





Article

Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System

Faheem Ahmad Reegu ^{1,2,*} , Hafiza Abas ¹, Yonis Gulzar ^{3,*} , Qin Xin ⁴ , Ali A. Alwan ⁵ , Abdoh Jabbari ², Rahul Ganpatrao Sonkamble ⁶  and Rudzidatul Akmam Dziyauddin ¹

- ¹ Razak Faculty of Technology and Informatics, Universiti Teknologi, Johor Bahru 50480, Malaysia
 - ² College of Computer science and Information Technology, Jazan University, Jazan 45142, Saudi Arabia
 - ³ Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia
 - ⁴ Faculty of Science and Technology, University of the Faroe Islands, Vestarabryggja 15, FO 100 Torshavn, Denmark
 - ⁵ Schools of Theoretical and Applied Science, Ramapo College of New Jersey, Mahwah, NJ 07430, USA
 - ⁶ Computer Engineering, MIT Art, Design and Technology University, Pune 412201, India
- * Correspondence: freegu@jazanu.edu.sa (F.A.R.); ygulzar@kfu.edu.sa (Y.G.); Tel.: +966-545-719-118 (Y.G.)

Abstract: The healthcare industry has been transitioning from paper-based medical records to electronic health records (EHRs) in most healthcare facilities. However, the current EHR frameworks face challenges in secure data storage, credibility, and management. Interoperability and user control of personal data are also significant concerns in the healthcare sector. Although block chain technology has emerged as a powerful solution that can offer the properties of immutability, security, and user control on stored records, its potential application in EHR frameworks is not yet fully understood. To address this gap in knowledge, this research aims to provide an interoperable blockchain-based EHR framework that can fulfill the requirements defined by various national and international EHR standards such as HIPAA and HL7. The research method employed is a systematic literature review to explore the current state of the art in the field of EHRs, including blockchain-based implementations of EHRs. The study defines the interoperability issues in the existing blockchain-based EHR frameworks, reviews various national and international standards of EHR, and further defines the interoperability requirements based on these standards. The proposed framework can offer safer methods to interchange health information for the healthcare sector and can provide the properties of immutability, security, and user control on stored records without the need for centralized storage. The contributions of this work include enhancing the understanding of the potential application of blockchain technology in EHR frameworks and proposing an interoperable blockchain-based EHR framework that can fulfill the requirements defined by various national and international EHR standards. Overall, this study has significant implications for the healthcare sector, as it can enhance the secure sharing and storage of electronic health data while ensuring the confidentiality, privacy, and integrity of medical records.

Keywords: blockchain; electronic health records (EHRs); healthcare; security; privacy



Citation: Reegu, F.A.; Abas, H.; Gulzar, Y.; Xin, Q.; Alwan, A.A.; Jabbari, A.; Sonkamble, R.G.; Dziyauddin, R.A. Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability* **2023**, *15*, 6337. <https://doi.org/10.3390/su15086337>

Academic Editor: Gwanggil Jeon

Received: 6 February 2023

Revised: 15 March 2023

Accepted: 3 April 2023

Published: 7 April 2023



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

1. Introduction

Blockchain and smart contracts are expected to open up new possibilities for securing patient data that can be shared and accessed via electronic health records (EHRs). Integrating blockchain healthcare infrastructure will improve people's lives significantly [1]. EHR systems are becoming more popular as a convenient means of transferring medical data between various healthcare organizations. However, obtaining needed patient records from various EHRs is difficult since existing EHR databases are either expressly connected to a specified healthcare provider or are confined to a geographical border [2].

Blockchain-based data storage and access can help patients by allowing remote monitoring, lowering costs, and improving care outside health clinics. In a healthcare context where patient information confidentiality must be protected, the growing use of IoT devices raises various privacy and security concerns [3]. By safeguarding electronic health records via a distributed peer-to-peer connection and providing a safe solution for medical data sharing in healthcare efficiency, blockchain will revolutionize how electronic health records are exchanged and processed. The blockchain method is proposed to keep the procedure for comprehending distributed ledger technologies alive and well. Blockchain was primarily proposed as a means of storing digital records of cash-related transactions that are independent of central authorities or economic alliances [4].

Innovations have fueled this revolutionary blockchain technology to enable improved transactions, such as insurance billing, health information, and smart contracts. It provides for permanent data entry and authentication and a distributed transaction record. Data interchange, increased access to medical information, and framework monitoring will all be part of the blockchain substructure that spans a product's complete life cycle [5]. Blockchain and other developing technologies such as the internet of things (IoT) and cloud computing will be utilized to create more reliable EHR systems. IoT devices may gather various health-related data, such as that of blood pressure, blood sugar level, temperature, and ECG. Records can be stored in cloud storage for improved resource scalability and usage. The security, durability, immutability, and interoperability features of blockchain will be discussed. Blockchain is ideal for use when access to patient medication or health information is required. It will significantly improve the system of patient care services [6].

This research work combines two EHR frameworks and can result in a substantial shift in the healthcare system. The goal is to demonstrate how the HIPAA and HL7 frameworks may work together to communicate data for the betterment of health systems at a high level. The use of IoT devices is growing every day, improving people's comfort and lifestyles [7]. It is proposed that IoT devices be secured using blockchain technology to prevent tampering and illegal access. However, instead of using the Ethereum platform, this can be implemented using Hyperledger. Hyperledger does not utilize bitcoin, and transactions are private rather than public; furthermore, it has not considered approving the company that created the gadget (maker) and its users to prevent counterfeiting. Figure 1 illustrates blockchain-based patient healthcare record management [8].

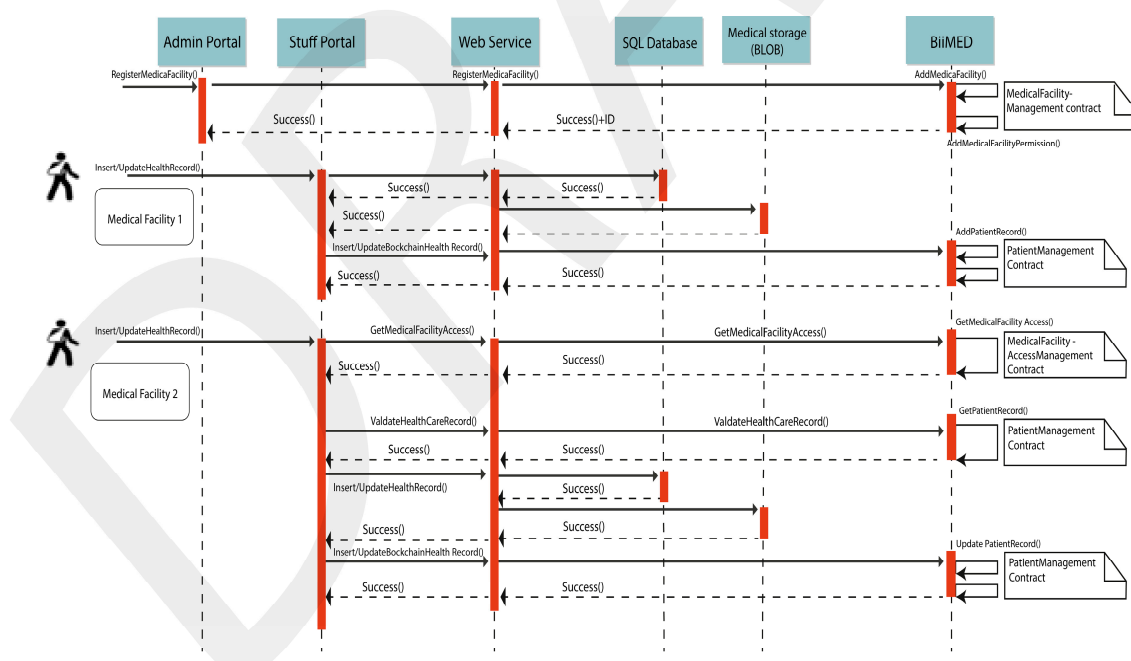


Figure 1. Blockchain-based patient healthcare record management.

The composition of this research papers is as follows. Section 2 summarizes the existing contributions in blockchain-based healthcare management system. Section 3 provides technical details of our proposed blockchain-based electronic healthcare management systems and Section 5 describes the innovative contributions of this research work and future directions.

2. Literature Review

Existing blockchain-based interoperable EHR systems and their international standards are discussed as follow.

MedRec: is a working model that attempts to obtain interoperability among providers and to grant patients more extensive and precise control over who can access their information. MedRec operates on the Ethereum blockchain and its standards treat health records as assets; smart contracts restrain access to these assets. This prototype describes medical records on-chain as generic query strings that can be executed against a provider's database to obtain the entire document. Patients can invoke these smart contracts through a user interface to restrain who can see the related records and which features of those records are viewable. Therefore, MedRec leverages the permission-less blockchain for two main objectives: providing patients with more enhanced authority over their health data and providing data to be transferred more efficiently among various providers through interoperable query strings [9].

The FHIRChain framework is blockchain-based and is designed to meet the requirements of the Office of the National Coordinator (ONC) by encapsulating the Health Level 7 (HL7) and Fast Health Interoperability Resource (FHIR) standards for the sharing of health-related data [10]. The FHIRChain provides trustless and decentralized storage for metadata and sustains data ownership by enabling the exchange of data without downloading or uploading data. Furthermore, it reduces the risks of corrupted data and ensures that the original data ownership is maintained. In FHIRChain, the reference pointers are encrypted and decrypted to provide digital identity and authentication. Once authenticated successfully, the data can be directly downloaded from the source and displayed correctly to the user [10].

The blockchain-based approach to HIE (health information exchange) provides an approach for sharing data based on blockchain. This system exchanges distinct centralized sources of trust in support of network consensus. Based on proof of structural and semantic interoperability, it predicts consensus. In this approach, the blockchain plays a crucial role in supporting data sharing and high-level protocols and structures required for applying this novel technology to healthcare. The consensus algorithm is designed to enable data interoperability. This system has applied additional security measures on the blockchain using smart contracts and network-wide keys [11].

Moreover, safety is its highest priority. Thus, blockchain-based data-sharing is the logical solution for the severe problems and issues of sharing healthcare information. The configuration of input forms in EHR systems uses spreadsheets, available EHR archetypes, and template authors. Sundvall [12] has suggested a framework facilitating the reuse of free EHR prototypes and template semantics. The proposed framework based on the spreadsheet approach will, of course, not make existing non-standardized EHR content more convenient to share in a structured form. The organizations with an already existing EHR installed will not abruptly change all configurable EHR-entry forms from non-standardized to standardize. However, they can do it incrementally with other methods, information change management, and maintenance tasks.

Ancile is a blockchain-based framework proposed to provide secure interoperability and organizes access to health records through patients, third parties, and providers while maintaining the patients' crucial data. This framework uses a smart contract, an Ethereum-based blockchain for higher access control and corruption of data which employs unconventional cryptographic techniques for enhanced security. The Ancile framework exhibits a blockchain-based system that attains higher levels of decentralization, although

acknowledging that some nodes are required to be of the highest authority. To provide significant data integrity and privacy preservation, Ancile uses smart contracts and maintains accessibility and interoperability. This framework uses specific Ethereum tools to generate storage and a cost-effective system for blockchain. The effective use of authorization and encryption determines priority of access control and security [13].

It is a framework for the redistribution and secure sharing of medical imaging data through the blockchain consensus. The blockchain framework helps abolish third-party access to secure health data and satisfy numerous norms of a practical healthcare system. The blockchain framework has been shown to generalize the various domains of healthcare systems [14]. The significant drawbacks of the framework constitute the imprecise conductive domain and the complexity of the security and privacy models. The review of the fundamental principles of blockchain technologies has enabled us to come up with an overview of blockchain implementation that can provide us with a tool to exchange information sharing without relying on a centralized authority. There are various distinctive advantages to these types of approaches. However, we have focused on how a blockchain can satisfy various requirements of an interoperable healthcare system. There are also numerous notable drawbacks to this blockchain technology. Knowing about those drawbacks and considering the advantages of the already existing options is essential before we begin large-scale blockchain implementation [15].

Blockchain technology provides a layout of an architectural model of redistributed personal healthcare data. It proposes a conceptual prototype to control the personal healthcare data obtained from numerous healthcare providers by depending on blockchain technology in a peer-to-peer network [16]. It allows healthcare providers and patients to effectively receive personal healthcare information while ensuring data security and integrity. The blockchain provides immutable data records without the need for a third party. The PHI data are obtained from a variety of healthcare providers that are all part of the same blockchain network. Our model will allow the parties to efficiently manage and collect PHI data in a single view, while also providing a reasonable guarantee of dataset integrity. Table 1 briefly explains the existing blockchain-based interoperable EHR system using EHR standards.

Table 1. Review of blockchain-based-interoperable EHR system using EHR standards.

S. No	Study	Title	Interoperable Standard
1	[17]	MedRec: using blockchain for medical data access and permission management	HL7
2	[18]	A blockchain-based approach to health information exchange networks	HL7
3	[16]	Blockchain technology for providing an architecture model of decentralized personal health information	HIPAA
4	[3]	FHIRChain: applying blockchain for secure and scalable sharing of clinical data	HL7
5	[12]	Configuration of input forms in EHR systems using spreadsheets, open EHR archetypes and templates	openEHR
6	[19]	A framework for secure and decentralized sharing of medical imaging data via blockchain consensus	DICOM

Table 1. Cont.

S. No	Study	Title	Interoperable Standard
7	[13]	Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	HL7
8	[20]	A blockchain framework for patient-centered health records and exchange (health chain): evaluation and proof-of-concept study	HL7
9	[20]	Resolving data interoperability in ubiquitous health profiles using a semi-structured approach	SNOMED CT

Notes: HL7, Health Level 7; SNOMED-CT, Systematized Nomenclature of Medicine—Clinical Terms; DICOM, Digital Imaging and Communication.

2.1. EHR Data Security Standards

(A) GDPR

The General Data Protection Regulation (GDPR) defines “personal data” as any information that can be used to identify an individual. GDPR, in theory, applies to all “controllers” and “processors” dealing with personal data, regardless of their location.

The General Data Protection Regulation (GDPR) is a data protection and privacy regulation in the European Union (EU) and European Economic Area (EEA). This regulation pertains to the transfer of personal data outside of the EU and EEA. GDPR applies to any healthcare organization or individual who collects and processes data. The general principles that safeguard data with the new GDPR are consent, purpose, data minimization, transparency, accuracy, privacy-by-design or privacy-by-default, data subject rights, retention period, accountability, security safeguards, and data breach protection [21].

(B) HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Healthcare providers must adhere to their professional code of ethics by ensuring that their patients’ secrets and privacy are upheld, which is a requirement per the Hippocratic Oath of the 4th century BC. The Nightingale Pledge circa 1893 gives information about nurses keeping their patients’ personal information confidential. Health practitioners are expected to adhere strictly to the health code of ethics, which requires them to be professionals and not reveal their patients’ private information to any third party.

Immediately after the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) was implemented, stakeholders in the health sector combined efforts to ensure that the national standards which give direction on protected health information (PHI) are adhered to. According to Soni, the term HIPAA has benefited healthcare workers when someone wants to access information from the healthcare system. HIPAA is more complicated as compared to the information collected when entering healthcare.

Through HIPAA, collection, handling, and dissemination of health information have become a simple process. It also helps limit unauthorized personnel from accessing health records, using them for financial gain, and abusing the patients in question. The HIPAA regulations enable workers to enjoy medical care benefits and employer coverage [22]. When an individual does not have coverage, their health is at risk. As per HIPAA, when an individual is fired or is seeking a new job, their insurance coverage and that of their dependents are to be maintained (Reamer, 2018). Title II of HIPAA helps improve the overall functioning of the health systems and avoid the misuse of health information for personal gain [23].

Patients always remain a point of focus in the healthcare system. Therefore, health practitioners must understand the importance of maintaining health insurance and keeping health records secure to enhance outcomes [24]. According to the United States Department of Health & Human Services (HHS), HIPAA provides guidelines for performance by health providers and volunteers. Advanced practice nurses (APNs), or health information management (HIM) practitioners, play a crucial role in improving medical outcomes [25].

More health interdisciplinary bodies should be developed since there is only HIPAA. The Health Information Technology for Economic and Clinical Health Act (HITECH) provides policies that give guidelines on health operations. Kaneko and Yuda underscored that it is essential that practitioners understand the HIPAA and HITECH policies regarding electronic health record systems and patients' medical care information [26].

HIPAA is divided into two distinct groups; that is, according to Title I and Title II. Title I enables individuals to enjoy the insurance benefits provided to them and their dependents by their new employer. HIPAA is differentiated from the Consolidated Omnibus Budget and Reconciliation Act (COBRA) because it refers to changing and transferring pension funds from one worker to another when they change jobs. At the same time, COBRA enables healthcare coverage to be maintained but under the condition that total market prices are not paid [27]. The HIPAA highlights the following advantages to the beneficiary: (1) new employers must provide coverage to their new employees and their dependents, (2) an individual can access healthcare even after losing coverage, (3) employers should not limit their employees on the number of times they should use their insurance coverage, and (4) individuals have opportunities of renewing their health insurance coverage through their new bosses. Title II is also concerned with the administrative consolidation of electronic health systems to ensure the security of personal medical information [28]. Title II protects private medical records from being handled by unauthorized personnel.

According to Title I-HIPAA, it is not a must for the employer to offer health insurance; therefore, employees are limited in healthcare coverage [29]. Employees may save time searching for jobs offering medical care insurance coverage [30]. Organizations with uninsured workers compromise their workers' health. When employees change their working environment, there is a high possibility of receiving different insurance coverage compared to their previous employer [31]. Thus, healthcare insurance may need to be in a position to dictate the quality of healthcare the beneficiary is supposed to receive, and HIPAA may not be able to bring social justice and equality in healthcare.

HIPAA restricts medical practitioners from using PHI in healthcare activities such as treatment. Authorization from the patient is required if one is to access personal and private medical records [32]. For example, a medical practitioner should give copies of the patient's medical records as requested by the patient's attorney; then, the patient must authorize it. The patient can send a signed document to the provider to show that he or she is in agreement and has authorized the provider to give out his/her medical information. HIPAA permits patients to receive accounting disclosure of their 6-year private medical records before the date of request (45CFR164.528).

HITECH contains records of every person or entity to which the patient's medical records were disclosed [10]. Before the American Recovery and Investment Act, entities covered by HITECH were not expected to provide the accounting disclosure for TPO to law enforcement agencies and national security officials. The current law requires covered entities to ensure PHI in EHRs is not disclosed, even in the cases of TPO. This law requires that the information given be dated three years before the demand for the records. In this framework we are using HIPAA and HL7 (Health Level 7) as healthcare messaging standards. HL7 (Health Level 7) is a messaging standard used to exchange clinical and administrative data between different vendors' healthcare applications, typically within an enterprise. The HIPAA (Health Insurance Portability and Accountability Act) was enacted in 1996 with the goal of streamlining healthcare transactions across enterprises while protecting patients' privacy rights.

2.2. Problems Facing the Healthcare Industry and the Use of Blockchain as a Potential Solution

The healthcare industry faces a myriad of challenges in the modern era, with one of the most pressing being the security threats posed by healthcare applications. These threats include data breaches, cyberattacks, and other forms of unauthorized access to sensitive medical information. Such security breaches can have severe consequences, including financial losses, damage to reputation, and even compromised patient health.

In recent years, blockchain technology has emerged as a potential solution to these security threats. Blockchain technology provides a decentralized, secure, and tamper-proof system for storing and sharing data. By leveraging blockchain technology, healthcare organizations can maintain secure records of patient data and ensure that patient information remains confidential and protected.

In our paper “Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications,” we discuss the various security threats faced by healthcare applications and explore how blockchain can act as a countermeasure solution. Our paper provides an in-depth analysis of the potential benefits of using blockchain technology in the healthcare industry and provides practical recommendations for implementing blockchain-based solutions.

Overall, it is clear that the healthcare industry faces significant challenges when it comes to security threats. However, with the adoption of blockchain technology, healthcare organizations can improve data security and maintain the confidentiality and privacy of patient information. Our paper provides a valuable contribution to the ongoing discussion of these issues and offers insights into how blockchain technology can be used to address the challenges facing the healthcare industry.

Certainly, in our paper “Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications,” we not only discuss the security threats faced by healthcare applications but also present a solution in the form of a blockchain-based interoperable framework.

This framework enables secure data sharing and communication between different healthcare providers while maintaining patient privacy and data integrity. By using blockchain technology, this framework can provide a transparent, immutable, and decentralized system that eliminates the need for intermediaries and minimizes the risk of data breaches and cyberattacks.

Moreover, our proposed framework allows for seamless integration with existing healthcare systems and enables the interoperability of different data formats and protocols. This interoperability enables healthcare providers to share and access patient data from different sources, regardless of the system used, improving patient care and reducing costs.

Overall, our paper highlights the various security threats faced by healthcare applications and presents a blockchain-based interoperable framework as a solution to these problems. This framework has the potential to revolutionize the healthcare industry by enabling secure and efficient data sharing and communication between healthcare providers while maintaining patient privacy and data integrity.

2.3. Issues and Challenges of Implementing Blockchain in Health Care

The healthcare industry is advancing blockchain technology, but in addition to security concerns, it also faces scalability, privacy, and regulatory issues.

Scalability: A major obstacle to the widespread adoption of blockchains is scalability. Blockchains process a predetermined number of transactions per block and have prefixed block size and block creation times. Although the transaction processing (utilization) is slow, these settings help to accomplish immutability, tamper-evident features, ledger redundancy, and decentralized verification and validation of transactions. The Ethereum platform, for instance, only handles 15 transactions per second. Additionally, blockchains keep a growing ledger starting with the first (genesis) block (for instance, the size of the Ethereum full node sync is now 1+ terabytes and growing 5). The participant nodes in the blockchain network all have access to the ledger. As a result, each node needs a lot of network and storage space to store the ledger.

Privacy: Permissionless blockchains are by their very nature insecure. In permissionless blockchains, the ledger is distributed among network nodes and transactions are made available to everyone. To track user activity and obtain private information, the attacker can use the ledger and a variety of techniques (graph analysis, social engineering, phishing, and transaction linkage). Due to the fact that blockchain applications distribute

personal information in a database that is accessible to the public, these privacy concerns are intensifying and limiting their use in healthcare applications.

Regulations: Blockchain encourages disintermediation, in which no one is in charge of offering services, controls, and related datasets. The standardization and rules for BBHAs may be overwhelmed by privacy laws, such as the Health Insurance Portability and Accountability Act (HIPPA) and the EU General Data Protection Regulation (GDPR). In accordance with the GDPR, users are the data controllers, but the immutable ledger prevents users from deleting (or updating) their data. Who should be held responsible for breaking laws and regulations is a critical problem for regulators in governance.

Another issue facing using blockchain technology in health care is the lack of technical knowledge. Not all users have access to expensive hardware and software resources, and many are not familiar with the latest technologies. This is particularly true for older individuals who may not use laptops or computers. **Government-Owned Hospitals and the Challenges of Implementing Blockchain.** Many hospitals are owned by the government, which means that the implementation of new rules requires government involvement. However, some governments are resistant to adopting new technologies, making it difficult to implement blockchain technology in government-owned hospitals. This is due to the highly decentralized, distributed ledger nature of blockchain, which does not have a central authority or third party to make decisions. Instead, decisions are made by the blockchain itself.

In addition, healthcare systems are often distributed, with hospitals located in multiple places. This makes maintaining a blockchain a difficult task. Without a streamlined system, it is nearly impossible to maintain all medical records together in order to adopt blockchain as a technology. Another challenge of blockchain is its speed. Processing speed can be slow, particularly if the network is very large. Confirmations can take a long time, resulting in slow information sharing.

While blockchain technology is highly secure and does not involve third parties, there are still many potential attacks that can occur, such as 51% attacks doubling spending, and Sybil attacks [33]. Hackers often target users' wallets in order to steal money. In addition, some hackers may try to increase their incentives by mining unnecessary blocks and increasing traffic on the network.

Sybil Risk: The Sybil attack is a P2P network attack in which the attacker connects with victim nodes using a variety of false identities in order to isolate them from other trustworthy nodes [25].

Double Spending Risks: The practice of the same transaction occurring more than once is known as double-spending. Similar to this, an attacker can change the transaction state and make the same transaction twice in blockchain-based healthcare applications [34].

2.4. Benefits of Blockchain in Health Care: Ontological Representation of Healthcare Application Security Using Blockchain Technology

Data tampering, data theft, improper handling of medical records, counterfeit drugs, and man-in-the-middle attacks are some of the security threats in traditional health applications. Blockchain-based features and countermeasures can be used to overcome such threats.

Traditional healthcare applications do not give healthcare organizations much control over patient data security, which is a major worry. By design, blockchain has several controls that can minimize this threat. For instance, smart contract-based distributed access control limits users' access to medical data that has been stored. Fine-grained access control is made possible by powerful cryptographic primitives. A blockchain append-only structure and redundant ledger make it difficult to change or remove records.

Electronic health records contain sensitive data that attracts hackers who steal EHRs by taking advantage of flaws in traditional health applications. Blockchain-based healthcare applications, on the other hand, are secure against data theft. Blockchain operates over a peer-to-peer (P2P) network where nodes act as both servers and clients to send

and receive data instantly. This system works to prevent data from being accessed by unauthorized people.

Medical records must be kept private and secure, according to healthcare institutions. The patient's medical information is controlled and managed by the healthcare organizations in THAs, but non-relevant people can still access it. Permission settings and distributed access control are made possible by blockchain-based health applications when handling patient medical data. Additionally, during the consensus process, blockchain performs data validation before saving on the ledger.

The production and distribution of fake medicines is a widespread issue that has serious negative effects on people's health and the economy, but especially consumers. By recording each step in a log, blockchain provides a way to enable pharmaceutical traceability, real-time data access, and supply chain validation.

Man-in-the-middle attacks are becoming more prevalent in healthcare applications to obtain or alter sensitive data. IPFS, a distributed file system based on blockchain, is used to store data and create secure channels of communication. A P2P network used by blockchain makes it difficult for attackers to sniff or intercept communications [35].

2.5. Previous Frameworks That Have Been Implemented to Improve the Interoperability Problems

Many previous research studies revealed that health data interoperability remained a problem for healthcare over the past decade. Considering this, Jabbar et al. [36] discussed some valuable techniques to improve the interoperability challenges that help improve communication and enhance the ability to involve information technology in data exchange practices. Regarding this, enhancing artificial intelligence by applying digital health patterns is considered an effective technique to improve interoperability problems. Peixoto et al. [37] claimed that the involvement of technology helps to exchange patient information and assists the management in improving patient care. Moreover, the study of Hammami et al. [38] discussed the technique to increase patient data access, as this technique will make it easy for the management of healthcare to have easy access to all data in real time. According to Jabbar et al. [36], connected data-accessible tactics enable patients, healthcare providers, and caregivers to exchange health information successfully. Other than this, Y. Zhuang et al. [10] preferred to implement the prevalence of HIEs to promote interoperability in health care as this directly contributes to mitigating the issues that have been faced currently. The process of sending or receiving patients' health information through health information exchange (HIE) critically assists transfer of the patients' data to help in the information exchange process. With the help of this technique, healthcare practitioners can observe the impact of a patient's care efficiently [39,40].

FHIR is renowned broadly as the standard for integrating EHR; Google has been using it for the Cloud Healthcare API. Data Analysis from 2018 by the Centers for Medicare & Medicaid discovered that in the United States, around 32% of medical information technology inventors use 2015 FHIR-certified standards, and leading EHR corporations such as Cerner and Epic use FHIR standards to some extent. In 2019, Microsoft publicized the Azure API for FHIR. The integration of wearable information and personalized machines is also being done through FHIR standards. In 2010, a project known as SMART for FHIR intended for health applications to be used without alterations across disparate medical information systems was demonstrated within two months. SMART was implemented on FHIR for four unique EHR vendors. In 2018, the Apple Company broadcasted its version of a user-friendly personalized EHR known as Health Kit. All iPhone users can easily access it on their mobile phones and monitor themselves. They can also easily integrate information from fitness devices linked to Apple [41].

Normalizing standard-based medical data is now a significant constituent of the operative assimilation of data and phenotyping accuracy for secondary EHR data. FHIR is a nascent medical data standard for swapping medical electronic data and integrating and modeling unstructured data from an EHR for various scientific research applications. Hong N. et al. [42] conducted research to advance FHIR based on the phenotyping frame-

work of EHR for documentation of individuals suffering from obesity and its contribution to progressing other diseases from half-structured summaries of discharge supporting an “FHIR-based clinical data normalization pipeline (NLP2FHIR).” For gauging the FHIR-based EHR-phenotyping framework, a versatile-class and multi-label system of classification based on the “i2b2 Obesity” challenge task is implemented. The study’s results demonstrated that the FHIR-based HER-phenotyping method could effectively identify the obesity state and its associated diseases and effects using half-structured discharge summaries. This study has provided the initiative for refining the information linked to phenotyping portability throughout the EHR system and augmenting the interpretation of the phenotyping algorithms based on machine learning [43,44].

Sharing effectively and reusing EHRs requires technical resolutions to deal with different depictions and data models, such as domain and information models, and to permit support related to the clinical decision based on knowledge and facts. Maldonado et al. [45] developed a framework for supporting EHR interoperability for reasoning services and transformations proposed for clinical knowledge and data. The framework in this study is founded on workflows, whose principal components are refillable mappings. A platform based on the web is used to implement CLIN-IK-LINKS, which permits operators to make, alter, and erase mappings along with the definition and execution of workflows [46]. The CLIN-IK-LINKS platform permits the execution and configuration of medical data alteration workflows to adapt EHR data into EHR-semantic web standards. Hence, CLIN-IK-LINKS is a valued contributor to advancing the semantic interoperability of the mentioned EHR systems [47,48].

The review of existing blockchain-based EHRs highlights that only a few existing EHR systems have implemented the interoperability issue essential for cross-platform and multi-organization setup, even though frameworks have only partially implemented it. It only covers some aspects of interoperability defined by the EHR standards. Additionally, the implemented frameworks have considered a specific standard and need to be more generalized. There is a need to develop a new blockchain-based interoperable EHR framework that can fulfill the requirements defined by various national and international EHR standards such as HIPAA, HITECH, and HL7.

3. Materials and Methods

The proposed blockchain-based interoperable framework (BCIF-EHR) makes interoperability possible between the two frameworks HL7 and HIPAA, discussed earlier.

HL7 framework is enabled to share and fetch the data from the frameworks. It is being widely used in a considerable number of hospitals and healthcare systems. Because of its versatility and ability to communicate efficiently with patient incoming and outgoing data, it has been used extensively for the past three decades. On the other hand, HIPAA is an EHR framework having great privacy and web services features.

HIPAA is one of the most reliable and secure EHR frameworks, providing the best security and privacy for vulnerable health data. The HIPAA framework possesses a separate user privacy layer that keeps the patient data within limits, making it easier to process and share data among the frameworks. HIPAA is the best framework to provide web services as it has a dedicated web services layer. It is also a huge benefit to our proposed framework as it changes many things while dealing with the web systems in healthcare. The best part of the HIPAA framework is ensuring that the data sent to the HL7 framework must be transported securely. This is the point where the transport security layer of the HIPAA framework comes into play. It provides us with the ultimate data security and reliability while sharing data with other frameworks; hence, the interoperability of the two proposed frameworks becomes technically possible.

A framework is developed to address the challenges in electronic health record systems, named the BCIF-EHR blockchain interoperable framework. The framework aims to improve cooperation between different blockchain-based healthcare entities such as hospitals, clinics, and insurance companies. The BCIF-EHR framework allows for seamless

data sharing and integration. However, the framework places a focus on protecting patient data, particularly the privacy and security of electronic health records.

There is much research going on in the interoperability domain [13,40]. It is very crucial in the exchange of EHRs between two blockchain platforms. There are various challenges in such EHR exchanges.

1. There is a unique transaction format for every blockchain;
2. There can be various EHR standards for every system [13,49];
3. There are different ways to transfer data from one blockchain platform to another [47].

We have proposed a patient-centric system, where patients will control access to EHRs. In the architecture, we have assumed that the EHR system is on two different platforms in different hospitals. Every healthcare stakeholder should register in either of the systems using a smart contract/chain code. The doctor concerned should consult the respective patient and should upload the EHR. The EHR will be hashed, and its hash value will be stored in the blocks. This EHR will be allocated to the patient indicating the ownership. We have proposed partitioning of the EHR as offline and online. In online uploading of data, the patient's identity attributes will be stored, which will be mapped with offline data. Offline data can be uploaded on any document-oriented database. If any stakeholder of same system wants access to the EHR, then its consent will be sent to the patient. The patient may decide to whom and to what extent the EHR data are to be shared [50].

3.1. Proposed Approach

We have proposed hash-lock based mechanism for our system. In case the EHR is to be accessed from another platform, then this mechanism is used. For our better understanding, let us assume we have systems A and B. If any stakeholder from B wants to have access to A's patient EHR, then a hash lock is generated for the related EHR. That hash lock is shared with B's stakeholder. Then, the stakeholder from B can have access to the EHR. Figure 2 shows the blockchain-based electronic health record sharing framework.

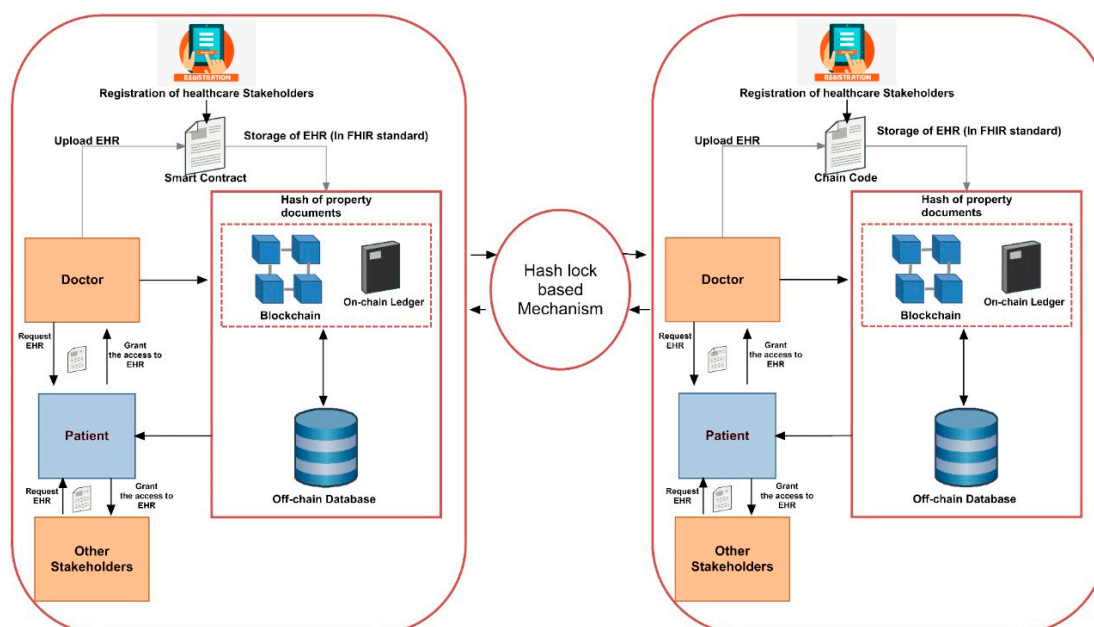


Figure 2. BCIF-EHR-Based Electronic Health Record Sharing Framework.

The framework involves three main parties: the patients, the healthcare providers, and the government agency issuing and managing the electronic health records. When a patient receives healthcare services, the patient is at the center of the process and can manage their electronic health records using digital wallets and user agents. They have complete control over their data, including electronic health records represented by virtual certificates.

Healthcare providers using traditional methods must be provided with the entire electronic health record to validate the information. Health data are stored as off-chain and on-chain. Off-chain data are the data which are stored in form of document-oriented databases. On-chain data are data with identity attributes along with the hash of whole health data.

The proposed BCIF-EHR blockchain-based interoperable framework employs cloud agents and wallets for storing electronic health records, making the records more accessible, and securing communication with other healthcare entities. The framework also uses blockchain technology to store electronically verifiable information, maintain public signing keys, and store the schemas of electronic health record virtual certificates for authenticity. Revocation data are also kept on the blockchain for public verification of the privacy-preserving nature of the data. Government agencies use institutional agents specifically designed for issuing and managing electronic health records, and also verify the authenticity of electronic health records and engage with patients and healthcare providers during and after the healthcare process.

3.2. Phases of Electronic Health Record System Using BCIF-EHR

The fundamentals of the BCIF-EHR idea are qualifications, which are a collection of assertions made by an issuer regarding a patient. Medical histories, prescriptions, test results, and digital badges are all considered credentials under this criterion. The BCIF-EHR strategy relies on standards, cryptography, distributed ledgers, and front-facing apps that enable computers to validate credentials as opposed to the common practice of using humans to do so.

3.2.1. Roles and Relationships

There are four critical roles played within the BCIF-EHR system. Firstly, the patient performs a critical task in the exchange of information that can be verified. Secondly, in the BCIF-EHR environment, the issuers are the entities, such as clinics, healthcare institutions, and insurance firms, which create credentials that can be validated. The relying or validating entity is also the medical service provider and is usually concerned with validating the originality of the credentials received. Finally, the information registry/recorder are frameworks that monitor the information required to validate a given credential.

A valid information issuer releases information regarding a specific patient upon receipt of the data from the subject. The patient presents credentials for verification. The medical care provider verifies the information utilizing a standardized verification method by amalgamating the credentials with valid data records, such as the one that contains the issuers' cryptographic keys. This allows the regulator to conduct his role without necessarily having to have the medical care provider contact the issuer for verification.

3.2.2. Scenario 1: Registration Phase

Patients and healthcare professionals without a BCIF-EHR agent, digital wallet, or any virtual certificates must register to use the electronic health record (EHR) system. In this case, UML sequence diagrams are used to illustrate the process. The BCIF-EHR framework requires a government agency to perform a one-time bootstrapping step before registration may be allowed. In this process, a distributed ledger is used to store a public digital identity and an accompanying DID document. This makes it possible for patients and healthcare professionals to access and exchange their electronic health records safely and quickly. Figure 3 shows a sequence diagram for registration phase.

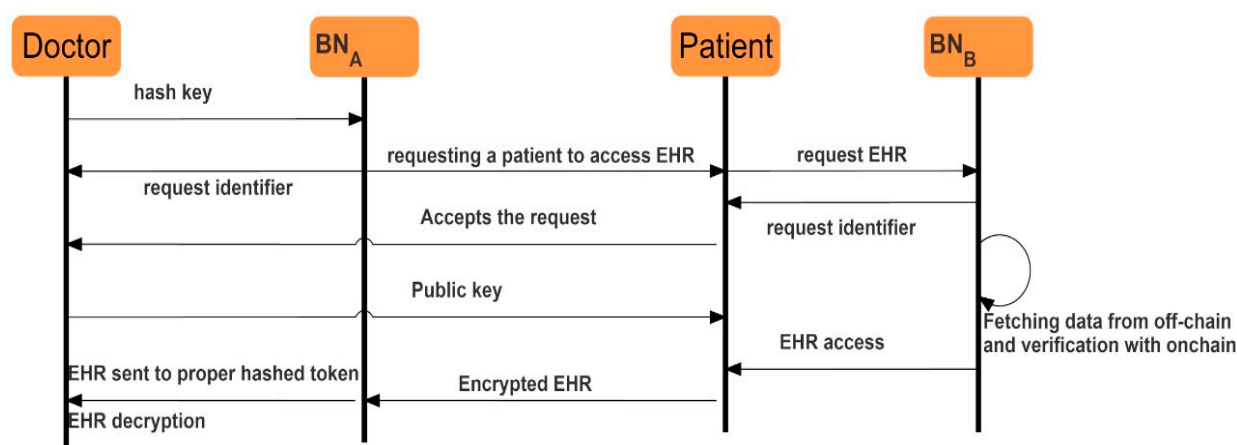


Figure 3. Sequence diagram for registration phase.

Patients can exchange electronic medical records by using laptops or smartphones to access public agency websites, or by visiting a nearby branch. Patients create a secret link that connects different credentials in an online certificate, preventing future partisan information exchange. Patients can use the generated public digital identity to establish an encrypted link with the government entity and complete the electronic health record exchange process. To complete the process, the subjects connect to the electronic health record cloud agent and scan their wallet apps. When a new public digital identity is created, the electronic health records endpoint sends a linkage request to the government agency. A linkage response is sent to the wallet of the government agency. At this point, the government agency has a secure connection with the patient, allowing the patient to securely share information. Because they do not have virtual certificates, the patients provide the necessary information about their identities to the government agency in order for their identities to be verified. Once patients open accounts, government agencies can verify their physical identification information. The government can deliver the information to the patient after validating the information and identifying the patient. The information delivered includes the expiry date, a summary of the information to be accepted, and the terms and conditions for revocation of the credentials.

While ensuring data security and integrity, this allows patients and healthcare providers to effectively receive personal healthcare information. Without relying on a third party, the blockchain provides immutable data records. The PHI data are gathered from various healthcare organizations connected by a blockchain. Our model will give the parties a single, highly effective view to manage and collect PHI data and a reasonable assurance of the datasets' integrity. This connection request contains the pairwise DID of the government organization, the healthcare provider's public key, as well as the service endpoint that the patient or owner can use to make contact with the organization. The patient's or owner's digital wallet then verifies the connection and generates a pairwise DID and keys for the government organization. The government agency's cloud agent/wallet receives the connection response and sends it on to the interface. The patient/owner can now securely exchange messages, public keys, VCs, and VPs with the government agency thanks to their encrypted end-to-end link. The patient/identity owner's must be confirmed because they haven't yet received any VCs. The patient or owner gives the government agency the necessary physical identification information on paper, by scanning it and sending it that way via email or a newly created link. These physical identity data and medical records can be verified directly at a government agency branch if the patient/owner opens an account. Following data and patient/owner identity verification, the government agency can send a credential offered to the patient/owner edge user agent. This credential offer also includes a preview of the data to be attested, as well as the credentials' expiration dates and revocation information. It is then sent to the government agency in blinded form, along with the link secret. This certificate allows for selective disclosure. This means that

the patient/owner can combine claims from multiple VCs and only include the VC-attested attributes that the verifier requires.

3.2.3. Scenario 2: Pre-Agreement and Verification

Healthcare providers and patients who aspire to share their electronic health records during the pre-contract stage are required to generate a pairwise public digital identity to deliver a request to the BCIF-EHR government agency.

At this point, the patient and the government agency have a secure and tamper-proof connection that can be utilized to share information, VCs, public keys, and VPs. Patients send the required public digital identity of the electronic health records to the government agency for validation utilizing their online wallet. Once the patient's identity is verified, the government agency's BCIF-EHR online entity publishes the EHR sharing requisition in the data records.

Healthcare providers can utilize smart devices to identify patients' EHRs in the government agency's online portal or by visiting a physical facility to personally identify the required EHR. After viewing the patient's electronic health records, the healthcare provider sends validation requests to the BCIF-EHR online government agency, which checks the validity of the credentials connected to the virtual certificates and gives the patients the required evidence of non-cancellation. Healthcare providers can release a credential provided to the patient as per the created linkage once the BCIF-EHR online agent deems the EHR validation process to be complete.

After reviewing the patient's electronic health records, the healthcare provider will submit a verification request to the BCIF-EHR cloud agent, who will then evaluate the accuracy of the VPs associated with the VC and provide consumers with the necessary proof of non-revocation. When the BCIF-EHR cloud agent determines that the EHR verification status is satisfactory, the healthcare provider can send a credential offer to the patient/owner end user agent using the established connection. This credential offer contains a preview of the data that will be confirmed, such as information about the credential issuer, the VC's expiration date, and credential revocation information. The patient/owner then confirms and sends the credential offer to the BCIF-EHR cloud agent. It will also include the credential issuer's identity, the VC's expiration date, and information about its revocation in this pre-agreement share request to the ledger.

3.2.4. Scenario 3: Bank Fund Transfer and Certificate Generation

While the pre-contract demand to share the electronic records is updated in the database, the government agency BCIF-EHR online entity informs the patient/healthcare provider online agent about the EHR sharing process. Upon being notified by the government agency, the healthcare provider sends a valid request to allow the government agency to access the EHR. Figure 4 depicts the process sequence for bank fund transfer and certificate generation.

A funds transfer request containing the public digital identity of the EHR is sent by the government agency's online entity. Upon the effective settlement of the funds, the healthcare provider's online agent submits the virtual certificate of funds transfer and settlement information. Additionally, the government agency notifies the patient as well as the healthcare provider's online agents concerning effective EHR sharing and submits the virtual certificates containing information about the government agency's online portal.

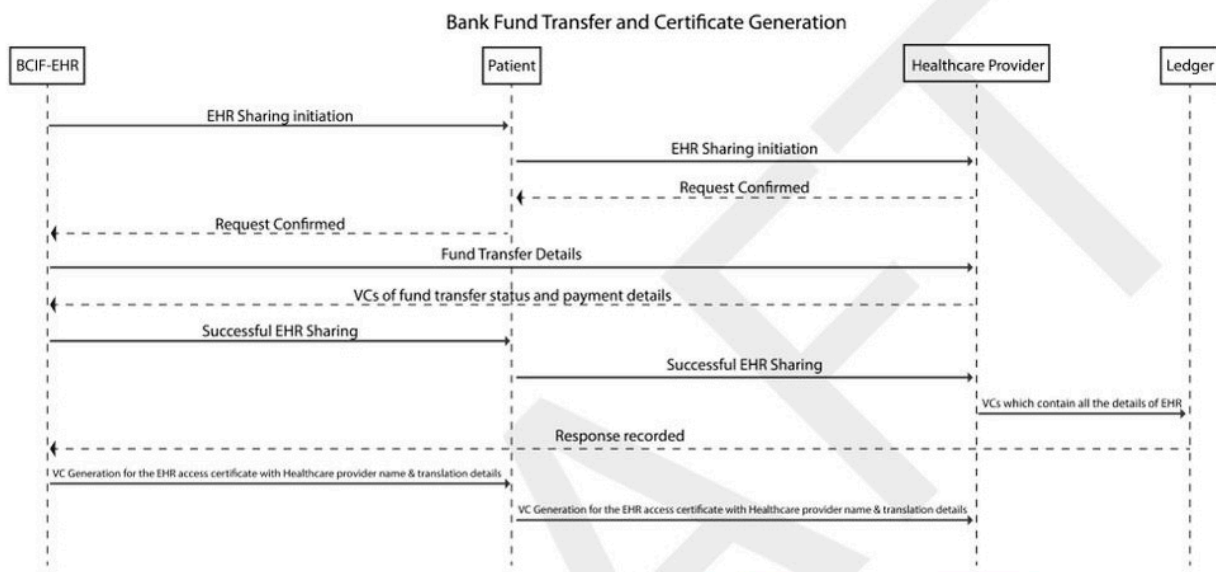


Figure 4. Bank fund transfer and certificate generation.

3.2.5. Scenario 4: Health Record Exchange between Two Hospitals

In this scenario, a patient is registered in hospital H_A , having blockchain BN_A . There is another hospital H_B with a BN_B blockchain network. If any healthcare stakeholder from H_B wants to have access to the health record of a patient from H_A , then BN_B will use a hash key which will be agreed by BN_A . Until and unless there is a lock on the health record BN_B can have access to that health record. The same process will apply if H_A wants to have access to the health record of H_B .

3.3. Tools and Techniques

Blockchain technology was implemented with all its necessities and regulations to make the two frameworks interoperable. Blockchain technology helped us to achieve heterogeneity in the two interoperable frameworks, HL7 and HIPAA, where the data is synced together and can be accessed by either framework. Users can add new patients and update each patient on the framework heterogeneously. The proposed technique was developed to assist software architects and analysts in adhering to health informatics standards throughout the development of healthcare projects. The method is built into a TIBCO plugin that supports both the HL7 and HIPAA frameworks. The technique formalizes and automates data sharing across the two heterogeneous frameworks. It includes tool modifications for detecting and producing those profiles and examples of applying them to the proposed framework.

Aside from the apparent benefit of automatically producing implementation components from UML analysis classes, the proposed technique could help develop HL7 implementation frameworks for various technologies. Each HL7 class (idea) can include EJB, CORBA, or NET components that adhere to the HL7 semantics (class types, entities, data types). Furthermore, behavioral components (e.g., control classes in the example) that manage any HL7 message utilizing the existing HL7 XML schema definition (XSD) documents may be readily developed using the same model-driven methodology. Harmonizing other health informatics standards outside of the HL7 specifications and their incorporation into the development process is still an issue that may be overcome using a similar method. The formalization of model transformations and mappings will require more investigation. It entails checking the model transformation's syntactic and semantic correctness concerning the standards. Table 2 provides implementation details of BCIF-EHR.

Table 2. Implementation details of BCIF-EHR systems.

Sr No.	Step	Summary
1	Review of health policies and EHR development.	Study of the guidelines related to the health policies in EHR frameworks.
2	Meta-analysis guidelines and systematic review.	To identify the use and application of blockchain-based technology in electronic healthcare systems.
3	Review of blockchain technology.	To identify the pros and cons of blockchain technology in EHR frameworks.
4	I am using a public blockchain.	To study how blockchain technology allows controlled access to public health-related data.
5	Review of EHR adoption.	Study the flow and growth of EHR-based systems in health care.
6	Review and implementation of security techniques in EHR frameworks.	Study the advanced security techniques used in the EHR frameworks and choose the best.
7	Previous work in EHR interoperability.	To review the previous efforts to achieve interoperability between EHR frameworks.
8	Scope of EHR interoperability.	To study the whole scenario to forecast the future scope of interoperability in EHR frameworks.
9	Effective interoperability framework.	EHR networks established and maintained at regional and national levels worldwide provide effective and standard access to and operational use of large amounts of health data.
10	Blockchain-based framework.	Smart techniques are utilized in an interoperable blockchain-based EHR architecture for mystification and knowledge control, with the sophisticated methodology used for additional security.

3.4. Data Duplication

The abovementioned diagrams clarify the workflow of the two proposed architectures and make them interoperable using blockchain technology. To make these two frameworks interoperable, data duplication is performed. This means that a copy of the data would be kept, which could be shared if any need arises. Data quality may appear to be a dry or even dull topic. However, as we have seen, data duplication in the medical setting may quickly escalate from a minor irritation or expense issue to a potentially life-threatening situation. Hospitals are steadily improving their condition as they implement EHR systems, but this is not a silver bullet in and of itself.

The data management business has a long history of detecting duplicate customer records and assisting in matching and merging such information so that technology may help. Deterministic matching checks for duplicates using standard identifiers such as first and last name, date of birth, address, and phone number; a unique patient record number is ideal for such an approach, but duplicates may be missed in the absence of one, as no single field may be able to provide a reliable match between records. Algorithms are used in probabilistic matching to determine the likelihood of matches. Field by field, two records are compared, and each record is given a weight that reflects how closely the fields match. For specific data items, rules-based algorithms use predefined confidence bounds. Data quality systems may combine these diverse techniques to discover potential instances of duplicate medical records. Table 3 provides detailed comparison of proposed framework with existing contributions.

Table 3. Comparison of BCIF-EHR with existing frameworks.

Reference	Individual EHR Frameworks	Proposed Framework
[51]	The “EHR system functional model (EHR-S FM)” is HL7. It enumerates the essential functions and applications that must be governed in an EHR system. Through the creation of practical profiles, this approach provides a consistent description and comprehension of procedures in medical-care settings. It provides a framework for driving high-standards requirements and requests and a standards-based approach for implementing functions linked to care settings and priorities. Every state utilizes it.	Because the EHR/EMR and analytics software will automatically acquire and analyze data from other systems, the interoperable framework can minimize time-consuming and duplicate activities. According to InstaMed’s tenth annual report, 87% of clinicians still collect patient data using paper and manual methods. This leads to a slew of laborious duties for medical personnel and a significant chance of medical record mistakes.
[52]	Through investing in medical information technology, the HITECH Act intends to improve the method by which services are given to patients. It encourages healthcare providers to adopt electronic health records (EHRs) to protect patients’ data privacy and security. There will also be consequences for breaking security and privacy standards.	Organizations can increase communications with other medical institutions by establishing EMR/EHR interoperability. Clinics, for example, can submit queries to pharmacies and obtain e-prescriptions. Furthermore, by making their systems more accessible to data exchange, healthcare institutions will be able to fill in information gaps more rapidly, giving them a fuller picture of the patient’s status. Accessing a patient’s longitudinal health data from other healthcare institutions is feasible thanks to EMR interoperability, which eliminates the need for lengthy phone calls, emails, and faxes.
[53]	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) guarantees that patients can access personal health information. The HIPAA Security Rule was also developed to require specified protections to safeguard patients’ electronic health information. Providers must comply with the Security Rule and take particular steps to protect protected health information.	A platform that complies with EHR interoperability requirements can improve your hospital’s patient experience. Health records can follow patients throughout healthcare systems because of interoperable EHR platforms. People may readily access their medical history and exchange it with new doctors, in other words. People do not have to redo diagnostic procedures or offer details about prior treatments to each new doctor if they use this technique. They also benefit from a better-coordinated, accurate, and efficient healthcare experience.
[54]	The HL7 consolidated CDA (C-CDA) is an implementation guideline that specifies a template library and proposes how to use it to gather specific documents.	Due to EHR interoperability difficulties with new software, many healthcare providers must reformat and transfer whole datasets, modules, and processes to another platform when updating. This makes the upgrading procedure both time-consuming and costly. EMR interoperability, on the other hand, may help you save money since it makes your platform compatible with new tools and software modules.
[55]	The open standard specifies how health data are managed, collected, recovered, and shared in electronic health reports (EHRs). The name of a new e-health tool consists of exposed particularizations, clinical software, and models that may be used to create standards and information with medical-care interoperability solutions.	Many healthcare providers must reformat and move whole datasets, modules, and procedures to another platform when updating their EHRs due to interoperability issues with new software. As a result, the upgrade method is both time-consuming and expensive. On the other hand, interoperability with EMR tools and software modules will help to save money by making the platform compatible with new tools and software modules. As a result, the increased capabilities of the system will outperform with fewer resources.

Table 3. Cont.

Reference	Individual EHR Frameworks	Proposed Framework
[56]	The OWL is used to solve various informatics problems and terminologies related to the definition and provenance of variables for qualitative reporting from EHR data. It has a defined meaning, is reusable, and allows for distributed web-based healthcare data processing.	Consider having a comprehensive picture of a patient's medical history, including care preferences, previous interactions, pictures, scans, and treatment outcomes. If providers can acquire and evaluate required data promptly, many misdiagnoses can be avoided. Access to EHR and EMR systems from other healthcare facilities allows clinicians to have a more holistic understanding of the patient's medical history and make more educated and accurate treatment decisions.
[57,58]	SNOMED-CT is a common therapeutic phrase, with "multilingual translation" receiving special attention. It is used in roughly fifty states. SNOMED-CT intends to provide EHR more significance by allowing for the operative and significant representation of healthcare data. It is critical in global efforts to offer patients affordable and high-quality healthcare.	Repeat testing and treatments can save money for healthcare providers and insurance. Medical personnel may treat more patients in the time saved on administrative chores. Trans-regional phone calls are reduced when EHR data are shared. Due to greater diagnostic accuracy, there are reduced risks of malpractice claims. Customer happiness rises, resulting in increased retention and profit potential. IT services are saved since there are fewer individual software upgrades, and feature additions exist.

4. Discussion

We have reviewed interoperable implemented EHR standards including HL7, HIPAA, openEHR, DICOM, and SNOMED-CT. Among such standards we have HIPAA and HL7 standards. From the literature survey, we have analyzed the importance of blockchain technology in the healthcare sector. The survey also helped to analyze the importance of HIPAA and HL7. We have proposed our BCIF-EHR framework with other existing frameworks. We have suggested how our framework is better than others.

The proposed framework focuses on interoperability of the two EHR standards, HIPAA and HL7. This interoperability helps in building a unique combined system which utilizes blockchain technology to combine the two proposed frameworks to share services and data. Our framework also proposed cross-chain EHR exchange. EHR can be exchanged from Ethereum to Hyperledger fabric and vice versa. Both the frameworks have been made interoperable, which means that processed data can be accessed from either of the two platforms. For the sake of reliability, a duplicate copy of the data is kept to be utilized in case of need. This combined system follows all the basic rules of blockchain technology and is up to the mark according to the latest blockchain conventions.

Various data sharing and privacy-preserving techniques were employed in the proposed framework. It is quite tough to track down a specific patient using only their data. We utilize encryption techniques on the patient private data stored on the blockchain in the suggested framework, which lowers the risks of unwanted access to the patient private data.

This system was largely utilized to protect data privacy while also sustaining EHRs, which keeps data secret while allowing anybody to access it from the outside. In the future, we will look at the feasibility of adopting the differential privacy model and try to figure out if there is a link between noise and blockchain size.

We propose a blockchain-based architecture for EHR exchange and maintenance that is both efficient and secure. Interoperability of EHRs utilizing the blockchain paradigm was also an option. The approach is patient-centric where health data will be controlled by patients only.

5. Conclusions and Future Direction

This article provides a discussion on the significance of BCIF-EHR by comparing key blockchain interoperable solutions available to the market based on their interoperability guidelines. Based on the comparisons, it can be concluded that none of the current BCIF-EHR solutions completely comply with the BCIF-EHR values. This paper also identifies the phases and the needs for BCIF-EHR utilization in the electronic health record system. The paper provides a detailed discussion of how healthcare organizations execute complete and functioning BCIF-EHR interoperable electronic health record systems. This article has provided the BCIF-EHR model and architectural components and summarized the BCIF-EHR parts needed for the establishment of BCIF-EHR solutions and how the requirements of BCIF-EHR interoperability can be fulfilled. Finally, this article discusses the application of BCIF-EHR in the electronic health record model for solving challenges in conventional electronic health record structures. However, the main shortcoming of this study is that the suggested model has not been effectively executed and thus cannot be applied to actual parties participating in electronic health record systems. Consequently, this article recommends further steps, such as the participation of government and other stakeholders in assessing the compatibility of BCIF-EHR and technological models, and recognition of the novel concept of BCIF-EHR by legislatures, regulators, and other stakeholders in the electronic health record system.

The proposed framework would be utilized to promote scalability in various systems. Only the hashes and minor EHRs on the blockchain need to be stored to save storage space. Furthermore, few nodes demand verified transactions with data hashes while executing private patient transactions. Due to this, the blockchains storage and mining costs will be further reduced. On the other hand, when more users join the system, the CLC search time will undoubtedly grow. As a result, specific novel approaches are necessary to efficiently search CLC with big local datasets.

This research showed the interoperability of the two EHR frameworks HIPAA and HL7. This interoperability helps build a unique combined system that utilizes blockchain technology to combine the two proposed frameworks with sharing services and data. Both frameworks have been made interoperable, meaning that processed data can be accessed from either of the two platforms. For the sake of reliability, a duplicate copy of the data is kept to be utilized in case of need. This combined system follows all the basic rules of blockchain technology and is up to the mark according to the latest blockchain conventions.

Various data-sharing and privacy-preserving techniques were employed in the proposed framework. It takes much work to track a specific patient using only their data. We utilized encryption techniques on the patient private data stored on the blockchain in the suggested framework, which lowers the risks of unwanted access to the patient private data.

The electronic health record (EHR) is a computerized record of a patient's medical history. It has resolved a slew of data handling and security concerns. The lack of standardization and regulation of file sharing continues to hinder EHR interoperability, and difficulties with applying the blockchain approach are significant issues that healthcare administrations must consider. Any professional utilizing EHR in the healthcare sector must integrate it so that errors can be avoided, and hacking risks can be decreased. EHR standards must be adopted to function properly under specific laws and regulations. The problems and issues discussed in this study are related to blockchain and EHR interoperability. In addition, a realistic interoperability solution is presented. This research aids in elaborating on the associated difficulties and solutions in EHR deployment and managing data and patient information. The benefits of an innovative and blockchain-based interoperability framework were discovered to be successful.

There is no such interoperable system working in the practical world right now. So, there is no substantial comparison of this research with any existing systems. It is one of a kind, based on a new idea, and carries the potential to be maintained and expanded further for the betterment of the healthcare industry

Future Directions:

Future research in the area of BCIF-EHR can focus on the following areas:

- Implementing the BCIF-EHR framework in real-world electronic health record systems to evaluate its effectiveness and efficiency in terms of data sharing and interoperability.
- Investigating the security and privacy implications of using BCIF-EHR in electronic health record systems. This could include studying the potential vulnerabilities of the framework and developing solutions to mitigate them.
- Developing methods for integrating BCIF-EHR with existing electronic health record systems, including those that are not built on blockchain technology.
- Investigating the scalability of BCIF-EHR, particularly as more and more healthcare organizations adopt the framework and the volume of data shared increases.
- Exploring the use of smart contracts in BCIF-EHR to automate certain processes, such as data sharing agreements and permissions.
- Examining the regulatory and legal implications of using BCIF-EHR in electronic health record systems and developing guidelines for compliance.
- Investigating the potential for using BCIF-EHR to facilitate data sharing between different countries, and the potential benefits and challenges of doing so.
- Developing a decentralized authentication and access control mechanism for BCIF-EHR to ensure that only authorized individuals and organizations can access the shared data.

Overall, BCIF-EHR has the potential to revolutionize the way electronic health record systems work by enabling seamless data sharing and interoperability across different blockchain networks. Future research in this area should focus on evaluating and improving the effectiveness, security, and scalability of the framework, and developing solutions to any challenges that may arise.

Author Contributions: Conceptualization, F.A.R., H.A., Y.G., R.G.S., Q.X. and R.A.D.; Methodology, F.A.R., H.A., Y.G., Q.X., R.G.S. and R.A.D.; Software, F.A.R. and Y.G.; Validation, F.A.R., H.A., A.A.A., A.J. and R.A.D.; Formal analysis, F.A.R.; Investigation, F.A.R., Y.G., A.A.A. and A.J.; Resources, Q.X.; Writing—original draft, F.A.R.; Writing—review & editing, H.A., Y.G., A.J., R.G.S. and R.A.D.; Visualization, Y.G. and A.A.A.; Supervision, Y.G.; Project administration, Y.G. and Q.X.; Funding acquisition, Y.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under GRANT 3091.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would also like to express their gratitude to Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under GRANT 3091.

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

References

1. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, *42*, 156. [[CrossRef](#)] [[PubMed](#)]
2. Reegu, F.A.; Mohd, S.; Hakami, Z.; Reegu, K.K.; Alam, S. Towards trustworthiness of electronic health record system using blockchain. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 2425–2434.
3. 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](#)] [[PubMed](#)]

4. Khan, A.U.; Shahid, A.; Tariq, F.; Ghaffar, A.; Jamal, A.; Abbas, S.; Javaid, N. *Enhanced Decentralized Management of Patient-Driven Interoperability Based on Blockchain*; Springer International Publishing: New York, NY, USA, 2020; Volume 97, ISBN 9783030335069.
5. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [[CrossRef](#)] [[PubMed](#)]
6. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [[CrossRef](#)]
7. Pillai, B.; Biswas, K. *Blockchain—ICBC 2019*; Springer International Publishing: San Diego, CA, USA, 2019; Volume 11521, ISBN 978-3-030-23403-4.
8. Kim, D.H.; Ullah, R.; Kim, B.S. RSP Consensus Algorithm for Blockchain. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4. [[CrossRef](#)]
9. Ekblaw, A.; Azaria, A.; Halamka, J.D.; Lippman, A.; Vieira, T. *A Case Study for Blockchain in Healthcare: “MedRec” Prototype for Electronic Health Records and Medical Research Data White Paper MedRec: Using Blockchain for Medical Data Access and Permission Management*; IEEE Access: Vienna, Austria, 2016; ISBN 978-1-5090-4055-1.
10. Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.P.; Shyu, C.R. A patient-centric health information exchange framework using blockchain technology. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2169–2176. [[CrossRef](#)]
11. Gramoli, V. From blockchain consensus back to Byzantine consensus. *Future Gener. Comput. Syst.* **2020**, *107*, 760–769. [[CrossRef](#)]
12. Sundvall, E.; Terner, A.; Broberg, H.; Gillespie, C. Configuration of Input Forms in EHR Systems Using Spreadsheets, openEHR Archetypes and Template. *Stud. Health Technol. Inform.* **2019**, *264*, 1781–1782. [[CrossRef](#)]
13. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [[CrossRef](#)]
14. Riaz, R.; Kim, K.H.; Ahmed, H.F. Security analysis survey and framework design for IP connected LoWPANs. In Proceedings of the Proceedings—2009 International Symposium on Autonomous Decentralized Systems, ISADS 2009, Athens, Greece, 23–25 March 2009; pp. 29–34.
15. Dar, A.A.; Alam, M.Z.; Ahmad, A.; Reegu, F.A.; Rahin, S.A. Blockchain Framework for Secure COVID-19 Pandemic Data Handling and Protection. *Comput. Intell. Neurosci.* **2022**, *2022*, 7025485. [[CrossRef](#)]
16. Rahmadika, S.; Rhee, K.H. Blockchain technology for providing an architecture model of decentralized personal health information. *Int. J. Eng. Bus. Manag.* **2018**, *10*, 1–12. [[CrossRef](#)]
17. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [[CrossRef](#)]
18. Beinke, J.H.; Fitté, C.; Teuteberg, F. Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study. *J. Med. Internet Res.* **2019**, *21*, e13585. [[CrossRef](#)] [[PubMed](#)]
19. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [[CrossRef](#)] [[PubMed](#)]
20. Satti, F.A.; Khan, W.A.; Lee, G.; Khattak, A.M.; Lee, S. Resolving data interoperability in ubiquitous health profile using semi-structured storage and processing. *Proc. ACM Symp. Appl. Comput.* **2019**, *F1477*, 762–770. [[CrossRef](#)]
21. Pournaghi, S.M.; Bayat, M.; Farjami, Y. MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 4613–4641. [[CrossRef](#)]
22. He, X.; Alqahtani, S.; Gamble, R. Toward Privacy-Assured Health Insurance Claims. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1634–1641. [[CrossRef](#)]
23. van der Linden, H.; Kalra, D.; Hasman, A.; Talmon, J. Inter-organizational future proof EHR systems. A review of the security and privacy related issues. *Int. J. Med. Inform.* **2009**, *78*, 141–160. [[CrossRef](#)]
24. Chen, H.S.; Jarrell, J.T.; Carpenter, K.A.; Cohen, D.S.; Huang, X.; Hospital, M.G. Blockchain in healthcare: A patient-centered model. *Biomed. J. Sci. Tech. Res.* **2019**, *20*, 15017–15022.
25. Hasanova, H.; Baek, U.; Shin, M.; Cho, K.; Kim, M.-S.; Myung-Sup Kim, C. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Int. J. Netw. Manag.* **2019**, *29*, e2060. [[CrossRef](#)]
26. Reisman, M. EHRs: The Challenge of Making Electronic Data Usable and Interoperable. *Pharm. Ther.* **2017**, *42*, 572.
27. Heart, T.; Ben-Assuli, O.; Shabtai, I. A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. *Health Policy Technol.* **2017**, *6*, 20–25. [[CrossRef](#)]
28. Al Mamun, A.; Azam, S.; Gritti, C. Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. *IEEE Access* **2022**, *10*, 5768–5789. [[CrossRef](#)]
29. Donawa, A.; Orukari, I.; Baker, C.E. Scaling Blockchains to Support Electronic Health Records for Hospital Systems. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 550–556. [[CrossRef](#)]

30. 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](#)] [[PubMed](#)]
31. Alamri, M.; Jhanjhi, N.; Humayun, M.; Arabia, S. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 244–258.
32. Zheng, Z.; Pan, J.; Cai, L. Lightweight Blockchain Consensus Protocols for Vehicular Social Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5736–5748. [[CrossRef](#)]
33. Iqbal, M.; Matulevicius, R. Exploring Sybil and Double-Spending Risks in Blockchain Systems. *IEEE Access* **2021**, *9*, 76153–76177. [[CrossRef](#)]
34. Masseport, S.; Lartigau, J.; Darties, B.; Giroudeau, R. Proof of usage: User-centric consensus for data provision and exchange. *Ann. Telecommun.* **2020**, *75*, 153–162. [[CrossRef](#)]
35. Matulevičius, R.; Iqbal, M.; Ammar Elhadjamor, E.; Ghannouchi, S.A.; Bakhtina, M.; Ghannouchi, S. Ontological Representation of Healthcare Application Security Using Blockchain Technology. *Informatica* **2022**, *33*, 365–397. [[CrossRef](#)]
36. Jabbar, S.; Lloyd, H.; Hammoudeh, M.; Adebisi, B.; Raza, U. Blockchain-enabled supply chain: Analysis, challenges, and future directions. *Multimed. Syst.* **2021**, *27*, 787–806. [[CrossRef](#)]
37. Guimarães, T.; Silva, H.; Peixoto, H.; Santos, M. Modular Blockchain Implementation in Intensive Medicine. *Procedia Comput. Sci.* **2020**, *170*, 1059–1064. [[CrossRef](#)]
38. Lahami, M.; Maalej, A.J.; Krichen, M.; Hammami, M.A. A Comprehensive Review of Testing Blockchain Oriented Software. *ENASE* **2022**, 355–362. [[CrossRef](#)]
39. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [[CrossRef](#)]
40. Reegu, F.A.; Abas, H.; Jabbari, A.; Akmam, R.; Uddin, M.; Wu, C.-M.; Chen, C.-L.; Khalaf, O.I. Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A Systematic Review and Open Research Challenges. *Secur. Commun. Netw.* **2022**, *2022*, 9227343. [[CrossRef](#)]
41. Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [[CrossRef](#)]
42. Song, H.; Zhu, N.; Xue, R.; He, J.; Zhang, K.; Wang, J. Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. *Inf. Process. Manag.* **2021**, *58*, 102507. [[CrossRef](#)]
43. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W.C. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access* **2020**, *8*, 54371–54401. [[CrossRef](#)]
44. Reegu, F.A.; Abas, H.; Hakami, Z.; Tiwari, S.; Akmam, R.; Muda, I.; Almashqbeh, H.A.; Jain, R. Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records. *Secur. Commun. Netw.* **2022**, *2022*, 1953723. [[CrossRef](#)]
45. Lau, E. Decoding the Hype: Blockchain in Healthcare—A Software Architecture for the Provision of a Patient Summary to Overcome Interoperability Issues. Master's Thesis, Utrecht University, Utrecht, The Netherlands, June 2018.
46. Reegu, F.; Zada, K.W.; Mohd, D.S.; Arshad, Q.; Armi, N. A Reliable Public Safety Framework for Industrial Internet of Things (IIoT). In Proceedings of the 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Virtual Conference, 18–20 November 2020; pp. 189–193. [[CrossRef](#)]
47. Stanimirović, D. Special Topic Interoperability and EHR: Combining openEHR, SNOMED, IHE, and Continua as approaches to interoperability on national eHealth. *Appl. Clin. Inf.* **2017**, *8*, 810–825. [[CrossRef](#)]
48. Reegu, F.A.; Al-Khateeb, M.O.; Zogaan, W.A.; Al-Mousa, M.R.; Alam, S.; Al-Shourbaji, I. Blockchain-Based Framework for Interoperable Electronic Health Record. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 6486–6495.
49. Daraghmi, E.Y.; Daraghmi, Y.A.; Yuan, S.M. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [[CrossRef](#)]
50. Sonkamble, R.G.; Phansalkar, S.P.; Potdar, V.M.; Bongale, A.M. Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. *IEEE Access* **2021**, *9*, 158367–158401. [[CrossRef](#)]
51. Saripalle, R.; Runyan, C.; Russell, M. Using HL7 FHIR to achieve interoperability in patient health record. *J. Biomed. Inform.* **2019**, *94*, 103188. [[CrossRef](#)] [[PubMed](#)]
52. Gill, E.; Dykes, P.C.; Rudin, R.S.; Storm, M.; McGrath, K.; Bates, D.W. Technology-facilitated care coordination in rural areas: What is needed? *Int. J. Med. Inform.* **2020**, *137*, 104102. [[CrossRef](#)] [[PubMed](#)]
53. Farhadi, M.; Haddad, H.; Shahriar, H. Compliance Checking of Open Source EHR Applications for HIPAA and ONC Security and Privacy Requirements. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019; pp. 704–713. [[CrossRef](#)]
54. Dolin, R.H.; Alschuler, L.; Beebe, C.; Biron, P.V.; Boyer, S.L.; Essin, D.; Kimber, E.; Lincoln, T.; Mattison, J.E. The HL7 clinical document architecture. *J. Am. Med. Inform. Assoc.* **2001**, *8*, 552–569. [[CrossRef](#)] [[PubMed](#)]
55. Muinga, N.; Magare, S.; Monda, J.; Kamau, O.; Houston, S.; Fraser, H.; Powell, J.; English, M.; Paton, C. Implementing an Open Source Electronic Health Record System in Kenyan Health Care Facilities: Case Study. *JMIR Med. Inform.* **2018**, *6*, e22. [[CrossRef](#)] [[PubMed](#)]

56. Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; da Silva, V.F.; Goldim, J.R.; Schmidt, D.C. Analyzing the performance of a blockchain-based personal health record implementation. *J. Biomed. Inform.* **2019**, *92*, 103140. [[CrossRef](#)]
57. Roehrs, A. OmniPHR: A Blockchain Based Interoperable Architecture for Personal Health Records. Ph.D. Thesis, Universidade do Vale do Rio dos Sinos, São Leopoldo, Brazil, 2019.
58. Wani, S.; Imthiyas, M.; Almohamedh, H.; Alhamed, K.M.; Almotairi, S.; Gulzar, Y. Distributed denial of service (Ddos) mitigation using blockchain—A comprehensive insight. *Symmetry* **2021**, *13*, 227. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Reproduced with permission of copyright owner. Further reproduction
prohibited without permission.