applied sciences

MDPI

Review

Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons

Dilbag Singh [1], Suhasini Monga [1,*], Sudeep Tanwar [2], Wei-Chiang Hong [3,4,*], Ravi Sharma [5] and Yi-Lin He [3]

1 Department of Computer Science and Engineering, Chaudhary Devi Lal University, Sirsa 125055, India
2 Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad 382481, India
3 Department of Information Management, Asia Eastern University of Science and Technology, New Taipei 22064, Taiwan
4 Department of Information Management, Yuan Ze University, Chungli, Taoyuan 32003, Taiwan
5 Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, Dehradun 248001, India
* Correspondence: suhasini.monga@gmail.com (S.M.); samuelsonhong@gmail.com (W.-C.H.)

Abstract: Blockchain technology was bestowed through bitcoin; research has continuously stretched out its applications in different sectors, proving blockchain as a versatile technology expanded in non-financial use cases. In the healthcare industry, blockchain is relied upon to have critical effects. Although exploration here is generally new yet developing quickly, along these lines, researchers in computer science, healthcare information technology, and professionals are continually geared to stay up with research progress. The study presents an exhaustive study on blockchain as a technology in depth from all possible perspectives and its adoption in the healthcare sector. A mapping study has been conducted to search different scientific databases to identify the existing challenges in healthcare management systems and to analyze the existing blockchain-based healthcare applications. Though blockchain has inherent highlights, such as distributed ledger, encryption, consensus, and immutability, blockchain adoption in healthcare has challenges. This paper also provides insights into the research challenges in blockchain and proposes solution taxonomy through comparative analysis.

Keywords: blockchain; healthcare; electronic health records (EHR); consensus; decentralized applications; healthcare management systems (HMS)

Citation: Singh, D.; Monga, S.; Tanwar, S.; Hong, W.-C.; Sharma, R.; He, Y.-L. Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons. *Appl. Sci.* **2023**, *13*, 2380. https://doi.org/10.3390/app13042380

Academic Editor: Andrea Li Bassi

Received: 21 December 2022
Revised: 8 February 2023
Accepted: 9 February 2023
Published: 13 February 2023

1. Introduction

In recent times, cryptocurrency has emerged to be a quintessential thing in almost all trades of the world. Bitcoin, referred to as the primary cryptocurrency, enjoyed enormous success in the financial market in 2016. The core principle technology that underlies bitcoin is the blockchain. Blockchain was first projected in 2008 and enforced in 2009 by Nakamoto [1]. Blockchain, a decentralized, immutable, and robust technology, has been significantly impacting healthcare systems. The healthcare management system (HMS) is of social significance because the issues it addresses are legitimate worries [2]. The goal is to improve personal satisfaction by defeating genuine health issues [3]. Computer science has been integrated into healthcare, giving rise to healthcare information technology (HIT), which has prompted massive advancement in healthcare [4–6]. Although the healthcare sector is advancing, it suffers many challenges and loopholes [7]. HMS is one of the complex frameworks that must be highly secure and maintain confidentiality. HMS is designed using information communication technology (ICT) covering a vast domain of subsystems, including Hospital Information System (HIS), Healthcare Management Information System (HMIS), Internet-Based Telesurgery System (IBTS), Remote Patient Monitoring System (RPMS), Mobile Healthcare System(MHS) [8,9]. To design a resilient data framework in the healthcare sector, it is essential to distinguish changing necessities and constantly improve the framework plan [10]. It empowers the patient to obtain accurate healthcare data, the suppliers to improve the nature of care, and enables the healthcare executives to manage data [11]. Any intrusion in these frameworks can be generally costly, both financially and socially. By incorporating new technologies such as blockchain and IoT, healthcare quality and data management could be improved [12]. This review paper has been designed with the awareness that the adoption of blockchain technology in healthcare has significant promise for tackling the numerous difficulties in the HMS.

The structure of the review shown in Figure 1 is as follows: Section 1 gives an introduction, including the scope of the review and contributions of the paper. Section 2 presents the research methodology used for the review. Section 3 identifies challenges and loopholes in HMS. Section 4 provides a description of blockchain technology and the adoption of blockchain in healthcare. This section also proposes a BC-based solution taxonomy for HMS and a comparative analysis with traditional HMS. Section 5 highlights the critical challenges of BC adoption in HMS, and Section 6 concludes the paper.

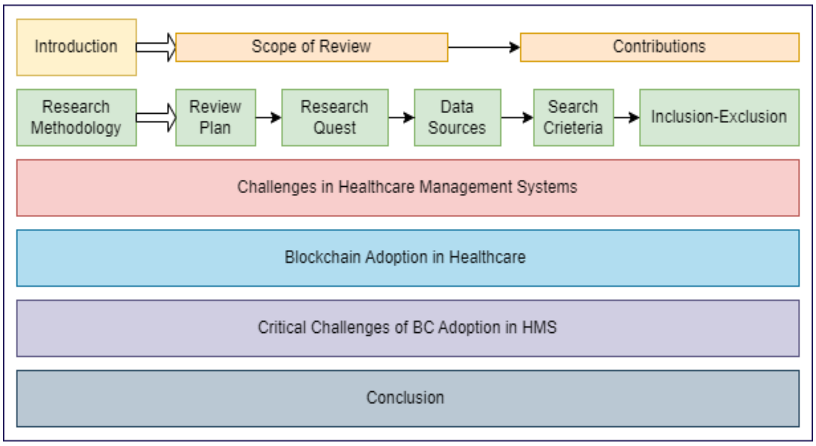

Figure 1. Structure of the review.

1.1. Scope of Review

Although BC is a novel technology, many review papers have been published to date by researchers on blockchain as an innovation and its various applications, including healthcare and research challenges. Blockchain had been reviewed from different perspectives, but major reviews focused either on blockchain applications or security aspects in blockchain [13–15]. Some authors have also reviewed the role of blockchain in healthcare specifically [16–18]. There is much ongoing research in blockchain, yet no comprehensive review considers all potential parts of the BC technology innovation and its adoption in HMS. The proposed review follows an all-encompassing methodology that covers BC as a technology, its impact in diverse applications, the adoption of BC in healthcare, and BC research challenges. An in-depth study is conducted to identify and understand the challenges in existing HMS. This paper explored security loopholes in HMS and cyber-attacks since 2009. The proposed review also summarizes the features of some popular blockchain-based HMS. Depending on the study of these systems and challenges, this paper proposed a solution taxonomy and comparative analysis with traditional systems.

The proposed review begins with related work presented in the form of a comparative analysis of existing literature and their disparities with the proposed review in Table 1. The novelty of the proposed review is clearly depicted in Table 1 covering all the key factors that no other review paper has done before. The wider scope of the proposed review focused not only the BC adoption in healthcare but also explored challenges in existing HMS and BC.

Table 1. Comparison of proposed survey with existing state-of-the-art surveys.

Authors	Year	Objective	Merits	Demerits	1	2	3	4	5	6	7
Reyna et al. [13]	2018	To investigate and survey the BC integration in IoT	Critical Analysis of IoT-Integrated BC applications	No proposed solution for issues and challenges	Y	N	Y	N	Y	N	N
Gupta et al. [14]	2018	To provide a survey of BC from security perspective	Elaborated attacks in networks based on BC	Discussed threats only in bitcoin-based BC	Y	N	Y	N	Y	Y	N
Hölbl et al. [16]	2018	To highlight the difficulties and promising areas for blockchain research in healthcare	Categorically reviewed number of publications year-wise	Review of literature to date only. Latest research not covered	N	Y	Y	N	N	N	N
Gökalp, E. et al. [17]	2018	To analyze the opportunities and challenges of BC integration in healthcare	Analyzed features and challenges of BC in the proposed framework	Abstract view and discussed challenges pertaining to the proposed work only	N	Y	N	N	Y	N	Y
Chen et al. [6]	2018	To Survey BC usage in different domains	Survey on issues in various applications	Abstract work on technical aspects of BC	Y	N	N	N	N	N	N
Agbo et al. [18]	2019	To discuss the ongoing research in BC technology in healthcare	Detailed review of publications in BC in healthcare	Focus is on listing of research papers	N	Y	Y	Y	N	N	N
McGhin et al. [19]	2019	To assess the challenges and opportunities of BC in healthcare applications	Analysis of existing BC healthcare Applications	Not addressed immutability, decentralized access of data	N	Y	Y	N	Y	N	N
Alladi et al. [15]	2019	To provide a review of BC in industry 4.0 and IoT BC integration	Categorized existing commercial applications and future research directions	Only conceptual discussion on various components of BC	Y	N	N	N	Y	Y	N
Al-Jaroodi et al. [20]	2019	To explore BC in Industries the opportunities, benefits, and challenges	Benefits of BC in various domains	Focuses on BC domain in general	Y	N	N	N	Y	N	N
Khezr et al. [21]	2019	To provide a comprehensive review of BC-based healthcare applications	Comparison of data management, supply chain, IoT medical mechanisms	Potential threats and issues are not discussed in detail	Y	Y	Y	Y	N	Y	N
Soni et al. [22]	2019	To survey on working of BC covering threats and futuristic use cases of BC	Compared different types of BC	Only security and privacy issues are focused	Y	N	Y	N	Y	Y	N

Table 1. *Cont.*

Authors	Year	Objective	Merits	Demerits	1	2	3	4	5	6	7
Rouhani et al. [23]	2019	To review security, performance, and applications of smart contracts	Categorizes technology platforms and programming languages for smart contracts	Performance comparison only on the basis of smart contract security issues	Y	N	Y	Y	N	N	N
de Aguiar et al. [24]	2020	Aims to address BC-based strategies for healthcare applications	Presented SWOT analysis of BC	Not covered BC technicalities and development frameworks	N	Y	Y	N	Y	Y	N
Hathaliya et al. [25]	2020	To present an analysis of existing systems for security and protection in Healthcare 4.0	Presented security attacks and various systems in healthcare	Focused on security and privacy issues only	N	Y	N	N	N	Y	Y
Taylor et al. [26]	2020	To review utilization of blockchain for cybersecurity purposes	Focused on BC in IoT, AI, and other security frameworks	Compared BC applications through a single perspective	Y	N	N	N	N	Y	N
Durneva et al. [27]	2020	To evaluate the issues using BC for patient care, also to offer a research agenda for next studies	Segregated research studies on blockchain in HIT using frequency measure	Abstract view of BC HIT implementation and complex structure of paper	N	Y	N	N	Y	N	N
Chukwu et al. [28]	2020	To investigate and assess the various BC models suggested, prototyped, or put into effect	PRISMA chart for review structure and Bibliometric analysis	Very complex flow of the paper, not focused on challenges of BC	N	Y	N	Y	N	Y	N
Tandon et al. [29]	2020	To analyze the research on blockchain applications in the medical field	Planned SLR of the research articles using citation analysis	Focused on limited data sources, including highly cited journal papers only	N	Y	N	N	N	Y	Y
Attaran [30]	2020	To identify the challenges and opportunities of BC in healthcare	Presented challenges of healthcare and their BC solutions	Confined to BC from an application standpoint	N	Y	N	N	Y	N	N
Abu-elezz et al. [31]	2020	To classify the advantages and disadvantages of using BC in the healthcare sector	Summarized threats and benefits of BC	Very basic overview of threats and benefits of BC	N	Y	N	N	N	N	N
Gaynor et al. [32]	2020	To examine existing concerns of BC technology in healthcare	Evaluation using Marco's framework	Focused on impact of BC in three applications only	N	Y	N	N	N	N	Y

Table 1. *Cont.*

Authors	**Year**	**Objective**	**Merits**	**Demerits**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Song et al. [33]	2021	To understand BC as a service and its implications	Analyzed scope of BC as service for various business models	Does not cover real-time applicability	Y	N	N	N	Y	Y	N
Saeed et al. [34]	2022	To explore paradigm shift in healthcare using BC	Assessment of BC-based healthcare applications	Not covered technicalities and challenges of BC	N	Y	N	N	N	Y	N
Guntur et al. [35]	2022	To discuss BC and its scope in healthcare sector	Categorically discussed merits and demerits of types of BC	Very basic review of BC healthcare applications	N	Y	Y	N	Y	N	N
Proposed Review	2022	To review BC adoption in healthcare, including challenges, solutions, and comparisons	Holistic approach for BC adoption in healthcare, including proposed solution taxonomy	Exploring challenges of BC technology and their resolutions	Y	Y	Y	Y	Y	Y	Y

1: Diverse Domains, 2: Healthcare Focused, 3: BC Technical Features, 4: Development Frameworks, 5: Challenges in BC, 6: Comparative Analysis, 7: Proposed Solution Taxonomy.

1.2. Contributions

Based on the exhaustive study and review, the following are the major contributions of this paper:

- A comprehensive review and comparison of the existing literature with the proposed review have been made based on key factors. An in-depth analysis of challenges and loopholes in existing healthcare management systems;
- A holistic description of blockchain, architecture, development frameworks, and diverse applications. In addition, an exhaustive review of existing blockchain-based healthcare management systems has been performed;
- Proposed blockchain-based solution taxonomy for a healthcare management system and a comparative analysis has been performed with traditional systems;
- Various research challenges in the blockchain have been identified and discussed.

2. Research Methodology

The research methodology used in this paper is discussed in this section; our search approach includes all possible literature reviews conducted in blockchain and healthcare.

2.1. Review Plan

The proposed review starts with recognizing a research quest including different aims, corresponding data sources, and keywords for database search, followed by inclusion and exclusion criteria for a quality selection of related literature.

2.2. Research Quest

Every research process starts with a research quest defining different aims of the research to be conducted. Table 2 describes the research quest used in the review.

2.3. Data Sources

Standard peer-reviewed databases (such as Scopus, IEEE Xplore, ScienceDirect, ACM Digital Library, and Springer link) have been used to search the existing literature and electronic data sources. Other resources, such as conferences, reports, technical book chapters, and online articles available on different sites, are included.

Table 2. Research quest used in review.

Research Quest	Description
RQ1: Study of Challenges in HMS	Comprehensive review and analysis of various challenges in HMS, security loopholes, and cyberattacks in HMS since 2009.
RQ2: Blockchain Technology	Study of blockchain features, architecture, and diverse applications. Comparison of Consensus algorithms and development frameworks required for BC implementation.
RQ3: Blockchain Adoption in HMS	Exploration of blockchain adoption in healthcare indicating the potential use cases. Summarized features of popular blockchain-based systems or prototypes through a tabular representation.
RQ4: Critical Challenges of Blockchain Adoption in HMS	Discussion on research challenges of blockchain technology adoption in HMS.

2.4. Search Keywords

Search has been conducted using keywords such as "Blockchain technology", "Blockchain in Healthcare", and many other related keywords, as shown in Figure 2.

Figure 2. Possible search keywords used in review.

2.5. Inclusion-Exclusion

Based on the search keywords given in Figure 2, an inclusion-exclusion criterion has been followed in this paper. Figure 3 draws a line between inclusion and exclusion criteria used for the screening and selecting studies for this paper.

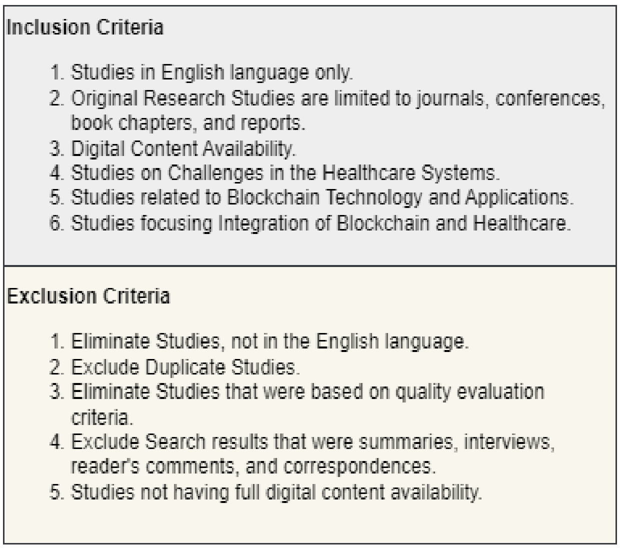

Figure 3. Criteria for screening and selection of studies.

The first phase included 150 publications, including research papers, articles, patents, book chapters, theses, conferences, and reports. The second phase categorized 150 publications into two categories original research and review. In the third phase, 100 publications were selected based on relevance. The final phase selected 84 final sets of quality publications (research papers, articles, conferences, book chapters, and reports) to be included in the proposed review.

3. Challenges in Healthcare Management Systems

The healthcare sector suffers from many challenges, loopholes, and issues in various domains [36]. Based on related research work, this study identifies the various challenges in existing HMS depicted in Figure 4.

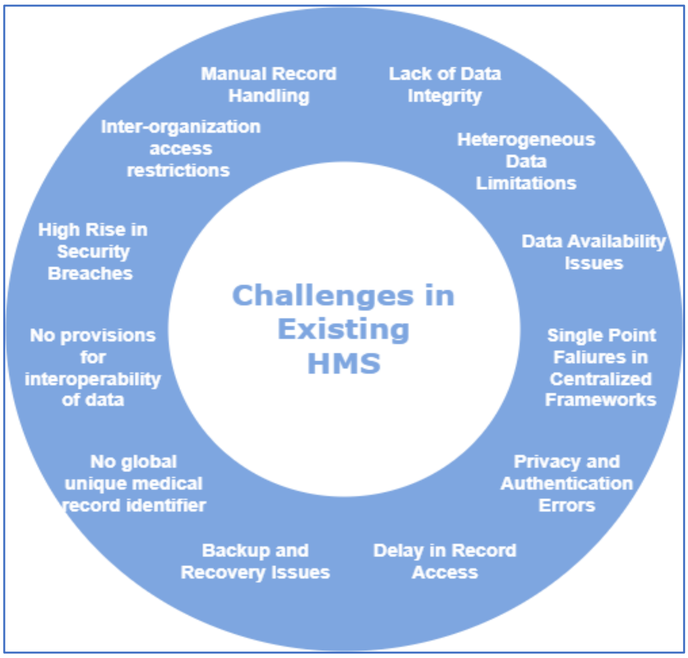

Figure 4. Challenges in the existing HMS [37–39].

- **Manual Record Handling:** There has been no patient data sharing among different healthcare providers, even though there have been many advancements in medical record management in the healthcare sector [40]. Medical records are still primarily managed in the form of handwritten forms or reports in most hospitals. Paper-based medical records are created with several healthcare providers as patients see various specialists, change healthcare plans, or move to a new city. The records are often housed in distinct, independent data silos, each with its storage configuration, security system, and descriptive semantics. Because of manual record systems, data sharing has been more challenging for patients, providers, and payers;
- **Lack of Data Integrity:** Data modification and duplication are major issues in data management. Data integrity is always tampered with by a chance of error while maintaining health records, as different persons are involved at different locations. Errors such as mismatched records, incomplete information, data duplication, missing lab reports, and no historical data make health records less integral. In addition, medical records are central to a healthcare institution and cannot be accessed outside; critical healthcare cannot be granted in such cases as up-to-date information is not available [41];
- **Data Availability Issues:** Manual record keeping has many limitations, including the need for large storage areas and difficulties with data retrieval. Data availability issues still exist with current EHRs because the data are housed in a centralized database that is only accessible within the hospital or healthcare facility, even though the switch

to EMR and EHRs made data retrieval slightly easier. Data are also lost permanently in the current systems in the event of server latency and failure;

- **Privacy and Authentication Errors:** Keeping health data private has been another challenge for HMS. Health records are the most pertinent for every patient for which the access must be patient-centric. There must be a provision for patient control over health information sharing and confidentiality. HMS suffers from privacy breaches where records are less private and can be modified [39]. Authentication issues such as access control and eavesdropping are also having a bad effect on private health information;
- **Delay in Record Access:** Most healthcare systems now allow patients to examine some of their medical records online. However, these portals provide information that needs to be finished in terms of timing and integrity. Medical records are an important part of managing a patient. It is essential that medical professionals and facilities can quickly access patient records. A delay in record access could endanger a patient who is experiencing major health issues;
- **High Rise in Security Breaches**: The biggest challenge in HMS is security. Several attempts of security breaches have led to the loss of critical health data. Many disastrous situations have occurred due to threats such as insider attacks, Wi-Fi attacks, data stealing, hacking, and many more. No robust, secure mechanism can avoid these attacks, as there is a central server for data storage. Even cloud storage is also vulnerable to these threats [39];
- **No provisions for Interoperability of Data:** Varying information standards across different healthcare providers is another challenge that hampers health record quality. Interoperability has been an issue in HMS as different stakeholders, complex cycles, and clinical guidelines are involved. These factors create enormous hindrances in conveying improved patient care. Interoperability among medical services suppliers, frameworks, and medical care data has been one of the most critical prerequisites in giving accurate health information;
- **Backup and Recovery Issues:** Data loss can occur for many reasons, including natural disasters, information security breaches, manual errors, and tampering with information by intruders. HMS has been facing these issues on an operational basis, where data recovery is challenging. There must be an efficient system to track the operations and actions taken by different people involved in the system. Many healthcare systems store their data on a central server where a single point of failure can lead to the failure of the entire system. Backup and recovery are significant hindrances when it comes to health information retrieval;
- **Heterogeneous Data Limitations:** Healthcare data are a combination of different information forms, including heterogeneous data formats such as prescription slips, clinical lab reports, X-rays, MRI scans, etc. These diverse-natured records are difficult to handle and manage. HMS faces many challenges due to the heterogeneity of records and data scaling. Due to the expounding of patients' health historical records, HMS has been suffering a lot while storing these heterogeneous data for a long time;
- **Inter-Organization Access Restrictions**: HMS still suffers from inter-organization access restrictions. Because the data are stored locally/centrally on the server, the system cannot access it outside a healthcare organization. Lack of trust prevails among healthcare providers, especially while sharing patient information. There is no safe connection for sharing health data throughout the health system;
- **Single-Point Failure in Centralized Frameworks:** Centralized EHRs have addressed several EMR-related issues, such as digitally managing substantial volumes of data utilizing a central server. However, the single point of failure problem still affects the system. Many healthcare systems save their data on a central server, where the loss of one component might bring down the entire system. A single point of failure is essentially a weakness in the design, configuration, or execution of a system, circuit, or component that poses a risk because it could lead to a situation in which just one issue or malfunction stops the entire system from working;

- **No Global Unique Medical Record Identifier:** Identity management, which has been classified as a connected attribute that belongs to an entity, is one of the primary challenges. There are gaps because digital identity management is not widely used, and each user record exists in several copies. The provider-centric system only allows the treating physician to view patient information. Viewing health information is restricted for patients. The patient does not have the authority to manage their health information, and they are also unaware of who is authorized to access it.

Patients must exchange their medical records and data throughout the healthcare ecosystem since it is a complicated system with many different actors. The exchange of patient data simultaneously cannot be prohibited, and security rules must be handled to make this possible. Over the years, security and privacy attacks on healthcare systems have occurred often. The most significant cyberattacks and the loopholes behind them are listed in Table 3.

Table 3. Summary of cyberattacks over the years [22,39].

Loophole	Attack	Year of Occurrence	Place of Attack
Media Tamper	AIDS Trojan DoS	1989	Becker's Hospital
Identity Theft	Medical Record Hacking	2009	HealthNet, Affinity Health Plan, Inc.
		2011	Tricare, Memorial Healthcare System, Nemours Foundation
		2012	U.S. Medicaid, South Carolina Government
		2014	Community Health Systems
		2015	Care First Bluecross, Medical Informatics Engineering, UCLA Medical Center
		2016	21st Century Oncology, Apple Health Medicaid, Inuvik Hospital
		2018	Centers for Medicare & Medicaid Services
		2019	Health Sciences Authority Singapore, Life Labs
Unauthorized Access	Stolen Computer/Lost	2010	Emergency Healthcare Physicians, Lincoln Medical & Mental Health, New York City Health & Hospitals Corp.
		2013	Advocate Medical Group, Crescent Health Inc. Walgreens
Low Security Levels	Ransomware Wanna Cry	2017	Grozio Chiruguzia
	Ransomware Clop	2020	Accellion
	Ransomware Conti	2021	Irish Health Service Executive
	Phishing	2020	Magellan Health

The cyberattacks mentioned above have harmed many individuals because they can no longer access their medical information confidentially. Figure 5 illustrates the number of persons affected by cyberattacks since 2009. These years were chosen for the study because it was 2009 when medical record digitalization became a new development that had an impact on the world, and IT expansion in healthcare systems began. BC has built-in security features since data are encrypted using the sender's private key [39], and only the proposed recipient can decode data using the sender's private key. Blockchain technology can be an efficient way to overcome the obstacles and challenges in HMS described above.

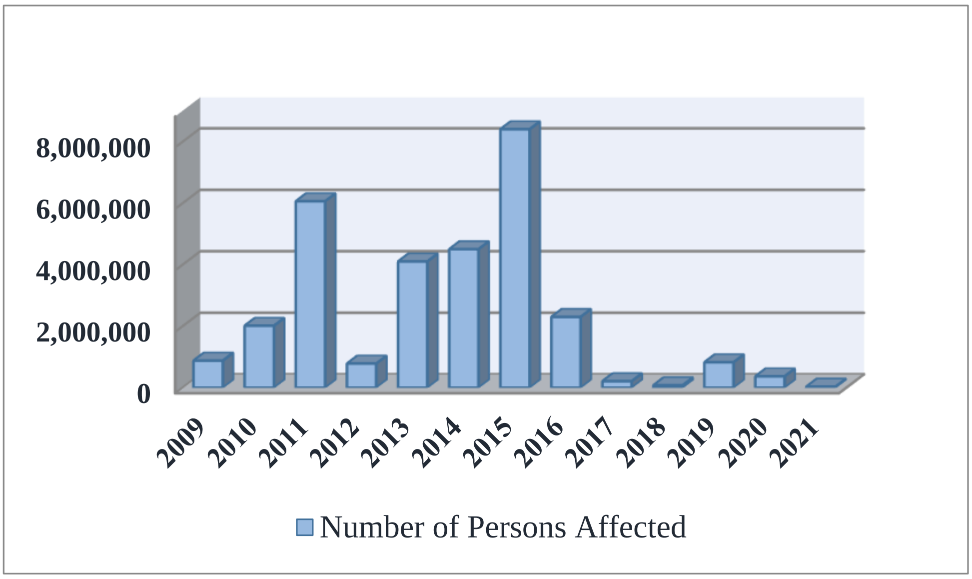

Figure 5. Year-wise number of persons affected due to cyberattacks in HMS [22,39].

4. Blockchain Adoption in Healthcare

Blockchain is enabled by integrating many core technologies, such as cryptographic hash, digital signature, and distributed consensus mechanism [42]. BC has various significant features that are the reasons for BC's popularity [43]. Decentralization is the major one where the control is not managed by a single centralized administrator. BC framework becomes more resilient to assaults due to this redundancy of data in the decentralized network [44]. Once a block is created in the blockchain, the records become immutable. Blockchain utilizes encryption algorithms to secure the legitimacy of the data [45,46]. The transactions in the blockchain are auditable as the validation is performed on the basis of timestamps, which provides ease to users to keep track of the previous records [47]. Transparency is the key to blockchain that is implemented using pseudo-anonymity [48].

A great trust mechanism is provided to the users of blockchain [49]. Whenever a new node is added to the network, a number of participants have to be in a consensus in order to confirm the node data in the blockchain [50]. There are different types of blockchains, but the most popular categories are: public, private, and consortium. A public blockchain is open, and anyone can participate in the network, whereas in a private blockchain, every transaction must be authenticated and validated by the administrator or nodes with admin rights [51]. A consortium blockchain is a partially private blockchain and is also called a hybrid/federated blockchain.

Blockchain architecture consists of decentralized peer-to-peer networks, hashing techniques, and consensus algorithms. A blockchain is a chain of blocks connected through the hash value of the previous block and so on [52]. A block stores information such as block index, time-stamp, nonce, block hash, previous block hash, and transactions [53,54]. Figure 6 gives an example of a simple blockchain. It comprises a distributed ledger of immutable transactions where every transaction is circulated to all the nodes in the peer-to-peer network [55,56]. The transaction is cleared when the nodes have agreed to acknowledge the new transaction into the distributed ledger [57]. Each block in the chain will have transactions $T \times 1$, $T \times 2$, ... $T \times n$, as shown in Figure 6.

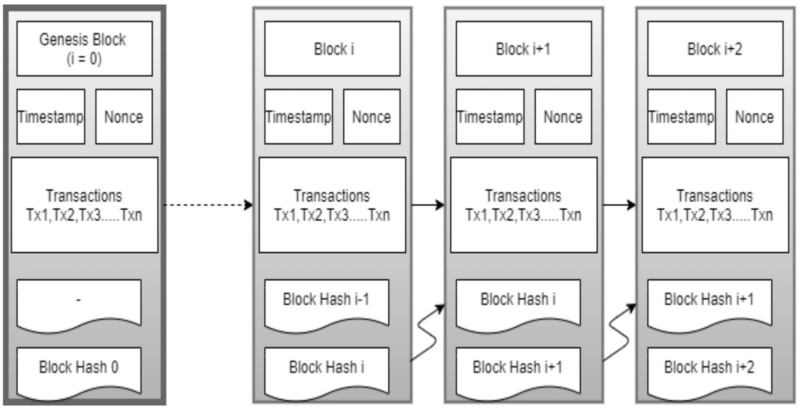

Figure 6. A simple blockchain [58].

From Figure 6, we can visualize that each block of the blockchain has a hash of the previous block as well as the hash of the current block, which is determined using the information stored in the block [58]. Thus, it is accepted that altering the information in a blockchain is practically unimaginable [59]. This hash is the critical component in a blockchain that furnishes security to forestall altering the information in a block [48]. Consensus mechanism refers to an arrangement of nodes that validates single transactions or n transactions [60].

Initially, blockchain innovation was intended for its most widespread usage in the financial sector [61]. However, today, its utility is growing in different sectors [62]. Potential energy applications having integration of blockchain have been divided into the following categories: trading energy markets, financing green energy, vehicles running on electricity, and energy production processes. Future blockchain-based identity management solutions are projected for emergency cases of identity. One prominent use case of blockchain could be land registration, where BC can consequently improve the potency of the registration process [63]. BC can be efficiently utilized in government sectors; voting systems can be built with blockchain and smart contracts, and every individual can see their vote and the general factual cycle [64]. BC improvises insurance applications in different regards; those are fraud disposal, claims mechanization, and information examination with the IoT [65].

BC has been developed as an eminent innovation, giving a breakthrough, and has distinguished potential in healthcare. In healthcare, BC can help build a global HMS, connecting patients, doctors, insurance companies, pharmacists, and medical researchers [66]. ICT and blockchain are empowering innovations for the decentralization and digitalization of healthcare systems [67]. Since the focus of this review is blockchain adoption in healthcare thus, Figure 7 depicts the impact of blockchain in various healthcare and its innovative use cases. A brief description of innovative BC use cases in healthcare is as follows:

Insurance and Claims: Health insurance and claims handling can profit from BCs transparency, decentralization, unchanging nature, and auditability of records [68]. Blockchain can be utilized for the approval of cases, which may build the productivity and security of the cycle [69]. The product can store encoded patient identifiers, health information, and supplier claims in a blockchain that payers and suppliers share [70].

Patient Care and Clinical Labs: Patient care and clinical lab record handling in HMS have been a challenge regarding security, timeliness, privacy, and sharing [71]. BC is a combination of disruptive technologies that can help resolve all the challenges associated with existing HMS [72]. The medical services industry will be more efficient with the applications and incorporation of blockcha.

Pharma and Supply Chain: Another recognized use case of blockchain is Pharma and supply chain management, especially in the medication/drug industry [67]. The conveyance of fake or inadequate prescriptions can have desperate ramifications for the patients [73]. Falsifying is a critical issue inside the drug business, but blockchain innovation has been recognized as having the ability to address this problem [16,24].

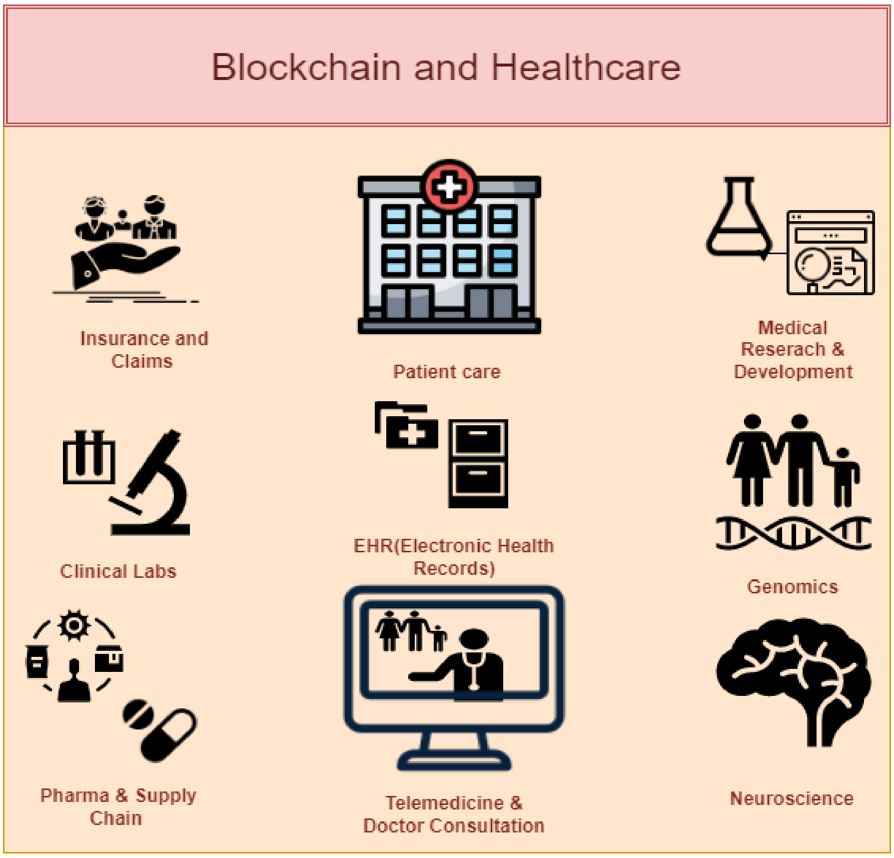

Figure 7. Blockchain adoption in healthcare [16,68,71,74].

Neuroscience: Blockchain innovation has been developed as a data innovation in a few neuroscience applications, for example, mind increase, cerebrum reenactment, and cerebrum thinking. Digitizing and storing all the cerebrum information requires a secure medium to store that information. An unwavering quality and blockchain innovation helps in the accurate and precise storage of brain information [23].

Telemedicine and Doctor Consultation: Telemedicine has enormous potential to convey real-time medical care [73]. The current telesurgery framework has security, protection, and interoperability issues, which restricts its appropriateness in medical care in the future [75]. BC-based telesurgery frameworks can certainly alleviate the issues and could be more effective [76].

Medical Research and Development: Blockchain has an intriguing use case in biomedical research, training, and development. Blockchain can assist with misrepresenting information and under-revealing or rejecting unfortunate outcomes in medical research. Blockchain makes it simpler for patients to provide authorization for their information to be utilized with the end goal of exploration [16].

Genomics: Human genomic ventures are creating a massive volume of genomic information widely utilized in biotechnology and clinical examination [77]. So there is a requirement for apparatuses and innovations that can help prepare and examine genomic information. Blockchain innovation has developed as a contemporary answer for storing and trading genomic information with security [24]. A study uses blockchain to produce and access genomic information with security-saving and decentralized techniques [51].

Electronic Health Records: The most well-known use of blockchain in healthcare is in EHR or EMR management to make information safer and dependable [64,74]. The constraint in EHR before blockchain innovation was that patients' information was dissipated among different medical services suppliers, and the past information was not open even in EHR frameworks [38]. Numerous analysts propose blockchain as a unique answer for storing patients' EHRs, having current data secure for a lifetime and can be recovered anytime [23]. A few prototypes based on blockchain have been developed by different companies such as MedRec [75], FHIRChain [78], MedBlock [79], MedShare [80], and many more. Over the past few years, different prototypes of blockchain-based HMS have been developed. Table 4 presents the summary of application features of the popular blockchain-based HMS:

Table 4. Summary of popular blockchain-based HMS.

Blockchain-Based HMS	Summarized Application Features
MedRec [75]	MedRec, product of MIT Media Lab and Beth Israel Deaconess Medical Center based on Ethereum. It targeted giving patients control over their information to determine who can get to them through fine-grained admittance consents based on blockchain.
Medicalchain [81]	Medicalchain has been developed utilizing a double blockchain structure. The first blockchain controls admittance to health records and was constructed utilizing Hyperledger Fabric. The second blockchain is on Ethereum, using the ERC20 token for administrators of the platform.
Ancile [82]	A blockchain-based structure developed on Ethereum blockchain using smart contracts for efficient and secure access control, non-repudiation of data, and utilized enhanced cryptographic procedures for additional security.
DPS [83]	Data preservation system based on Ethereum provided dependable data storage assuring the evidence of information while safeguarding security for critical health.
MedBlock [79]	MedBlock, a distributed ledger, two-layer architecture with a block structure based on Merkle-Tree, permitted effective EMR access and EMR recovery [79]. The hybrid consensus system accomplished the agreement of EMRs without huge energy utilization and organization clog.
MedShare [80]	MedShare, a framework that addresses the issue of enormous health data sharing among big data seekers. MedShare provided information provenance, examination, and control for shared health information in a cloud.
FHIRChain [78]	A system intended to meet ONC (Office of the National Coordinator for Health Information Technology) prerequisites by epitomizing the HL7 Fast Healthcare Interoperability Resources (FHIR) standard for shared medical information. A decentralized application has been developed based on computerized medical identity for distant tumor care.

4.1. Proposed Solution Taxonomy

Based on the review conducted, several challenges, issues, and loopholes have been identified in the existing HMS in Section 4. To resolve these challenges, BC can be an efficient solution. Healthcare data exchange is crucial for creating an efficient healthcare system and delivering high-quality healthcare services. Healthcare information is a valuable and private asset that patients must own and control. The present study proposes a solution taxonomy for a global healthcare management system in order to govern, own, securely access, and exchange information in accordance with patient authentication without compromising patient privacy. The proposed solution can be implemented in order to develop a full-stack blockchain-based framework for decentralized identity and robust data management for medical records in a global healthcare management system. The proposed solution taxonomy is divided into four components:

- **Block Creation:** The first time the information is entered, a new block will be created;
- **Patient Identity Management:** Once the block is created, a unique key for the patient will be generated that will act as a primary key in the distributed database. This identity or key will only be used for accessing patient records globally;
- **Data Management and Interoperability:** The patient health record information, such as disease symptoms, prescriptions, X-ray reports, lab reports, etc., will be inserted into the database, and the new block with the hashed key will be appended to the blockchain. Once a block is created, it becomes immutable that cannot be deleted. Any node could share the interoperable data with due permissions;

- **Consensus and Security:** If an existing record is to be searched or shared, it must be validated using a patient-hashed key and a joint consensus of the doctor/hospital and patient. Encrypted key ensures that each block having critical health data is secure in the blockchain and no one can access it without permission.

4.2. BC Development Frameworks

The proposed solution taxonomy can be developed as a decentralized blockchain system for healthcare management using a blockchain development platform. BC development begins with an intelligent component called smart contracts [84]. It is a programming code written in explicit language for various blockchains (public, private, and consortium) that can be executed when a specific condition is met [3]. An SC is a programming code written in a specific programming language, for example, Solidity, Go, Kotlin, or Python. SC is an immutable and enforceable project code [34].

There are many frameworks available for BC development [54]. Selection of a BC development platform is tough and requires a clear understanding of each platform. Thus an analytical comparison of popular development frameworks is shown in Table 5 for the selection of the best blockchain development platform.

Table 5. Comparison of popular BC development frameworks [1,3,42,84,85].

Basis	Bitcoin	Ethereum	Hyperledger	Corda	Ripple	Quorum	IOTA
BC Type	Public	Public, Private, Hybrid	Private/ Enterprise	Private/ Enterprise	Payments	Private/ Enterprise	Public
Fully Developed	Yes	Yes	Yes	Yes	Yes	Yes	In Progress
Industry	Financial Industry	Cross Industry	Cross Industry	Financial Industry	Financial Industry	Cross Industry	Banks and Financial Services
Preferable Applications	Crypto-Currency	SC and Crypto-Currency	Smart Contracts	SC and Crypto-Currency	Crypto-Currency	Smart Contracts	Crypto-Currency
Programming Language	C++	Solidity, Serpent, LLL	Golang, Java	Kotlin, Java	C++	Solidity	Java
Consensus	PoW	PoW, PoS	PBFT	Raft	Probablity Voting	Raft, BFT	Tip Selection algorithm
Currency	Bitcoin	Ether	Chaincodes	Dubbed XDC	Ripple (XRP)	Ether	IOTA coin
Governance	Nakamoto, bitcoin developer, bitcoin org	DAO	Linux Foundation	R3 Company	Ripple Labs	Ethereum, JP Morgan Chase	IOTA, Popov
Transaction Throughput	~a few thousand tps	~200 tps	>2000 tps	~170 tps	>1500 tps	~ few hundred	between ~7–15 tps
Mode of Operation	Trustless	Trustless	Validator node for trust	Trustless	Trustless	Trustless	Trustless
User Authentication	Digital Signature	Digital Signature	Enrollment Certificate	Password	Biometric	Password	Digital Signature

4.3. Comparison between Traditional and Blockchain-Based HMS

There are numerous advantages of blockchain-based HMS over traditional HMS. Traditional HMS here refers to manual systems, local electronic systems, and centralized server systems. After a systematic and rigorous review, various key factors were identified that acted as the basis for comparison. Table 6 gives a comparative analysis between Traditional HMS and BC-based HMS. It is evident from the review and comparison that BC-based HMS can bring remarkable changes and greatly benefit society.

Table 6. Traditional HMS and blockchain-based HMS.

Key Factors	Traditional HMS	Blockchain-Based HMS
Documentation	More	Less/Not required
Data storage	Manual/Centralized	Decentralized
Data availability	Delayed	Up to date
Integrity	Less	More
Security	Less	More
Immutable records	No	Yes
Consensus	No	Yes
Single trusted record	Multiple copies	Single universal copy
Access	Internal	Anywhere
Patient-centric	No	Yes
Hash key	No	Yes
Data recovery/Backup	Vulnerable to data loss	Minimal risk of data loss

5. Critical Challenges of BC Adoption in HMS

Although blockchain is very efficient in overcoming the issues and loopholes in healthcare management systems, there are still challenges in integrating BC into HMS. There is still hesitation in adopting the BC technology by different organizations and people. Some of the critical challenges are identified and discussed below:

- **Data Storage and Scalability**

The blockchain gets heavier every day as a result of the rising transaction volume. The network may have fewer nodes with sufficient processing capacity to handle and validate data on the blockchain as a result of the increased storage and computational power demands. However, large block sizes could slow down propagation and result in blockchain branches. Therefore, voluminous data storage and scalability are challenging issues [1].

- **Data Access and Reliability**

The decentralized idea of BC has both strengths and weaknesses. A decentralized network avoids the risk of a single point of failure, but still, the blockchain suffers from data access and reliability issues. It is because some blockchain characteristics leave BC vulnerable to a digital attack. As a result, one of the key challenges in blockchain is data access and reliability [4,75].

- **Privacy and Security**

Encryption provides protection and security, but healthcare stakeholders still believe the accessibility of a database, even in encrypted form, is a critical problem. Therefore, in the context of blockchain, it is crucial to managing access control appropriately [17]. Healthcare information is acquired from several stakeholders, which may result in unintentional invasions of protection, privacy, and security. Therefore, it is necessary to analyze and foresee the information before granting access control [4,49].

- **Complex Decentralized Architecture**

Since blockchain combines complex technologies, it is tough to adapt to working on blockchain frameworks. In addition, medical services, doctor suppliers, and insurance payers still rely on paper-based records rather than electronic medical records, so adapting the blockchain framework is challenging [68]. It is exceptionally hard to arrange every one of these elements to receive blockchain as an innovation [4].

- **Lack of Legislative Standards**

For the blockchain-based healthcare system to function, both public and private blockchains must be interoperable. This highlights the requirement for internationally coordinated standards and agreements that span national boundaries and jurisdictions [17]. Numerous associations, such as IEEE and ITU, are attempting to deliver new BC innovation norms that are yet to be finalized. Various tasks are going on in blockchain principles by IEEE to make blockchain usage for the future; however, it requires legitimate rules, laws, guidelines, and approaches [4,9].

- **Ownership and Governance**

The development of suitable rules for global governance rights of ownership relating to medical transactions for the blockchain-based healthcare system is challenging. It will be hard to convert the current regulatory framework to the new administration's policy objectives managing blockchain's digitally documented, automated, and ubiquitous nature. Careful clarification is required on the ownership of records, access privileges granted, and distributed storage architecture of blockchain [17,86].

- **Operational Cost Constraints**

The costs of establishing and operating a digitized system, as well as the transition from conventional health information systems, are not fixed. It is still not conceived well that an open-source technology and the distributed nature of blockchain can help lower them. The healthcare system based on the blockchain requires constant availability of resources for troubleshooting, upgrading, backup, and reporting purposes. Thus these systems suffer from constraints of operational costs [17,86].

- **Lack of Adoption**

In order to provide the necessary computational power for both creating blocks of a transaction and cryptocurrency, blockchain technology needs a network of connected computers. Through incentive systems, participants should be motivated to contribute to computer power. Additionally, it might be necessary to motivate health organizations to use blockchain technology and join the shared network. As more entities participate, the influence of blockchain will grow [17].

- **Transparency**

Blockchain technology emphasizes transparency, which may not always be desirable in the healthcare industry. The data replicated on various nodes becomes transparent and could be accessed maliciously by participating nodes. Since healthcare data are critical in nature, sometimes this exposure of sensitive information conflicts with the organization's policies and individuals' interests. Transparency of data on BC is one of the major reasons for the hesitant adoption of BC. Additionally, access to all data pertaining to a user is made possible by hacking or acquiring the user's secret encryption key [17].

- **Selfish Miners Attack**

The blockchain is vulnerable to attacks from selfish, complicit miners. Selfish miners hold their mined blocks without broadcasting them, and the public is only made aware of the secret branch if certain conditions are met. All miners would accept the private branch because it is longer than the current public chain. Sincere miners are spending their time on a pointless branch prior to the private BCs release, while selfish miners are mining their own secret chain without interference. Thus, selfish miners typically earn more money. Selfishness might easily reach 51% power as rational miners would be drawn to join it [1].

6. Conclusions and Future Work

The objective of the study was to present all pervasive views of blockchain technology and its adoption in healthcare, along with its challenges, comparisons, and solutions.

A detailed comparison of the proposed work with existing literature has been made on various vital points: diverse domains, healthcare focused, blockchain technical features, development frameworks, challenges in blockchain, comparative analysis, and proposed solution taxonomy. The findings of the research identified challenges and security loopholes in the existing healthcare management systems. There have been many security and privacy attacks over the years in the healthcare systems that have been studied. The most significant cyberattacks and their impact have been summarized in the paper. The present study concludes that there is a dire need for a more secure and efficient technology for building healthcare management systems. Thus, it can be concluded that blockchain is an innovation that can resolve the prevailing challenges in healthcare and has great potential. Blockchain technology has been explained from every view through its essential features, architecture, diverse applications, and adoption in healthcare. To resolve these issues and challenges, a solution taxonomy is proposed that is divided into four components. The first component creates the block, and patient identity is generated in the second component; the third component deals with interoperable data management, and the fourth component handles the consensus and maintains security levels of encrypted data. In addition, a comparative analysis has been performed on various development frameworks for blockchain prototype implementation. This paper also compared traditional and blockchain-based healthcare management systems, highlighting the benefits of blockchain technology, such as decentralized data storage, immutability, robust security, consensus, and many more. At last, the paper concluded with the identification of some of the critical research challenges, such as scalability, complex architecture, governance issues, lack of legislative standards, and adoption in blockchain technology implementation for further scope. These critical challenges must be addressed and researched in the future for the betterment of healthcare services in society.

Author Contributions: Conceptualization: W.-C.H., D.S. and S.T.; writing—original draft preparation: S.M. and D.S.; methodology: S.M., R.S. and S.T.; writing—review and editing: W.-C.H. and S.T.; visualization: S.M., R.S., S.T. and Y.-L.H.; software: S.M., D.S. and Y.-L.H.; investigation: W.-C.H., D.S., S.M. and S.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received a sponsorship from the National Science and Technology Council, Taiwan (MOST 111-2410-H-161-001), and Far Eastern Memorial Hospital Industry-Academy Cooperation Project (FEMHIACP-111-0001).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

List of Abbreviations

Abbreviation	Meaning
HIT	Healthcare Information Technology
IoT	Internet of Things
SC	Smart Contract
BC	Blockchain
EMR/EHR	Electronic Medical/Health Records
HMS	Healthcare Management Systems
ICT	Information Communication Technology
HIS	Hospital Information System
HMIS	Healthcare Management Information System
RPMS	Remote Patient Monitoring System
IBTS	Internet-Based Telesurgery System
MHS	Mobile Healthcare System

References

1. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [CrossRef]
2. Sadiku, M.N.O.; Eze, K.G.; Musa, S.M. Blockchain Technology in Healthcare. *Int. J. Adv. Sci. Res. Eng.* **2018**, *4*, 154–159.
3. Suhasini, M.; Singh, D. Blockchain Based Framework for Secure Data Management in Healthcare Information Systems. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 16933–16946.
4. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
5. Lewis, R.; McPartland, J.; Ranjan, R. Blockchain and financial market innovation. *Econ. Perspect.* **2017**, *41*, 1–17.
6. Chen, W.; Xu, Z.; Shi, S.; Zhao, Y.; Zhao, J. A Survey of Blockchain Applications in Different Domains. In Proceedings of the ICBTA, Xi'an, China, 10–12 December 2018; ACM: San Francisco, CA, USA. ISBN 978-1-4503-6646-5/18/12. [CrossRef]
7. Hathaliya, J.J.; Tanwar, S.; Tyagi, S.; Kumar, N. Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach. *Comput. Electr. Eng.* **2019**, *76*, 398–410. [CrossRef]
8. Faujdar, D.S.; Sahay, S.; Singh, T.; Jindal, H.; Kumar, R. Public health information systems for primary health care in India: A situational analysis study. *J. Fam. Med. Prim. Care* **2019**, *8*, 3640–3646. [CrossRef]
9. 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 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
10. Gupta, R.; Thakker, U.; Tanwar, S.; Obaidat, M.; Hsiao, K.F. BITS: A Blockchain-driven Intelligent Scheme for Telesurgery System. In Proceedings of the 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), Hangzhou, China, 5–7 October 2020; pp. 1–5. [CrossRef]
11. Hathaliya, J.J.; Sharma, P.; Tanwar, S.; Gupta, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. In Proceedings of the IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India, 13–14 December 2019; pp. 87–91.
12. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
13. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
14. Gupta, D.D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **2018**, *3*, 1–17. [CrossRef]
15. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access* **2019**, *7*, 176935–176951. [CrossRef]
16. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
17. Gökalp, E.; Gökalp, M.O.; Çoban, S.; Eren, P.E. Analysing Opportunities and Challenges of Integrated Blockchain Technologies in Healthcare. *Eurosymp. Syst. Anal. Des.* **2018**, *11*, 174–183.
18. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef]
19. McGhin, T.; Choo, K.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
20. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
21. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
22. Soni, S.; Bhushan, B. A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications. In Proceedings of the 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; pp. 922–926.
23. Rouhani, S.; Deters, R. Security, Performance, and Applications of Smart Contracts: A Systematic Survey. *IEEE Access* **2019**, *7*, 50759–50779. [CrossRef]
24. de Aguiar, E.J.; Faiçal, B.S.; Krishnamachari, B.; Ueyama, J. A Survey of Blockchain-Based Strategies for Healthcare. *ACM Comput. Surv. CSUR* **2020**, *53*, 1–27. [CrossRef]
25. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
26. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.A. Systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
27. Durneva, P.; Cousins, K.; Chen, M. The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review. *J. Med. Internet Res.* **2020**, *22*, e18619. [CrossRef]
28. Chukwu, E.; Garg, L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access* **2020**, *8*, 21196–21214. [CrossRef]
29. Tandon, A.; Dhir, A.; Najmul Islam, A.K.M.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
30. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. *Int. J. Healthc. Manag.* **2020**, *15*, 70–83. [CrossRef]

31. Abu-elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. *Int. J. Med. Inform.* **2020**, *142*, 104246. [CrossRef]
32. Gaynor, M.; Tuttle-Newhall, J.; Parker, J.; Patel, A.; Tang, C. Adoption of Blockchain in Health Care. *J. Med. Internet Res.* **2020**, *22*, e17423. [CrossRef] [PubMed]
33. Song, J.; Zhang, P.; Alkubati, M.; Bao, Y.; Yu, G. Research advances on blockchain-as-a-service: Architectures, applications and challenges. *Digit. Commun. Netw. DCN* **2021**, *8*, 466–475. [CrossRef]
34. Saeed, H.; Malik, H.; Bashir, U.; Ahmad, A.; Riaz, S.; Ilyas, M.; Bukhari, W.A.; Khan, M.I.A. Blockchain technology in healthcare: A systematic review. *PLoS ONE* **2022**, *17*, e0266462. [CrossRef]
35. Guntur, L.N.; Dornadula, G.; Nimbagal, R.N. Blockchain Technology: A Breakthrough in the Healthcare Sector. In *Transformations Through Blockchain Technology*; Idrees, S.M., Nowostawski, M., Eds.; Springer: Cham, Switzerland, 2022; pp. 137–160. [CrossRef]
36. Alhadhrami, Z.; Alghfeli, S.; Alghfeli, M.; Abedlla, J.A.; Shuaib, K. Introducing Blockchains for Healthcare. In Proceedings of the International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, UAE, 21–23 November 2017; IEEE: New York, NY, USA, 2017.
37. Sun, J.; Yan, J.; Zhang, K.Z.K. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financ. Innov.* **2016**, *2*, 26. [CrossRef]
38. 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. [CrossRef]
39. Monga, S.; Singh, D. A Blockchain Solution for Secure Health Record Access with Enhanced Encryption Levels and Improvised Consensus Verification. In *IOT with Smart Systems. Smart Innovation, Systems and Technologies*; Choudrie, J., Mahalle, P., Perumal, T., Joshi, A., Eds.; Springer: Singapore, 2022; Volume 312. [CrossRef]
40. Bodavala, R. Evaluation of Health Management Information System in India Need for Computerized Databases in HMIS. Available online: https://cdn1.sph.harvard.edu/wp-content/uploads/sites/114/2012/10/rp176.pdf (accessed on 21 July 2022).
41. Boulos, M.N.K.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*, 25. [CrossRef] [PubMed]
42. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Sadoun, B. HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0. In Proceedings of the International Conference on Computer, Information and Telecommunication Systems, CITS, CITS, Beijing, China, 28–31 August 2019; pp. 1–5.
43. The Future of Blockchain: Applications and Implications of Distributed Ledger Technology, Charter. Account. Available online: https://charteredaccountantsworldwide.com/the-future-of-blockchain/ (accessed on 21 July 2022).
44. Risius, M.; Spohrer, K. A Blockchain Research Framework. *Bus. Inf. Syst. Eng.* **2017**, *59*, 385–409. [CrossRef]
45. Dinh, T.T.A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.L. Blockbench: A framework for analyzing private blockchains. In Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; ACM: San Francisco, CA, USA, 2017; pp. 1085–1100.
46. Mistry, C.; Thakker, U.; Gupta, R.; Obaidat, M.S.; Tanwar, S.; Kumar, N.; Rodrigues, J.J. MedBlock: An AI-enabled and Blockchain-driven Medical Healthcare System for COVID-19. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. [CrossRef]
47. Pereraa, S.; Nanayakkaraa, S.; Rodrigoa, M.N.N.; Senaratnea, S.; Weinand, R. Blockchain technology: Is it hype or real in the construction industry? *J. Ind. Inf. Integr.* **2020**, *17*, 100–125. [CrossRef]
48. Gupta, R.; Reebadiya, D.; Tanwar, S.; Kumar, N.; Guizani, M. When Blockchain Meets Edge Intelligence: Trusted and Security Solutions for Consumers. *IEEE Netw.* **2021**, *35*, 272–278. [CrossRef]
49. Kaushik, A.; Choudhary, A.; Ektare, C.; Thomas, D.; Akram, S. Blockchain—Literature Survey. In Proceedings of the 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017.
50. Grishin, D.; Obbad, K.; Estep, P.; Quinn, K.; Wait Zaranek, S.; Wait Zaranek, A.; Vandewege, W.; Clegg, T.; César, N.; Cifric, M.; et al. Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation. *BHTY Blockchain Healthc. Today* **2018**, *1*, 1–23. [CrossRef]
51. Guegan, D. *Public Blockchain Versus Private Blockchain*; Centre d'Economie de la Sorbonne: Paris, France, 2017; pp. 1–6.
52. Gorkhalia, A.; Ling, L.; Shrestha, A. Blockchain: A literature review. *J. Manag. Anal.* **2020**, *7*, 321–343. [CrossRef]
53. Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and 5G integrated softwarized UAV network management: Architecture, solutions, and challenges. *Phys. Commun.* **2021**, *47*, 101355. [CrossRef]
54. Kakkar, R.; Gupta, R.; Tanwar, S.; Rodrigues, J.J.P.C. Coalition Game and Blockchain-Based Optimal Data Pricing Scheme for Ride Sharing Beyond 5G. *IEEE Syst. J.* **2021**, *16*, 6321–6327. [CrossRef]
55. Gupta, R.; Bhattacharya, P.; Tanwar, S.; Kumar, N.; Zeadally, S. GaRuDa: A Blockchain-Based Delivery Scheme Using Drones for Healthcare 5.0 Applications. *IEEE Internet Things Mag.* **2021**, *4*, 60–66. [CrossRef]
56. Reinforcing the Links of the Blockchain. IEEE Future Directions Blockchain Initiative White Paper. IEEE. Available online: https://blockchainincubator.ieee.org (accessed on 21 July 2022).
57. Bethesda, D. Blockchain: The Chain of Trust and its Potential to Transform Healthcare. In *IBM Ideation Challenge—Use of Blockchain in Health IT and Health Related Research*; IBM Global Business Services Public Sector Team: Armonk, NY, USA, 2016; pp. 1–12.

58. Ivan, D. Moving toward a Blockchain-Based Method for the Secure Storage of Patient Records. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*; ONC/NIST: Gaithersburg, MD, USA, 2016.
59. Shah, K.; Chadotra, S.; Tanwar, S.; Gupta, R.; Kumar, N. Blockchain for IoV in 6G environment: Review solutions and challenges. *Clust. Comput.* **2022**, *25*, 1927–1955. [CrossRef]
60. Witchey, N.J. Healthcare Transaction Validation via Blockchain Proof-of-Work, Systems and Methods. U.S. Patent No. 10,038,340, 2 July 2019.
61. Weernink, M.O.; Engh, W.V.D.; Francisconi, M.; Thorborg, F. *The Blockchain Potential for Port Logistics*; White Paper-Blockhain: Delft, The Netherlands, 2017.
62. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
63. Lewis, A.; Larson, M. *Understanding Blockchain Technology and What It Means for Your Business*; Asian Insights Office, DBS Group Reserach: Shanghai, China, 2016.
64. Zhang, P.; Walker, M.A.; White, J.; Schmidt, D.C.; Lenz, G. Metrics for assessing blockchain-based healthcare decentralized apps. In Proceedings of the IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; pp. 1–4.
65. Efanov, D.; Roschin, P. The All-Pervasiveness of blockchain Technology. In Proceedings of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures, Moscow, Russia, 1–6 August 2017; BICA, Elsevier Ltd.: Amsterdam, The Netherlands, 2018; p. 123.
66. Bocek, T.; Rodrigues, B.; Strasser, T.; Stiller, B. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
67. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Das, G. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [CrossRef]
68. Lu, Y. Blockchain: A survey on functions, applications and open issues. *J. Ind. Integr. Manag.* **2018**, *3*, 1850015. [CrossRef]
69. Dennis, R.; Owen, G. Rep on the block: A next generation reputation system based on the blockchain. In Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 131–138.
70. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology Applications in Health Care. *Circ. Cardiovasc. Qual. Outcomes* **2017**, *10*, e003800. [CrossRef]
71. Linn, L.A.; Martha, B.K. Blockchain for Health Data and Its Potential Use in Health It and Health Care Related Research. In *Use of Blockchain for Healthcare and Research Workshop*; ONC/NIST: Gaithersburg, MD, USA, 2016.
72. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
73. Shah, K.; Gupta, R.; Agrawal, S.; Tanwar, S.; Sharma, R. Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G. *J. Inf. Secur. Appl.* **2022**, *67*, 103179.
74. Krousel-Wood, M.; McCoy, A.B.; Ahia, C.; Holt, E.W.; Trapani, D.N.; Luo, Q.; Price-Haywood, E.G.; Thomas, E.J.; Sittig, D.F.; Milani, R.V. Implementing electronic health records (EHRs): Health care provider perceptions before and after transition from a local basic EHR to a commercial comprehensive EHR. *J. Am. Med. Inform. Assoc.* **2018**, *25*, 618–626. [CrossRef] [PubMed]
75. Azaria, A.; Ekblaw, A.; Vieiro, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2nd International Conference on Open and Big Data, Vienna, Austria, 22–24 August 2016; pp. 25–30.
76. Chakarborty, S. Applications of Blockchain in Healthcare Industry. Available online: https://www.upgrad.com/blog/applications-of-blockchain-in-healthcare/ (accessed on 21 July 2022).
77. Ozercan, H.I.; Ileri, A.M.; Ayday, E.; Alkan, C. Realizing the potential of blockchain technologies in genomics. *Genome Res.* **2018**, *28*, 1255–1263. [CrossRef]
78. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef]
79. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef]
80. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MedShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
81. MedicalChain. White Paper 2.1. Available online: https://www.allcryptowhitepapers.com/medicalchain-whitepaper/ (accessed on 21 July 2022).
82. 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. [CrossRef]
83. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-Based Data Preservation System for Medical Data. *J. Med. Syst.* **2018**, *42*, 141. [CrossRef] [PubMed]
84. Gupta, R.; Patel, M.M.; Shukla, A.; Tanwar, S. Deep learning-based malicious smart contract detection scheme for internet of things environment. *Comput. Electr. Eng.* **2022**, *97*, 107583. [CrossRef]

85. Decker, C.; Wattenhofer, R. Information propagation in the bitcoin network. In Proceedings of the IEEE P2P 2013 Proceedings, Trento, Italy, 9–11 September 2013; pp. 1–10.
86. Health Informatics. Available online: https://nhsrcindia.org/health-informatics (accessed on 21 July 2022).