. Indeed, the use of blockchain for EMRs is a significant focus in the literature, with 48%[14] of the 30 selected papers addressing this topic. The features of blockchain, including decentralization, immutability, data provenance, reliability, robustness, smart contracts, security, and privacy, are touted as being highly suitable for the storage and management of patients' EMRs [14][55].

Several papers focus on facilitating patient-centric data sharing among various healthcare stakeholders, aligning with regulations like the European General Data Protection Regulation (GDPR) that mandate explicit patient consent for processing sensitive personal data. Blockchain is widely seen as a viable technology for building healthcare platforms that empower patients to control the sharing, processing, or usage of their data [14][15][55].

Examples of blockchain-based EMR management include Guardtime, which secures over 1 million patient records in Estonia using blockchain [15]. The MedRec project by MIT Media Lab and Beth Israel Deaconess Medical Center empowers patients to control access to their data through fine-grained permissions on blockchain [34]. The Gem Health Network (GHN) by US startup Gem enables shared access to data among healthcare practitioners [34], while Healthbank, a Swiss digital health company, empowers patients to control their data using blockchain [34]. Additionally, the Medicalchain project aims to facilitate the sharing of patients' medical records across international healthcare institutions. [55]

Various initiatives and projects, including Factom, HealthCombix, Patientory, SimplyVital, IBM's Watson, BurstIQ, Bowhead, QBRICS, and Nuco, are also leveraging blockchain for patient-centric EMRs. [55]

Barriers to blockchain-enabled patient-centric EMRs include interoperability among disparate solutions, scalability issues due to the high volume of clinical data, patient engagement challenges, data security, privacy concerns, and lack of incentives [55]. Proposed solutions to address these challenges include storing healthcare data on the cloud and using blockchain for storing pointers and fingerprints. [75]

Several technical papers report on the implementation of blockchain-based EMR applications, with different approaches adopted to tackle these challenges. Some propose solutions to enhance the security and privacy of EMR data on blockchain.

For instance, HealthChain is an EMR application developed using the IBM Blockchain's Hyperledger Fabric, ensuring data confidentiality, scalability, and security. [16] Ancile, built on the Ethereum blockchain platform, employs smart contracts for access control, data security, privacy, and interoperability of EMRs. [73] MedRec and the medical data preservation system (DPS) by Li et al. are examples of EMR implementations on the Ethereum blockchain platform [74]. Other blockchain-based EMR applications include MedBlock, BlockHIE, FHIRChain, and MeDShare. [43][75][76]

Addressing privacy concerns, schemes using private and consortium blockchains, asymmetric encryption, and cryptographic functions are proposed to secure and preserve EMRs. Architectures like Healthcare Data Gateway (HDG) and MediBchain enable patients to own, control, and share their data in a privacy-preserving manner. [78][79]

4.1. Challenges and Constraints of Blockchain-Based Electronic Health Record (EHR) Systems

This section outlines several technical challenges associated with blockchain technology, including throughput, latency, scalability, privacy and security, interoperability, and usability.

4.1.1. Throughput

As the number of transactions and participating nodes in a network increases, additional checks are required, resulting in network congestion. Therefore, throughput is a crucial factor to consider when operating within healthcare ecosystems. Accelerated access to essential diagnoses could potentially save lives.

4.1.2. Latency

The duration required to validate a block in a blockchain varies depending on the consensus mechanism and blockchain architecture. Given the dynamic nature of healthcare systems, information should be accessed within a timely manner.

4.1.3. Scalability

This is a significant concern, particularly in relation to the vast amount of data involved in healthcare systems. Storing high-volume biomedical information directly on the blockchain could lead to performance degradation and increased latency. [80]

4.1.4. Interoperability

This refers to the ability to exchange information between different entities. Applications developed by various vendors or on different framework platforms may face challenges in interoperability. For example, exchanging data between healthcare systems developed on Ethereum and Hyperledger Fabric platforms can be problematic. [81][29]

4.1.5. Privacy and Security

Blockchain-based healthcare systems raise concerns regarding data privacy. Despite employing encryption techniques, there are fears that personal information could still be identified on a public blockchain. Additionally, the use of blockchain keys for data encryption is vulnerable to unauthorized access. Immutability, a key feature of blockchain, conflicts with the European Union's General Data Protection Regulation (GDPR), specifically the "right to be forgotten." Since data stored on a blockchain cannot be erased or modified, fulfilling requests for complete deletion of a patient's clinical history becomes challenging. [29]

4.1.6. Usability

This concerns facilitating patients' management of their own information on the blockchain. However, patients of varying ages may not be willing or equipped to participate in managing their EHR. Several potential solutions to these limitations have been proposed. For instance, to address scalability issues, an "off-chain" storage approach can be implemented, where only references to information are stored on the blockchain, while the actual data are encrypted and stored using the Interplanetary File System (IPFS). This approach also resolves GDPR's "right to be forgotten" concern, as the original data stored on IPFS can be permanently erased. Additionally, the use of permissioned blockchains, such as private or consortium blockchains, and smart contracts can establish and modify standards for managing the storage and accessibility of patient data. [40]

5. Blockchain-Based Solutions in Existing Healthcare Systems

In this section, we explore the solutions proposed in prior studies to tackle various technological obstacles. Confidentiality, privacy, scalability, legitimacy, authenticity, trustworthiness, non-repudiation, traceability, and auditability represent the present array of pertinent security aims in healthcare systems that need attention. Previous research endeavors have aimed to tackle these security considerations comprehensively, while others have concentrated on specific aspects of the security needs within medical data systems.

5.1. Proposed Solutions for the Safety of Medical Data

Previous studies have proposed that overlaying blockchain layers onto a conventional system can enhance the security efficacy of existing medical systems when paired with cryptographic methods. Leveraging the foundational aspects of blockchain, research endeavors [82] transformed the centralized structure of EHR network communication among healthcare providers into a decentralized network, thereby offering numerous benefits and addressing security issues. The decentralized EHR network has minimized reliance on third parties, enhancing infrastructure for health management systems, personal information storage management, advanced data access management, and ensuring safety and confidentiality. Researchers in [83] have introduced a novel cryptosystem integrating existing cryptosystems' attributes, such as attribute-based encryption (ABE) and identity-based encryption (IBE), alongside blockchain technology to ensure secrecy, authentication, and integrity of medical information while enabling complete access control to cloud-backed medical data. In studies [84][85][86], the consent mechanism in blockchain was optimized, wherein the consensus algorithm governs access, storage, and distribution of medical data within an EHR network. The EHR system is vested with authority over decisions requiring approval from all network participants, thereby instilling a high level of certainty before allowing data modifications.

This functionality introduces an additional layer of certainty to the healthcare information repository network, rendering it less susceptible to single point of failure attacks and deterring ransomware and denial-of-service attacks. Researchers in [87] enhanced security elements and reduced complexity in the existing EHR system by incorporating a cipher controller into the blockchain and employing encryption techniques prior to the transmission or reception of network data. Each patient possesses a unique identity and identifier within the blockchain system, preventing unauthorized data usage and ensuring robust data protection. In [88], security and scalability limitations in the existing Health Information Exchange (HIE) system were addressed by adopting a novel integrated ACP and consortium blockchain to enhance diagnostic accuracy and treatment efficacy. Furthermore,

homomorphic encryption, as proposed by Qu [89], presents another avenue for tackling the privacy concerns surrounding patient data within a blockchain framework. This approach involves leveraging homomorphic encryption to store data on a blockchain without fundamentally altering the blockchain's properties. It provides privacy protection and facilitates computation over encrypted data without disclosing the actual data. The Ethereum platform can serve as a suitable environment for developing blockchain-based applications aimed at improving privacy and control over patient data, given its support for homomorphic encryption for data stored within the blockchain.

Authors of [90] proposed a PCA (Principal Component Analysis) blockchain end-to-end architecture to tackle IoT RPMS (Remote Patient Monitoring System) security challenges posed by generating vast volumes of data streams while safeguarding patient anonymity. The privacy and security implications of data transmission and transaction recording over IoT-RPMS were examined by the authors of [91]. The updated architecture for IoT devices incorporates blockchain distribution benefits and various other network security and privacy features to ensure secure transmission and analysis of massive data volumes in RPM. The FHIR safety criterion is utilized in [92] and introduces an IoT RPM Chain Model FHR, combining blockchain's distribution characteristics to enhance patient privacy and security through collaborative healthcare decision-making. In [93], it was concluded that deploying smart contracts in the blockchain network benefited users by eliminating third parties and leveraging additional self-executing, immutable, self-verifying, and auto-enforcing features for managing device-generated data in IoT-RHS (Resource Host Monitor). To mitigate security concerns like DDoS, data breaches, hacking, and clinical remoteness, these components are interconnected and synchronized across a distributed network of IoT devices owned and managed by various organizations.

5.2. Proposed Solutions for Resolving Privacy Issues with Medical Data

Considerable efforts have been dedicated to enhancing the privacy of medical data for both patients and healthcare providers by integrating cryptographic approaches into decentralized EHR networks or other healthcare applications. Researchers in [94] sought to develop an effective technique based on Elliptic Curve Cryptography (ECC) atop existing blockchain-based EHR systems to ensure data accessibility and preserve privacy within the network.

Additionally, [95] demonstrated the use of Ciphertext Policy Attribute-Based Encryption (CP-ABE) in securing data-sharing privacy within a cloud-based EHR system. This approach provides robust data confidentiality and enables data owners to exchange encrypted data with authorized storage users while maintaining the access control system. In [74], is tackled the issue of storing patients' medical information in a database by ensuring its tamper-proof nature through the utilization of Ethereum blockchain features A Data Preservation System (DPS), functioning as a peer-to-peer network database, employs proof of primitivity as a consensus mechanism to permanently preserve data on the blockchain. However, every patient's severely restricted access to EHRs through the blockchain system poses challenges in exchanging such information with service providers or researchers. These challenges were addressed by researchers in [96] through the introduction of an Attribute-Based Signcryption (ABS)-based system with multiple authorities in decentralized EHRs based on blockchain, ensuring patient confidentiality and interoperability.

Moreover, [97] established double privacy preservation capabilities in decentralized EHRs across various healthcare providers using ABS for blockchain healthcare applications. Internal blockchain features have yielded numerous advantages for EHRs. However, transparency features may compromise the privacy and confidentiality of Personal Health Records (PHRs). To address this, methods such as the proxy re-encryption method were modeled atop blockchain applications, distributing the re-encryption task among several nodes to enhance privacy while maintaining data integrity within the blockchain.

5.3. Proposed Solutions for Problems with Medical Data Integrity

The authors of [98] proposed a system to address the challenge of maintaining medical data confidentiality and integrity within a centralized local database by transitioning it into a decentralized database. Leveraging the unique characteristics of blockchain technology, this approach enhances

security, anonymity, and reliability. Additionally, this system generates a hashed copy of stored medical data to ensure data integrity. Subsequently, copies of the data can be distributed to organizations, such as medical research institutions, to maintain integrity while mitigating the risk of a database administrator with malicious intent. Consequently, when entities request access to patient medical data, smart contracts automatically execute the process. By storing medical information in a decentralized database, implementing an authentication mechanism, and encrypting patient records with a symmetric key,it was achieved authenticity, scalability, and security in managing medical data. The integrity of medical data was validated by genuine participants, with data stored on a Hyperledger Fabric blockchain, preventing attackers from altering or deleting data. [98]

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

The authors of [99] tackled the challenge of centralized authentication by establishing a secure, decentralized authentication provider to safeguard the system against specific security attacks encountered during the transfer of patient data between providers. Their proposed solution addresses authentication and authorization issues present in current EHR healthcare systems, particularly those related to the exchange of sensitive information among multiple healthcare service providers.

Interestingly, blockchain could serve as a means of authentication. In [100], a suggestion was made to utilize IoT-RPM for authenticating and securely communicating with stored devices created by healthcare systems through a blockchain-based mechanism. By implementing a blockchain system, users' identities and authorization could be protected against potential threats, as information cannot be physically removed.

5.5. Proposed Solutions to Interoperability Issues with Medical Data

In [101], the integration of AI with the EHR blockchain was proposed to bolster the secrecy, security, and interactivity of medical data. This solution aims to address the challenges faced by the medical system regarding interoperability and the exchange of medical data among different healthcare service providers. Leveraging blockchain transactions facilitates collaboration among numerous EHR stakeholders while preventing data fragmentation. Within the context of an unreliable cloud platform, Ref. [94] utilized blockchain attributes to tackle the issue of compromised patient confidentiality during the interoperable exchange of medical data among providers of medical big data. Through the regulation of data distribution and synchronization across various EHR providers by the consensus mechanism, blockchain usage ensures efficient data exchange and minimizes errors. In [76], the challenge of secure, protected, and accessible communal clinical decision-making in data sharing was addressed by integrating the Fast Healthcare Interoperability Resources (FHIR) of the HL7 standard with blockchain. This fusion improved information sharing and led to more informed treatment decisions.

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

To tackle the issue of compromised patient confidentiality in the interoperability of medical data exchange among healthcare providers, blockchain technology was employed by the authors of [75]. In [102], researchers introduced a novel blockchain-based framework called the Healthcare Data Gateway (HDG), aiming to efficiently and securely manage the exchange of patient data while upholding patient privacy. This architectural development resolves challenges within healthcare systems related to the aggregation, storage, and analysis of personal healthcare data without compromising privacy, ensuring that data ownership and control reside with the patient rather than being distributed across various healthcare providers. In [103], the authors proposed the OmniPHR blockchain-based architecture to integrate Personal Health Records (PHRs) between patients and healthcare providers, addressing issues related to scattered patient data records, thereby facilitating the management and retrieval of up-to-date and duplicate-free data.

In [75], blockchain technology was employed to tackle the issue of compromised patient privacy and security during the sharing of medical data among healthcare providers. Meanwhile, [71] introduced a unique blockchain-based framework called the Healthcare Data Gateway (HDG) to securely store and

exchange medical data while upholding patient confidentiality. This architectural innovation addresses the complexity of gathering, preserving, and analyzing private health data without compromising confidentiality, ensuring that patients retain ownership and control of their information rather than having it dispersed among numerous healthcare service providers.

6. Discussion

We use this section to cross-examine the remaining research questions that were not discussed by this research such as addressing these challenges, limitations and remaining open issues. This literature review effectively identified both objective and subjective aspects of research aimed at comprehensively understanding the ecosystem surrounding EHRs in blockchain technology. By addressing research inquiries, it uncovered several common study elements, including challenges, unresolved issues, types of available information, relevant principles, objectives, designs, and functionalities concerning EHRs and blockchains. The key findings highlighted in this survey underscore the importance of achieving EHR interoperability through blockchain adoption by healthcare providers and the value of open standards. Moreover, various blockchain solutions prioritize addressing storage challenges, such as enhancing patient control over sensitive health information. Given the sharing, accessibility, and integration of health data, these aspects could be crucial for improving healthcare administration. Subsequently, we delved into several privacy-preserving strategies related to EHRs. While these strategies offer data security, research must consider factors like storage capacity and performance. The throughput of blockchain processes is influenced by various procedures related to data retrieval, encryption/decryption, and compliance checks, in addition to privacy mechanisms. We compiled findings on different privacy-preserving approaches for EHRs and assessed their efficacy. Although data access times and storage costs may be relatively high compared to other methods, considering factors like data privacy, security, integrity, and interoperability, blockchain adoption could offer significant advantages for healthcare systems. [17]

6.1. What Are the Challenges and Limitations of the Blockchain-Based Applications?

Several challenges have been identified in the development of blockchain-based applications, including interoperability, security, privacy, scalability, speed, and patient engagement. Interoperability poses a challenge due to the lack of a standardized approach in developing blockchain-based healthcare applications. Applications developed on different platforms or by various vendors may struggle to communicate with each other, as seen in the example of two remote patient monitoring applications, one on the Ethereum platform and the other on Hyperledger Fabric. [68]

Security and privacy concerns arise despite encryption measures, as patient identities could potentially be revealed in public blockchains through data linkage. Additionally, malicious attacks from criminal organizations or government agencies could compromise patient privacy. Moreover, the immutability feature of blockchain poses a challenge regarding compliance with the GDPR's "right to be forgotten." According to this regulation, users have the right to request the complete erasure of their data. However, blockchain's immutability ensures that once data is stored, it cannot be deleted or altered. This presents a dilemma when attempting to completely erase a patient's medical history. [14][15][55]

Scalability is another significant challenge in blockchain-based healthcare solutions, particularly concerning the sheer volume of data involved. Storing extensive biomedical data on the blockchain can lead to severe performance degradation and may not be feasible in certain situations. Additionally, speed issues arise due to the inherent latency introduced by blockchain-based processing. For instance, the validation process in the Ethereum blockchain platform requires participation from all network nodes, resulting in considerable processing delays, especially under heavy data loads. [26] [28]

Engaging patients in managing their data on the blockchain presents yet another challenge. Many patients, particularly the elderly and young individuals, may lack interest or the necessary skills to participate in the management of their health data. This lack of engagement complicates efforts to ensure patient involvement and ownership of their healthcare information. [51]

6.2. How are current approaches addressing these challenges and limitations?

Various strategies are being proposed to address the challenges and constraints associated with implementing blockchain in health IT systems. For instance, in response to scalability issues, a solution involves storing encrypted health data "off-chain," where only condensed information about the data and access instructions are stored on the blockchain. This approach also resolves the GDPR's "right to be forgotten" concern, as the actual health data stored off-chain can be permanently erased, while retaining the blockchain pointer to the data. However, this workaround comes with limitations, such as partial loss of the redundancy built into blockchain, which enhances data availability. [75]

To boost data security and safeguard patient privacy, permissioned blockchains like private or consortium blockchains are favored over permissionless, public blockchains for healthcare applications. Additionally, rigorous software development processes and comprehensive security measures during code development can help mitigate security threats. In permissioned healthcare blockchains, mechanisms are implemented to reverse fraudulent or invalid transactions. Smart contracts based on blockchain technology enable the definition and programming of rules governing how healthcare applications operate and handle patient data. [16]

Moreover, to optimize system performance and increase processing speed, only select nodes are allowed to participate in consensus and validation processes. This approach contrasts with public blockchain protocols like Bitcoin, where any node can engage in consensus or validation processes. [16]

6.3. What research issues remain open, and what areas deserve future exploration?

As blockchain technology continues to gain traction in healthcare, there is a pressing need for researchers to develop more prototypes and proof-of-concepts to deepen our understanding and maturity of its application in the field. Many proposed frameworks, concepts, models, and architectures, such as those outlined in [58], must be implemented and rigorously tested to assess their efficacy and limitations.

Ensuring interoperability among different blockchain products is essential, underscoring the importance of open standards. While current efforts focus on testing blockchain prototypes for proof of concepts, achieving widespread adoption in operational healthcare settings necessitates the establishment of open standards for interoperability. Therefore, researchers should turn their attention to interoperability issues and participate in standardization processes, leveraging platforms like the ISO/TC 307 standards group to contribute their insights [55].

The challenges surrounding data security and privacy, interoperability, scalability, and speed in blockchain-based healthcare applications remain open research issues. Addressing these challenges requires sustained research efforts to bolster stakeholder confidence in the technology and facilitate its broader adoption in healthcare.

7. Conclusion

Blockchain technology, initially introduced through Bitcoin, has undergone significant evolution, emerging as a versatile technology applicable across various industries, including healthcare. To gain insights into the current state of blockchain technology in healthcare, we conducted a systematic review. Our study aimed to identify use cases, applications, challenges, development approaches, and areas for future research in blockchain-based healthcare applications. From our search and paper selection, we analyzed 30 papers to address our research questions.

Our findings reveal that blockchain has numerous use cases in healthcare, encompassing electronic medical records management, pharmaceutical supply chain management, biomedical research, education, remote patient monitoring, health data analytics, and more. Several blockchain-based healthcare applications have been developed as prototypes, leveraging emerging paradigms like smart contracts, permissioned blockchain, off-chain storage, among others. However, further research is essential to comprehensively understand, characterize, and evaluate the effectiveness of blockchain technology in healthcare.

Ongoing efforts need to be supplemented with additional research to tackle challenges such as scalability, latency, interoperability, security, and privacy associated with the integration of blockchain

technology in healthcare. This collective research endeavor will contribute to the continued advancement and successful implementation of blockchain in the healthcare domain.

References

[1] Alammary A, Alhazmi S, Almasri M, Gillani S. Blockchain-Based Applications in Education: A Systematic Review. Applied Sciences. 2019 Jan;9(12):2400.

[2] Rocha G da SR, de Oliveira L, Talamini E. Blockchain Applications in Agribusiness: A Systematic Review. Future Internet. 2021 Apr;13(4):95.

[3] Agbo CC, Mahmoud QH, Eklund JM. Blockchain Technology in Healthcare: A Systematic Review. Healthcare. 2019 Jun;7(2):56.

[4] Elghoul M, Bahgat S, Hussein A, Hamad S (2021) A review of leveraging blockchain based framework landscape in healthcare systems. Int J Intell Comput Inf Sci 0(0):1–13.

[5] Rabah K. Challenges & opportunities for blockchain powered healthcare systems: a review. Mara Res J Med Health Sci 2017; 1(1): 45–52.

[6] Ekblaw A, Azaria A, Halamka JD, et al. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Proc IEEE Open Big Data Conf 2016; 13: 13.

[7] Elghoul MK, Bahgat SF, Hussein AS, Hamad SH. Management of medical record data with multi-level security on Amazon Web Services. SN Appl Sci. 2023 Oct 8;5(11):282.

[8] Madine MM, Battah AA, Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y, et al. Blockchain for Giving Patients Control Over Their Medical Records. IEEE Access. 2020;8:193102–15.

[9] Makridakis S, Christodoulou K. Blockchain: Current Challenges and Future Prospects/Applications. Future Internet. 2019 Dec;11(12):258.

[10] Haddad A, Habaebi MH, Suliman FEM, Elsheikh EAA, Islam MR, Zabidi SA. Generic Patient-Centered Blockchain-Based EHR Management System. Applied Sciences. 2023 Jan;13(3):1761.

[11] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing List (2009).

[12] Tschorsch F, Scheuermann B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials. 2016;18(3):2084–123.

[13] Vujičić D, Jagodić D, Ranđić S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In: 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH) [Internet]. 2018 [cited 2024 Jan 11]. p. 1–6.

[14] Singh Y, Jabbar MA, Kumar Shandilya S, Vovk O, Hnatiuk Y. Exploring applications of blockchain in healthcare: road map and future directions. Frontiers in Public Health.

[15] Mettler M. Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.

[16] Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.

[17] Dey N, Ghosh M, Chakrabarti A. Quantum solutions to possible challenges of Blockchain technology. 2021.

[18] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress). Honolulu, HI: IEEE (2017), p. 557–64.

[19] Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System. Decentralized Business Review. (2008) p. 21260.

[20] Buterin V. A next-generation smart contract and decentralized application platform. White Paper. (2014) 3:2–1.

[21] Meyer M. Blockchain Technology: Principles Applications - IEEE Access. (2016).

[22] Cachin C. Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Vol. 310. Chicago, IL (2016), p. 1–4.

[23] Malone D, O'Dwyer KJ. Bitcoin Mining and its Energy Footprint. IET. (2014). p. 280–85. doi: 10.1049/cp.2014.0699

[24] Castro M, Liskov B. Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation, Vol. 99. New Orleans, LA (1999), p. 173–86.
[25] Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—a scoping review. Int J Med Inform. (2020)
[26] Garrido A, Ramírez López LJ, Álvarez NB. A simulation-based AHP approach to analyze the scalability of EHR systems using blockchain technology in healthcare institutions. Informatics in Medicine Unlocked. 2021 Jan 1;24:100576.
[27] Hashim F, Shuaib K, Sallabi F. MedShard: Electronic Health Record Sharing Using Blockchain Sharding. Sustainability. 2021 Jan;13(11):5889.
[28] Mattila V, Dwivedi P, Gauri P, Ahbab M. Enhancing Transaction Throughput In Public Blockchain Network Using Nested Chains. Ijssmr. 2022;05(02):257–63.
[29] Sonkamble RG, Phansalkar SP, Potdar VM, Bongale AM. Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. IEEE Access. 2021;9:158367–401.
[30] Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain Application in Healthcare Systems: A Review. Systems. 2023 Jan;11(1):38.
[31] Courtney R, Ware W. Some informal comments about integrity and the integrity workshop. In:Ruthberg ZG, Polk WT, , editors. Proc. of the Invitational Workshop on Data Integrity. Gaithersburg, MD: National Institute of Standards and Technology, Special Publication (1989), p. 500–68.
[32] Coiera E. Guide to Health Informatics. Boca Raton, FL: CRC Press (2015). doi: 10.1201/b13617
[33] Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Inf Manag J. (2015)
[34] Azaria, A. Ekblaw., T. Vieira., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In 2nd International Conference on Open and Big Data (pp. 25-30). IEEE.
[35] Nchinda Ngek, E. S., Nsioge, R. M., Ngenge, M. B., & Kadia, B. M. (2019). An intriguing case of lichen simplex chronicus in an elderly sub-Saharan African with longstanding scabies and sensory neuropathy. Pan African Medical Journal, 34,
Article 124.
[36] Mikula, T., & Jacobsen, R. H. (2018). Identity and Access Management with Blockchain in Electronic Healthcare Records. In 21st Euromicro Conference on Digital System Design (pp. 699-706). IEEE.
[37] Haque, R., Sarwar, H., Kabir, S. R., Forhat, R., Sadeq, M. J., Akhtaruzzaman, Md., & Haque, N. (2020). Blockchain-Based Information Security of Electronic Medical Records (EMR) in a Healthcare Communication System. In Intelligent Computing and Innovation on Data Science, (pp. 641–650). Springer.
[38] Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of Used Cryptography in Blockchain. IEEE Access, 7, 148550–148575
[39] Zhang, J., Li, Z., Tan, R., & Liu, C. (2021). Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology. BioMed Research International, 2021
[40] Pilares, I. C. A., Azam, S., Akbulut, S., Jonkman, M., & Shanmugam, B. (2022). Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. Sensors, 22(11), 4032.
[41] Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. In:Raj P, Deka GC, , editors. Advances in Computers, Vol. 111. Amsterdam: Elsevier (2018), p. 1–41.
[42] Homans GC. Social Behavior: Its Elementary Forms. Unknown. (1974).
[43] Fan K, Wang S, Ren Y, Li H, Yang Y. MedBlock: efficient and secure medical data sharing via blockchain. J Med Syst. (2018) 42:136.
[44] Usip PU, Ekpenyong ME, Ijebu FF, Usang KJ, Udo IJ. PeNLP parser: an extraction and visualization tool for precise maternal, neonatal and child healthcare geo-locations from unstructured data. In:Agarwal B, Balas VE, Jain LC, , editors. Deep Learning in Biomedical and Health Informatics. Boca Raton, FL: CRC Press (2021), p. 157–81.

[45] Usip PU, Ekpenyong ME, Ijebu FF, Usang KJ. Integrated context-aware ontology for MNCH decision support. In:Tiwari S, Rodriguez FO, ŽJabbar MA, , editors. Semantic Models in IoT and Ehealth Applications. Amsterdam: Elsevier (2022), p. 227–43. doi: 10.1016/B978-0-32-391773-5.00017-0
[46] Sharma R, Zhang C, Wingreen SC, Kshetri N, Zahid A. Design of blockchain-based precision health-care using soft systems methodology. Ind Manag Data Syst. (2020) 120:608–32.
[47] Pouyan Esmaeilzadeh TM. The Potential of Blockchain Technology for Health Information Exchange: Experimental Study from Patients' Perspectives. (2019).
[48] Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. IEEE Access. (2019) 7:147782–95.
[49] El-Gazzar R, Stendal K. Blockchain in health care: hope or hype? J Med Internet Res. (2020) 22:e17199.
[50] Wamba SF, Queiroz MM. Blockchain in the operations and supply chain management: benefits, challenges and future research opportunities. Int J Inf Manag. (2020) 52:102064.
[51] Singh D, Monga S, Tanwar S, Hong WC, Sharma R, He YL. Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons. Applied Sciences. 2023 Jan;13(4):2380.
[52] Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology Applications in Health Care. Circ. Cardiovasc. Qual. Outcomes 2017.
[53] Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. 2019.
[54] Zhou, L.; Wang, L.; Sun, Y. MIStore: A Blockchain-Based Medical Insurance Storage System. J. Med. Syst. 2018.
[55] Engelhardt, M.A. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technol. Innov. Manag. Rev. 2017.
[56] 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.
[57] J.M.; De la Corte-Rodriguez, H.; Rodriguez-Merchan, E.C.C.; la Corte-Rodriguez, H.; Carlos Rodriguez-Merchan, E. How Blockchain Technology Can ChangeMedicine. Postgrad. Med. 2018, 130, 420–427.
[58] Mamoshina, P.; Ojomoko, L.; Yanovich, Y.; Ostrovski, A.; Botezatu, A.; Prikhodko, P.; Izumchenko, E.; Aliper, A.; Romantsov, K.; Zhebrak, A.; et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 2017, 9, 5665–5690.
[59] Funk, E.; Riddell, J.; Ankel, F.; Cabrera, D. Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education. Acad. Med. 2018, 93, 1791–1794.
[60] Nugent, T.; Upton, D.; Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. F1000 Res. 2016, 5, 2541.
[61] Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. Symmetry 2018, 10, 470.
[62] Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
[63] Rouhani, S.; Deters, R. Security, Performance, and Applications of Smart Contracts: A Systematic Survey. IEEE Access 2019.
[65] Shabani M. Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? J Am Med Inform Assoc. (2019) 26:76–80.
[66] 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.
[67] Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J. Med. Syst. 2018, 42, 130.

[68] 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.
[69] Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR mHealth uHealth 2017, 5, e111.
[70] 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.
[71] 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.
[72] www.allcryptowhitepapers.com. Medicalchain Whitepaper [Internet]. The Whitepaper Database. 2018 [cited 2024 Feb 4]. Available from:
[73] Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B.; Marella, B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. Sustain. Cities Soc. 2018, 39, 283–297.
[74] Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-Based Data Preservation System for Medical Data. J. Med. Syst. 2018, 42, 141.
[75] Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MedShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access 2017, 5, 14757–14767.
[76] 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
[77] Monga, S.; Singh, D. Designing a Transformational Model for Decentralization of Electronic Health Record Using Blockchain. In Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S), Lecture Notes in Networks and Systems; Singh, P., Pawłowski, W., Tanwar, S., Kumar, N., Rodrigues, J., Obaidat, M., Eds.; Springer: Singapore, 2020; Volume 121.
[78] Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J. Med Syst. 2016, 40, 453.
[79] Cichosz, S.L.; Stausholm, M.N.; Kronborg, T.; Vestergaard, P.; Hejlesen, O. How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept. J. Sci. Technol. 2018, 13, 248–253.
[80] Yang, H., & Yang, B. (2017). A Blockchain-Based Approach to the Secure Sharing of Healthcare Data. In Proceedings of the Norwegian Information Security Conference 2017 (pp. 100–111). NIKS.
[81] Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A Survey on Blockchain Interoperability: Past, Present,and FutureTrends. arXiv.
[82] 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.
[83] 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.
[84] Jiang, S.; Jakobsen, K.; Bueie, J.; Li, J.; Haro, P.H. A Tertiary Review on Blockchain and Sustainability With Focus on Sus-tainable Development Goals. IEEE Access 2022, 10, 114975–115006.
[85] 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.
[86] 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.
[87] 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.
[88] 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.

[89] Qu, W., Wu, L., Wang, W., Liu, Z., & Wang, H. (2020). A electronic voting protocol based on blockchain and homomorphic signcryption. Concurrency and Computation: Practice and Experience, 34(16), e5817.
[90] 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.
[91] Mohammed, R.; Alubady, R.; Sherbaz, A. Utilizing blockchain technology for IoT-based healthcare systems. J. Phys. Conf. Ser. 2021, 1818, 012111.
[92] PPandey, P.; Litoriya, R. Securing and authenticating healthcare records through blockchain technology. Cryptologia 2020, 44, 341–356.
[93] 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.
[94] 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.
[95] Sharma, Y. A survey on privacy preserving methods of electronic medical record using blockchain. J. Mech. Contin. Math. Sci. 2020, 15, 32–47.
[96] 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.
[97] 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.
[98] 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.
[99] 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.
[100] 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.
[101] 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.
[102] 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.
[103] 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.