DOI: 10.2478/ias-2024-0017 • JIAS • 19(6) • 2024 • 249-265

A Survey of Distributed Ledger Technologies in the Health Domain

Ikramullah Khan[1*], Sudip Phuyal[1*], Ricardo Correia[2] and Joao C. Ferreira[1,3]

[1] University Institute of Lisbon (ISCTE-IUL), ISTAR, Lisbon, 1649-026, Portugal.
[2] BioGHP, Lisbon, Portugal; ricardo@bioghp.com
[3] Inov Inesc Inovação—Instituto de Novas Tecnologias, Lisbon, 1000-029, Portugal; Joao.Carlos.Ferreira@iscte-iul.pt

*Corresponding author(s): ikramkhan483@gmail.com; sudipphuyal@gmail.com;

Abstract: Healthcare providers face critical challenges in managing and exchanging patient health and medical records. Traditional health and medical data management systems, which often include paper-based records and work as closed, isolated silos, have demonstrated limitations in terms of data usability, interoperability, and patient privacy. This translates into limitations not only for providers but also for the patients, healthcare professionals, and other participants of the health- care value chain, hindering potential innovations and efficiency gains. Distributed Ledger Technology (DLT), such as the blockchain, is emerging as a possible solution to challenges in data management and beyond across several operational and administrative processes in healthcare services. This paper begins with an extensive overview of the literature with an emphasis on DLT implementations and applications in the healthcare industry. We examine how DLT has been used in real-world initiatives across the healthcare domain, highlight notable initiatives, and outline potential improvements. This may result from its adoption, namely in areas such as healthcare data sharing and interoperability, verifiability, transparency, or patient privacy and control. Overall, some of DLT's native capabilities, such as data immutability, sharing and reconciliation across parties with varying levels of trust, and user self-sovereignty may translate into solutions for several caveats of the current healthcare technological infrastructures, and contribute to improving healthcare outcomes by fostering innovations, enabling broader sharing of healthcare data, enhancing transparency over the use of data, equipping patients with greater control over their data, and enabling new or improved services and processes in healthcare.

Keywords: Distributed ledger technologies (DLT); blockchain; healthcare; medical records, data security; interoperability; patient-centric care; electronic health records (EHR); decentralization

1 Introduction

Distributed Ledger Technologies (DLTs) are revolutionizing business transactions worldwide, enabling collaboration beyond the confines of current regulatory frameworks [1]. DLT operates as an infrastructure for recording data in a distributed manner, devoid of central control, thereby prioritizing decentralized network governance and cryptographic data security. [2]. Satoshi Nakamoto introduced the concept of a trustless electronic transaction system in the seminal blockchain whitepaper 2008 [3]. Blockchain has gained significant attention across various sectors after its remarkable success in cryptocurrencies such as Bitcoin and Ethereum [4]. Widely regarded as a groundbreaking innovation, DLTs have immense potential in the organizational infrastructure and collaboration across economies, societies, and industries [5]. While initially prominent in finance, particularly in digital currencies, DLT's applicability spans diverse domains, including healthcare, where it addresses challenges like healthcare data sharing, interoperability, verifiability, transparency, or patient privacy and control [6]. The evolution of blockchain technology has seen successive generations, with Blockchain 1.0 pioneering cryptocurrency applications like Bitcoin, Blockchain 2.0 introducing Smart Contracts, and Blockchain 3.0 extending to non-financial sectors such as government, energy, and healthcare [7]. Many characterize blockchain as a catalyst for industry and innovation, leveraging the platform of technology to deliver computing resources universally and facilitate shared community engagement. Additionally, blockchain empowers patients by granting them more control over data ownership and consent management, allowing transparent data sharing and making it more verifiable through decentralized ledgers. In response to healthcare data management's persistent challenges, blockchain technology has emerged as a solution, offering decentralized and immutable ledgers to patient medical records. We have organized the rest of the paper as follows—section 2 details this survey's methodology, including search strategies, results, and data synthesis. Section 3 provides a literature review on DLT in the health domain, it highlights the blockchain initiatives in the healthcare domain, focusing on data sharing, interoperability, transparency, patient privacy, and control. Section 4 overviews the selected blockchain frameworks in the healthcare domain. The frameworks include six different implementations, namely Med-Rec, Medical-Chain, Patientory, Prov-Chain, IBM Blockchain for Healthcare, and Nebula Genomics blockchain. In Section 5, we concluded the paper with a discussion about the findings of potential in the blockchain to overcome the issues of data sharing and interoperability. In Table 3, we have a comparison chart of different blockchain networks, including their transaction fee in dollars and speed in transaction per second TPS.

2 Methodology

The preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement was first released more than a decade ago [8]. The PRISMA declaration was created to assist authors in reporting systematic reviews and meta-analyses more effectively. When it comes to information that is transparently and methodically synthesized, health decision-makers perceive systematic reviews as a vital resource [9]. The PRISMA statement in Moher [10] and the authors' suggested methodology in the paper by Briner and Denyer [11] provide a thorough, methodical, and scientific analysis of blockchain-driven applications for healthcare. The most recent studies on the use of blockchain technology in the healthcare sector are included in the literature survey. The systematic survey that was offered was determined by the following actions.

2.1 Search Strategy and Inclusion Criteria

This literature analysis was done in February 2024, and the search strategy and inclusion criteria were created to guarantee that pertinent, current, English language publications with reviews about blockchain in healthcare were chosen. The search was restricted to journal papers released from 2016 to 2024, and it used data from three reliable databases: Web of Science Core Collection, IEEEXplore, and Scopus. Duplicate articles were eliminated from the initial search results to preserve data integrity. Figure 1 shows the PRISMA workflow diagram. The search term was carefully selected to find articles that addressed blockchain in the context of electronic health records (EHR) or electronic medical records (EMR), emphasizing decentralization, DLT, and interoperability in healthcare. The 'Healthcare' industry was the population of interest, and the query added phrases like 'Interoperability' and 'Decentralization' as further filters to make sure the articles were relevant. '("DLT") AND("Blockchain") AND ("Electronic Medical Record" or "EMR" or "Electronic Health Record" or "EHR") AND ("Healthcare") AND ("Interoperability" or "Decentralization")" was the last search query that was used. The objective of our search approach was to locate an extensive range of current, relevant publications about the relationship between blockchain technology and healthcare, with a particular emphasis on decentralization and interoperability. Another search used the query 'Distributed Ledger Technologies in the Health Domain,' which produced about seventy-seven articles.

2.2 Search Results

As mentioned earlier, the specified query is being applied to the Web of Science and Scopus databases, and 167 articles were found. Removing 21 duplicates and auto-ineligible articles. We were left with a total of 114 articles that were screened. The chosen publications were then subjected to a systematic analysis using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) technique, as stated in reference [12]. PRISMA is a well-respected methodology that guarantees the transparent and methodical analysis of research papers in systematic reviews and meta-analyses. This technique is intended to assist researchers in evaluating the quality and relevance of the papers they are examining by streamlining the review process and maintaining high standards. Figure 1 shows the PRISMA Workflow. After removing duplicates and screening, 41 articles were included in the study.

2.3 Data Extraction and Synthesis

Zotero, Microsoft Excel, Scopus, and WoSCC web interfaces served as essential tools for managing and storing data pertinent to the articles during the systematic literature review conducted using the

PRISMA method. This data encompassed various aspects, including article title, author, publication year, subject area, keywords, and abstract. A qualitative assessment was also performed using these criteria to facilitate a comprehensive data analysis.

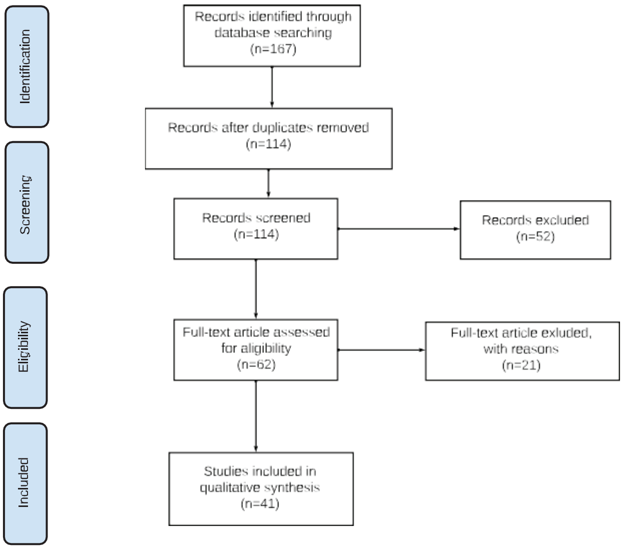
Identification
Screening
Eligibility
Included
Records identified through database searching (n=167)
Records after duplicates removed (n=114)
Records screened (n=114)
Records excluded (n=52)
Full-text article assessed for aligibility (n=62)
Full-text article exluded, with reasons (n=21)
Studies included in qualitative synthesis (n=41)

Figure 1. PRISMA Workflow, n is the number of research articles

3 Literature Review

The healthcare industry is undergoing a transformation driven by technological advancements and growing demand for efficient and easily accessible healthcare services. One of the critical challenges facing healthcare systems worldwide is the management and accessibility of patient medical records [13]. Numerous organizations have embraced blockchain technology, implementing it across various healthcare use cases [7]. The traditional paper-based and fragmented EHR systems have proven inefficient, error-prone, and susceptible to security breaches [14]. Blockchain's decentralized ledger, distributed across a network of nodes, minimizes the risk of single points of failure and data manipulation, thereby enhancing data integrity and security. Data stored in blocks with distributed ledgers are immutable on the blockchain, which preserves the integrity of medical records, while cryptography algorithms and consensus techniques ensure data protection and authentication. Smart Contracts streamline supply chain tracking, insurance claim processing, and patient consent management, reducing reliance on intermediaries. The transparent and auditable nature of blockchain preserves data history, facilitating effective monitoring of data usage and legal compliance within healthcare systems. Strategies like zero-knowledge proofs verify transactions without disclosing actual data, ensuring patient confidentiality while maintaining data authenticity and accuracy. Blockchain's adherence to defined standards, such as Fast Healthcare Interoperability Resources (FHIR), enables seamless interaction with existing healthcare systems, promoting efficient data sharing [15]. The potential of blockchain technology in the health industry is substantial, but in some cases its value may be exaggerated. The most challenging barriers to the health sector's digital transformation, like a lack of data interoperability, are not eliminated by blockchain [16].

DLT's blockchain, characterized by decentralized peer-to-peer systems implementing a public, trustless, append-only ledger, is relevant to the healthcare sector. Its distributed and trustless nature ensures complete decentralization, transparency, and independent execution, with all peers serving as ledger members, thus constituting a distributed ledger recording all transactions within the blockchain [16]. Blockchain technology embodies several essential features, including decentralization, immutability, audit trails, security, and traceability, offering a robust framework for secure and decentralized data management across various domains beyond cryptocurrency [17]. Ethereum, a decentralized computing system utilizing the Ethereum Virtual Machine (EVM) and native token ETH, enables the creation and execution of Smart Contracts, facilitating the storage and codification of data operations. Ethereum's payment policy, based on 'gas,' insentience's network nodes to validate and execute transactions while deterring malicious attacks [18]. DLT serves diverse purposes in the medical field, providing a secure and immutable ledger for storing EHRs and patient data. Each transaction is recorded as a ‘block’ in the chain, safeguarded by cryptographic hashes, ensuring data integrity and security. Smart Contracts automate data exchange processes while enhancing security measures, particularly in smart health systems, where data encryption and compression models are pivotal in securing EHR [15]. In the following sections, we unraveled the intricacies of blockchain’s role in healthcare data management and its potential to reshape the future of healthcare delivery.

Karmakar *et al.*[19] discuss the possibility of implementing blockchain and distributed ledger technology in the medical insurance domain. The integration of DLT presents a viable opportunity for adopting and optimizing the search, claim, and transaction model within insurance companies. Pillai *et al.*[20] discussed different attack scenarios compared to mitigating cost and damages. They also pointed out the possible mitigations and security measures for these attacks, including malware and Trojans, credential stuffing, password spraying, phishing campaigns, cryptojacking, stealing clicks, network-based attacks, 51 percent attacks, and other. Samanta *et al.* [21] describe the potential adoption of blockchain technology in the healthcare industry, which presents excellent potential for revolutionizing the growth of developing smart cities across the globe. This is made possible by smart cities’ deliberate application of cutting-edge technologies to restructure their healthcare systems and develop flexible delivery networks, making incorporating blockchain solutions in healthcare more accessible.

3.1 Distributed Ledger Technology (DLT’s)

Distributed Ledger Technology (DLT) is a progressive approach to storing records, transactions, contracts, and agreements within and between organizations [22]. Unlike conventional databases, DLT ensures data integrity through consensus mechanisms rather than centralized authority [1], making it more secure and decentralized. Figure 2. shows the DLT’s framework concept. Classification of DLT can be differentiated into the traditional ledger, Permissioned Private Ledger, Permissioned Public Ledger, and Un-permissioned Public Ledgers[23]. Permissioned Public ledgers enable open public participation in data contribution and consensus formation, ensuring universal ledger access without ownership by any single entity, thus facilitating unrestricted transaction injection into the ledger[23]. Public blockchains are more decentralized and inclusive than private blockchains. In a private blockchain, security and confidentiality are more important than decentralization. Security, scalability, and decentralization are intertwined, so enhancing one often diminishes another. This is also called the blockchain trilemma, the term coined by Ethereum founder Vitalik Buterin[24]. It facilitates fast, cost-effective, and secure data exchange processes while minimizing reliance on centralized authority for transaction management. Departing from traditional centralized models reliant on singular hubs for data integration, validation, and storage, DLT decentralizes these functions, with each interconnected node replicating, validating, and storing identical ledger copies. Subsequently, individual nodes independently update their respective ledgers, verifying alterations against updates from other network nodes [25]. Transactions are immutable, and the interconnected blocks are transmitted via a peer-to-peer network [26]. Attempts to tamper or modify records within these blocks undergo scrutiny by other nodes in the network; alterations are more challenging once a block is established and acknowledged. DLT improves trust between nodes in public (open) or private (closed) decentralized networks. Nodes connected in the network have a copy of the decentralized ledger with all the transactions within the network[27]. Its adoption within organizations reduces data manipulation, theft, and fraud.

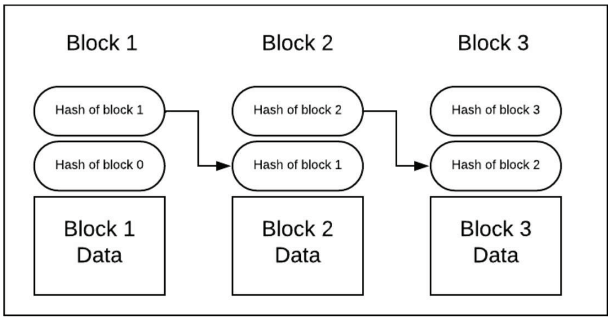

Figure 2. Distributed ledger technology’s (DLT) framework concept

3.2 Distributed Ledger Technology (DLT's) in the health domain

Efficient storage, interoperability, and accessibility of healthcare data are complex challenges. Emerging technologies, such as DLT, offer decentralized solutions for data transaction management [28]. The misuse of healthcare data is a prevalent concern, with numerous clinical data losses, unauthorized distribution to third parties, high patient cost burdens, and operational complexities for medical professionals. Implementing blockchain technology in healthcare systems is increasingly recognized to address data security and storage concerns, particularly regarding interoperability, data fragmentation reports, and retrieval difficulties. Leveraging DLT protocols, decentralized healthcare payment and insurance models are gaining momentum, offering investors transparency and trust while mitigating inefficiencies of the current system. By streamlining workflow communication and automating transactional services, blockchain and DLT innovations facilitate seamless processes, eliminating intermediaries and enhancing billing and claims procedures within the healthcare industry [6]. Moreover, these technologies hold promise in combating drug counterfeiting and improving healthcare data maintenance, addressing interoperability, data integrity, security, and cost management. Ultimately, the transformative potential of blockchain and DLT technologies underscores their pivotal role in revolutionizing healthcare operations, offering unprecedented advancements and value outcomes [29]. Table 1. shows different types of blockchain.

The healthcare blockchain ecosystem encompasses various stakeholders, including healthcare professionals and patients as data generators, the medical cloud for storage infrastructure, and the blockchain network comprising distributed ledger and Smart Contract functionalities for securing data access and interoperability. The healthcare industry demands strict security measures and protocols to safeguard sensitive patient information and ensure compliance with uncompromising data protection regulations. It requires security, interoperability, non-repudiation, access control, authentication, medical data sharing, and mobility. Blockchain technology offers distinct advantages tailored to the healthcare sector, including transparency, immutability, traceability, secure data exchange, decentralization, and cost-effectiveness. DLT applications within healthcare span diverse domains, including patient data management, drug traceability, cryptocurrency payment, clinical trials, data security, and the establishment of secure and decentralized healthcare setups [30]. Notably, EHR management facilitated by blockchain integration introduces features such as patient-controlled access, anonymous healthcare services, online EHR availability, confidentiality, integrity, access control delegation, zero-knowledge proof, emergency access, scalability, interoperability, and remote healthcare services [31]. Leveraging DLT enables the development of data protection-compliant solutions in trustless environments, ensuring data immutability, protection, and transparency as required [32].

Table 1 Types of Blockchain

	Pubic Blockchain	**Private Blockchain**	**Consortium Blockchain**
Permission	Public	Private	Public or Private
Organization	Decentralized	Partially Decentralized	Almost Decentralized
Security	High	Medium	Medium
Cost	High	Medium	Low
Identity	Anonymous	Identified	Identified
Example	Bitcoin, Ethereum	Company internal	Hyperledger, Corda

3.3 Challenges of Blockchain Technology in Healthcare

Both paper-based and electronic traditional health record systems have security flaws and inefficiencies [33]. Blockchain has obstacles but has the potential to revolutionize healthcare data management. When implemented, data processing may be redesigned, improving privacy, security, and interoperability in clinical trials, EHRs, and drug supply chains. Scalability, compatibility with current systems, and adherence to laws like GDPR and HIPAA are among the problems. The main challenges include standardizing data, protecting privacy and security, and encouraging wider use. Challenges include dangers related to data loss, user education, and budgetary issues. Blockchain's implementation in healthcare is further complicated by legal responsibility, the young age of the technology, and its smooth interaction with other cutting-edge technologies [34]. The use of blockchain technology in healthcare is hampered by significant financial limitations, particularly for smaller institutions, because of the high costs of system development, upkeep, and resource-intensive needs, which call for highly qualified staff and dependable infrastructure [35]. In addition, given the novelty and complexity of the technology, user education continues to be a major barrier that has to be overcome. In-depth training programs are needed to provide patients and healthcare professionals with the information they need to fully utilize blockchain's advantages [36] [37].

3.4 Potential Improvements

The scalability of blockchain technology is a big issue, particularly for Ethereum and Bitcoin-based healthcare applications. The difficulty is managing large amounts of healthcare data and transactions effectively without incurring undue expenses or delays [38]. Medical data and patient information flow necessitate quick and safe processing. The limits of current blockchain technology, particularly on public networks, might result in slower processing times, higher costs, and inefficiencies, which reduce the technology's usefulness for managing healthcare data. For blockchain to successfully satisfy the expectations of the healthcare industry, scalability is a critical issue [39].

3.5 Interoperability

Interoperability and broad acceptability are the two most important conditions for blockchain integration in healthcare. Blockchain adoption for data management is necessary for the healthcare ecosystem to succeed. Building an innovative and trusting culture while overcoming organizational and technical constraints is hard. For effective patient data transmission, interoperability necessitates smooth cooperation between blockchain systems and healthcare organizations. Different blockchain designs and data types provide obstacles, requiring protocols to establish communication. Establishing interoperability standards and closing these gaps would need cooperation between government agencies, digital companies, and the healthcare industry. This would enhance patient care [13] [40]. Integrating blockchain into antiquated healthcare systems that handle patient data is difficult. These systems need a lot of effort, money, and system upgrades to make them seamlessly compatible with blockchain technology since they do not have the necessary interfaces [41]. Fundamental modifications to data processing and storage techniques must align with blockchain, which may require new software interfaces. Hardware, network, and security protocol re-configurations may also be required. Healthcare organizations strive to surmount these obstacles to enhance data security, facilitate interoperability, and reap the rewards of sharing [42]. A searchable blockchain-based HIE system is suggested by L. Sigong *et al.* to address the trade-off between data usefulness and security. The system processes EHRs using a granular manner based on attributes. As a result, it permits effective EHR search and utilization without needless decryption procedures. The suggested approach improves data usability by enabling users to run targeted queries and statistical analyses on particular healthcare data. It uses the immutability and decentralization of blockchain technology to protect EHRs from potential privacy risks associated with HIE systems [43].

3.6 Regulatory Compliance and Data Sharing

BC-UADS framework implements blockchain-based user authentication and a data sharing scheme. It uses a consortium blockchain to provide a distributed and decentralized data-sharing platform in a permission network using the PoR consensus algorithm. This framework protects the authenticity, immutability, and transparency of patient HER data which are transferred online between different hospitals [44]. T. Wang *et al.* propose a mechanism for exchanging health data HSHB, which is built on a hybrid blockchain, that separates data sharing into two categories: alliance chain and private chain. To ensure the security and privacy of health data sharing, sensitive data is managed through Smart Contracts before being shared with outside organizations [45]. Healthcare is obligated by laws such as GDPR and HIPAA to protect patient data. Notwithstanding its advantages, blockchain's decentralization makes it difficult to adhere to these requirements [33]. Dispersed data complicates management and auditing and makes privacy compliance difficult. It is imperative to do a privacy legislation analysis of blockchain technology before implementing healthcare data systems. It could be necessary to use anonymization procedures to safeguard patient identities. Adherence is essential, necessitating blockchain solutions prioritizing data security and privacy [46][41].

3.7 Data Standardization and Data Security

Healthcare organizations and blockchain developers must collaborate to build solutions that make it easier for standardized healthcare data to be translated and compatible with blockchain systems to overcome this obstacle [47]. This may entail developing middleware or data transformation procedures to bridge the gap between current data formats and blockchain needs. Data standards and blockchain compatibility must be achieved to guarantee that blockchain-based healthcare solutions can successfully communicate and exchange data with traditional healthcare systems and providers [48]. It is essential to maximize blockchain's benefits while preserving healthcare data management continuity and enhancing interoperability. Blockchain improves data security but raises privacy issues for the medical field. It is still challenging to strike a balance between data interchange and privacy, particularly when it comes to patient data. Blockchain's immutability and openness raise the possibility of a patient data vulnerability, necessitating strict access control even in the face of cryptographic security [49]. Smart Contracts provide an open data interchange, automate permission, and give patients control over data access within prescribed bounds. Developing blockchain-based healthcare systems that guarantee data sharing and privacy is complex. For patient privacy, compliance with data protection rules such as GDPR and HIPAA is essential [50] [51].

3.8 Patient Privacy and Control

Cryptographic keys are used in blockchain systems to restrict access to data, and their loss can render data permanently inaccessible. This issue highlights the importance of safely handling and saving private keys to prevent the irrevocable loss of crucial medical data. A blockchain-based healthcare setting emphasizes the necessity of vital key management techniques and user education to reduce the danger of data loss [49] [52]. Blockchain networks use consensus protocols to verify transactions and the chain's current state [49]. Although blockchain technology is still in its infancy, it has the potential to solve concerns about patient privacy, interoperability, and data security in the healthcare industry [36]. Present concerns include less understandable user interfaces, complicated implementations, and scalability issues. As technology advances, these early difficulties should disappear and make it easier to employ for healthcare. Healthcare blockchain integration with AI and IOT needs compatibility and collaboration. IoT collects real-time medical data, AI improves processing, and blockchain guarantees security. Expert cooperation is essential to building a smooth IT environment [53] [54]. There are protocols, such as Proof of Work (PoW) and Proof of Stake (PoS), each with pros and cons. Careful consideration of security, energy efficiency, scalability, and decentralization is necessary when choosing the best approach for healthcare. Adapting the consensus process to healthcare requirements avoids inefficiencies, excessive energy use, and security threats [55].

3.9 Transparency

While implementing blockchain in healthcare, legal and liability considerations are crucial. The decentralized nature of blockchain presents issues for health data management in terms of accountability [56]. It becomes difficult to assign blame for mistakes or disagreements because of decentralized networks and cryptographic keys. To resolve this, specific legal frameworks and contracts outlining responsibilities and liabilities are required, guaranteeing that all parties understand and abide by the legal protections designed for blockchain-based healthcare systems [35]. For blockchain systems to operate well, a vital network infrastructure is essential. In rural or remote places, limited access to reliable networks reduces the device's efficacy. Investments in network infrastructure and enhanced internet connectivity are necessary to realize blockchain's promise in these environments [57].

4 Review of Healthcare Framework implementations with blockchain

A blockchain can store patient data since it maintains an immutable, decentralized, and transparent information record. Additionally, it uses complex, secure codes that can protect private medical information to hide the identity of any individual. The decentralized structure of the technology also enables quick information communication between doctors and patients. Table 2 compares some blockchain implementations in the healthcare domain. These applications are important in the healthcare sector because they aim to solve important problems that the sector faces with innovative means. Patients have more ownership over their health information, which helps to improve transactional transparency in areas and allows them to safely access and share their records with healthcare professionals and institutions. Blockchain implementation improves the efficiency of healthcare operations and resource distribution by cutting costs and simplifying administrative procedures. Furthermore, by enabling transparent and safe data sharing, these implementations promote research and innovation while speeding up medical developments and enhancing healthcare outcomes internationally.

Following are some blockchain implementations that were discussed focusing on the framework implementation. These are selected based on the relevance. By selecting a diverse range of these implementations, we ensure to cover the essential features and functionalities. This selection ensures that we benefit from well-rounded and versatile blockchain solutions.

Table 2 Comparison chart of blockchain implementations in healthcare

Name	**Year**	**public/private BC**	**Framework**	**Language implementation**
MedRec[58]	2016	Private blockchain (permissioned)	Ethereum, PyEthereum	Solidity (for smart contracts)
Medicalchain[59]	2018	Public blockchain (permissioned for certain features)	Hyperledger Fabric	Go (Golang)
SimplyVital Health	2017	Public blockchain (permissioned for certain features)	Ethereum blockchain	Solidity (for smart contracts)
ProvChain[60]	2017	Not specified (proprietary implementation)	Private Permissioned	platform-independent library
Patientory[61]	2015	Private blockchain (permissioned)	Ethereum blockchain	PTOY and solidity
IBM Blockchain Healthcare[62]	2017	Private blockchain (permissioned)	Hyperledger Fabric	Go (Golang)
Gem Health Network	2016	Public blockchain (permissioned for certain features)	Ethereum blockchain	Solidity (for smart contracts)
Hashed Health	2016	Private blockchain (permissioned)	Hyperledger Fabric	Go (Golang)
Tierion	2015	Public blockchain (anchoring data to Bitcoin blockchain)	Bitcoin blockchain	JavaScript
Factom	2015	Public blockchain (Factom Protocol)	Factom Protocol	Go (Golang)
MedicalDao	2017	Public blockchain (permissioned)	Ethereum blockchain	Solidity (for smart contracts)
Health Nexus	2018	Public blockchain (permission for certain features)	Ethereum blockchain	Solidity (for smart contracts)
Blockchain Health Co.	2017	Not specified (likely a mix of public and private)	Ethereum blockchain	Solidity (for smart contracts)
MediBloc[63]	2017	Public blockchain (MediBloc Network)	Ethereum blockchain	Solidity (for smart contracts)
Nebula Genomics[64]	2018	Public blockchain (Gene-Chain)	Ethereum blockchain	Solidity (for smart contracts)

4.1 Med Rec

MedRec uses Ethereum’s Smart Contracts to generate intelligent representations of medical records on separate network nodes. It creates contracts with data integrity, permissions, and record ownership metadata. The blockchain transactions provide cryptographically signed instructions for maintaining specific attributes. The state-transition features of the contract implement policies requiring data alteration only through authorized transactions [58]. The blockchain Smart Contract record contains information about permissions and reclaiming data access. This is to create a fresh, minimally functioning patient record for a physician or administrator. An ID, such as a name or SSN, can identify each patient record. A public-key cryptographic ID is assigned to every patient record.

The architecture contains the registrar contract, summary contract, and patient-provider relationship. The summary contract must maintain the patient's medical record history on file. The document includes references to patients–provider relationship contracts (PPRs) and reflects the current and former participants in the various nodes of the system. Almost always, the patient gets recommendations from the doctor, and they also have the right to provide authorized users access to their medical records. It notifies users from the EMR manager with acknowledgment from the patient for consent and provides updates. The patient can accept, delete, or reject connections, and the provider decides each one's status. This patient can leave the dispersed network and return to it several times.

The contract structures and relationships of the MedRec framework implementation are designed as follows. This design has four parts: the client, manager, library, and database. Each user has a distinct ID and address, and the registrar's contract address makes it simple to identify the summary contract. The services immediately reported any modifications to the summary contract. After taking note of the user, the EHR Manager established an automated connection to the local database. The client sends the cryptographically signed request, which is sent to the issuer to verify IDs to the Gatekeeper. The customer must receive their data back if the address was supplied. With the aid of the registrar contract, the patient chooses which data to share with other users utilizing his address. When all the elements are merged with the EHR program, it offers the user update, view, data sharing, and retrieval options.

4.2 Medichain

By enabling physicians and specialists to access medical information from anywhere in the EHR, medical data is kept within the appropriate geographic area. The blockchain describes how the patient's health data may be accessed over the cloud. Other medical professionals can access the patient's medical records using this manner. Research and pharmaceutical departments can access the data. The Business Network Archive (BNA), utilized to ascertain the physiognomies and capabilities of MediChain, is created using Hyperledger Composer [65]. The composer created the script, access control, and model files. Any user may be a caretaker, physician, or patient. Every user registering for one of the three roles receives a unique ID number. The health record is solely accessible to the owner. The owner and the caretaker have the right to exchange information.

The Medichain framework manages various types of patient health data, including prescriptions, bills, test results, and diagnostic images. Hashes of these assets are stored on the blockchain. Through their Smart Contract, the patient may access their electronic medical record. The script file (Smart Contract) controls access to the health record. The Smart Contract stores the patient log data and viewing authorization. Essentially, it gives us limited access to the data. The access control list keeps track of all access regulations, including role-based, unconstrained, and mandatory access control.

4.3 Patientory

Patientory eliminates the need for third-party middlemen. It is most frequently used for health information exchange (HIE). Improved integrity, reduced transaction costs, and eliminating middlemen are all advantages of a decentralized system such as blockchain technology. Using the HIE enhances the continuity of the care cycle and reduces pointless administrations with repeated tests. Every rule and regulation under the Health Insurance Portability and Accountability Act (HIPAA) is adhered to, including those concerning security and privacy [61]. Patient-related outcome measures (PROMs) are maintained by this system, which primarily allows customers to examine a patient profile to keep track of their medical history. PROMs can include a patient's side effects and personal satisfaction with the treatment. The system can facilitate communication between patients and doctors on the importance of treatment-related diseases by providing a comprehensive and detailed evaluation of drugs for individual conditions. The system uses simple methods such as visits, hospital charges, personalized therapy data, protection, and prescriptions from the pharmacy to assist the patient.

4.4 Prov-Chain

A data provenance architecture based solely on blockchain and cloud technology. The data that are kept on the blockchain are accessible to any peer. Without the help of a third party, Prov-Chain automatically creates an open timestamped history of all client activities on cloud data. While the data are accessible, the provenance auditor can never identify the original user. The final one is data validation, where records are accessible via the blockchain network, and numerous nodes verify each block. The transmission of provenance information is approved by Prov-Chain using a blockchain receipt.

The blockchain network, provenance database, provenance auditor, and cloud user are the elements that make up the Prov-chain architecture. Access to the user's data on the blockchain and permission to share them with others are granted. Then, blockchain nodes verify the data modifications. The next component is the cloud service provider, which offers user registration and storage benefits. It keeps track of any modifications to the data and can gather a great deal of information about activities carried out by each client to improve management. It also detects intrusions. Mainly, this precaution protects their computerized health records. Provenance database entries were kept on the blockchain network, which was utilized by the malicious system.

4.5 IBM Blockchain for Healthcare

The administration and access control of medical records and data are intended to be revolutionized by blockchain implementation in IBM Blockchain for Healthcare. Fundamentally, the blockchain indexes all user health records and data, acting as an access-control manager. The blockchain indexes contain transaction timestamps, encrypted linkages to health records, unique user identities, and metadata for quick and easy access to data, much like a library's card catalog. This method guarantees the safe monitoring of personal health information for the duration of an individual's life, including information gleaned via wearable sensors, mobile apps, and formal medical records. A separate data lake, scalable and able to hold a variety of data kinds, including documents, images, and key-value stores, is also included in the architecture[62].

IBM Healthcare implements blockchain technology to change medical records data management and access control. The blockchain serves as an access-control manager and index of all user health information and data. Similar to a library's card catalog, the blockchain indexes comprise timestamps for transactions, encrypted connections to medical records, distinct user identities, and metadata for rapid and simple data retrieval. This approach ensures that personal health data, including that obtained from official medical records, wearable sensors, and mobile apps, is safely monitored throughout an individual's life.

4.6 Nebula Genomics Blockchain

With personal genomics becoming increasingly popular, the proposed blockchain system solves essential concerns about the security and privacy of genomics data. Notably, issues have surfaced about the possibility of government access to genomics databases, the transparency of data utilization by personal genomics companies, and the dangers of discrimination based on genetic information. The framework prioritizes privacy by supporting pseudo-anonymous transactions made possible by cryptocurrencies such as Bitcoin, promoting user anonymity. This lowers the risk of security breaches and data misuse by enabling people to purchase genetic testing services while minimizing the acquisition of personally identifiable information. Furthermore, the framework recognizes the limitations of blockchain anonymity and suggests using cryptographic methods to improve user privacy and confidentiality in blockchain transactions, including genetic data, such as zero-knowledge proofs[64].

The framework for the genomics blockchain promotes user-centric data access control, enabling people to own the encryption keys for their genomics data. Using a decentralized method reduces the risk of data breaches and unauthorized access as there is less reliance on centralized genomics databases managed by genomics companies. By dispersing data access control, delegated access control improves security and transparency. It involves several independent organizations holding shares of encryption keys. The framework also highlights how crucial record auditability is and how blockchain technology makes this possible by allowing for clear communication of user consent, data sharing permissions, and requests for access to data. The framework utilizes blockchain technology to create unchangeable records, which fosters trust, encourages data exchange, and guarantees accountability in the handling and examining of genetic data.

5 Conclusion

Blockchain technology is an exciting prospect in healthcare. In this literature review we highlight the initiatives taken by researchers in the field of blockchain to implement the DLT in healthcare. After the success of blockchain in the finance industry, its acceptance is increasing in other sectors. The initiatives are discussed in chapter 4 concerning the implementations of DLT in healthcare. It can enhance patient data handling and security. However, several important issues must be resolved to realize this potential fully. Due to the blockchain trilemma, the blockchain network cannot simultaneously optimize decentralization, scalability, and security, especially regarding open blockchains. Regulatory compliance is still a significant worry because strict data protection rules like HIPAA and GDPR require blockchain solutions to be carefully aligned with legal standards. For smooth interoperability, data must be standardized, and standard data formats and protocols must be established. Creating standardized interfaces is necessary to achieve interoperability, guaranteeing that various blockchain systems can successfully communicate and exchange data. Comprehensive user education initiatives are necessary to ensure that patients and healthcare professionals know the advantages and workings of blockchain technology, which helps promote trust and acceptance.

Table 3 compares the blockchain networks with transaction fees in dollars and speed in TPS (transactions per second). These are the 15 highest market cap blockchain networks likely to be used for a healthcare application and are well-defined frameworks that provide clear guidance for all. As blockchain technology develops, it is anticipated to become more trustworthy and user-friendly, making deployment easier. Coordinated efforts and standardized communication protocols are necessary to build a smooth and connected healthcare environment and efficiently integrate blockchain with other developing technologies, such as AI and IoT. Blockchain technology has the potential to significantly improve healthcare services by providing safe, effective, and patient-centered solutions for data management and care delivery. Blockchain technology brings more innovative solutions to healthcare and better approaches to these problems.

The inadequacies of traditional methods such as paper-based and fragmented electronic health records in fulfilling industry expectations have led to the advent of DLT in the healthcare domain. Its decentralized structure, immutability, and cryptographic security are viable foundations for strengthening data security and giving patients more control over their health information. This study highlights how DLT changes healthcare applications by examining projects such as MedRec, Medical-chain, and others. These initiatives demonstrate how blockchain technology may increase transparent data sharing, expedite the control of patient data in their own hands, and encourage data exchange across healthcare stakeholders with more verifiable data. This research highlights the possibilities of DLT implementations in the healthcare domain with potential improvements in the domain by incorporating interoperability and transparency. The introduction of DLT opens a new paradigm for healthcare stakeholders searching for solutions which improves health data sharing security and patient privacy control, while promoting proactive patient involvement in their health ecosystem. In table 4, we discuss the key benefits and use cases of distributed ledger technology and blockchain in healthcare.

Table 3 Comparison chart of blockchain networks and the Transaction Fee (Dollars) and Speed (Transaction Per Second)

Name	**Transaction fee (Dollar)**	**Speed (TPS)**
Ethereum (ETH)	10 to 100	15-30
Tether (USDT)	1.00	15-30
BNB	1.00	1000
Solana (SOL)	0.01	65,000
XRP	0.01	1,500
Avalanche (AVAX)	0.01 - 0.05	4500+

TRON (TRX)	0.001 - 0.005	2000+
Polkadot (DOT)	0.01 - 0.10	1000+
Polygon (MATIC)	0.001 - 0.005	7500+
Bitcoin Cash (BCH)	0.001 - 0.05	60+
Cosmos (ATOM)	0.01 - 0.10	100+
Stacks (STX)	0.01 - 0.10	30+
Ethereum Classic (ETC)	0.01 - 0.10	15+
Hedera (HBAR)	0.0001 - 0.001	10,000+
NEAR Protocol	0.01 - 0.05	4000+

Despite its advanced features, Blockchain technology has several limitations and challenges that impede its widespread adoption and hinder its progress. Foremost among them is the need for more standardization, which slows development and complicates interoperability between blockchain systems. Moreover, while decentralized storage is a defining characteristic of blockchain, it raises concerns regarding privacy leakage and critical management. Ensuring data security stored on the blockchain ledger demands intricate cryptographic processes involving private and public keys.

Additionally, scalability remains a pressing issue, particularly in healthcare environments, where the increasing number of patients strains the computational resources. Furthermore, the technology is vulnerable to many specific vulnerabilities, including block withholding attacks, 51 percent attacks, double spending attacks, selfish mining attacks, eclipse attacks, block discarding attacks, difficulty raising attacks, and anonymity issues in blockchain technology that expose it to malicious exploits like identity theft and data exfiltration. Addressing these limitations and vulnerabilities is crucial for unlocking the full potential of blockchain technology and fostering its widespread adoption across diverse sectors.

Table 4 Distributed Ledger Technology Key benefits and use cases in bio medical healthcare

Distributed Ledger Technology Key benefits	**Improve medical record management**	**Enhance insurance claim process**	**Accelerate Research**	**Advance healthcare data**
Decentralized Management	The distributed ledger technology and digital wallets enable patients to manage their health record online. This removes all obstacles for gaining access or transferring of their medical data to another healthcare provider [66].	Real time claim processing becomes easy and transparent by replacing the health plan intermediation with transparent blockchain technology [67].	Institutions can keep full control of their computational resources while collaborating with other institutes by sharing data and analysis [68].	Decentralized health data becomes the backbone for digital health, incorporating data from patient-based and EMR systems to provide a data-pool, from which authorized users can access it [69].
Immutable Audit Trail	The data is unalterable, the stored data on private blockchain cannot be changed by anybody including healthcare providers and patients [70].	Based on blockchain immutability, claim auditing and fraud detection becomes more smooth for the payer and insurers [71].	Personal patient generated data with timestamp is available, this trackable data is available to research [72].	The distributed network of nodes contains the timestamped, tamper proof, continuously updated data. This could be adapted for basic and experimental model science.
Data Provenance	The medical records are verifiable and signed by the source, false records are plausibly denied [73].	The distributed Ledger Technology can address the problem of distributed nature of records with blockchain [74].	The MedRec Blockchian based health record and medical research data is enabled with crucial properties of provenance [75].	Altered and low quality medicine can be tracked and identified. Using blockchain the origin of the medicine product can be traced and transfer of ownership is clear and available to everyone [72].

Robustness/ Availability	Decentralized network advantage is that no single institution can be hacked or robbed to obtain a large number of patient records [66].	Enhance accessibility of patient data through decentralized ledger with online data access [71].	Healthcare data availability across the globe online for research and advancement of science and technology with decentralized blockchain networks. Real time data is accessible to improve emergency medical situations [76].	Blockchain enabled anti tampering capabilities during manufacturing, supply and disposition systems, which could make drug counterfeiting a non-issue [71].
Security/Privacy	The data is encrypted and only accessible with the private key of the patient. Even if the network is infiltrated the data is not readable [66].	Financial information is secured with the blockchain mechanism [71].	Individuals, healthcare providers, healthcare entities and medical researchers share vast amounts of genetic, diet, lifestyle, environmental and health data with security and privacy protection [76].	Patient centric consent management system.

Blockchain technology, characterized by its distributed transaction ledger and peer-to-peer network architecture, facilitates decentralized ownership of a ledger across all nodes within a network. The synchronization and verification of ledger updates occurs through a consensus protocol, eliminating the need for centralized authority. In the context of cross-regional sharing of electronic health records (EHRs), the transaction throughput of blockchain systems plays a crucial role in determining system performance, measured by the number of transactions processed per second. Adopting blockchain and DLT in healthcare has enhanced vital features such as availability, confidentiality with encryption, immutability, privacy, anonymity, increased data access speed, and transparency with decentralization.

Blockchain technology has the ability to greatly improve cyberattack resistance and security. The data authentication procedure in the developing Web5 technologies landscape will be significantly impacted by blockchain technology. Blockchain technology solves the issue of duplicate spending by introducing an extra degree of protection, which is especially important in the financial industry. Double spending is a major risk in financial transactions, but it's not the main problem in other areas, such as in the healthcare industry. In this case, protecting the confidentiality, accessibility, and integrity of sensitive medical data is the main priority.

Acknowledgements. This work is supported by the project Blockchain.PT (PRR – RE-C05-i01.02: AGENDAS/ALIANÇAS VERDES PARA A INOVAÇÃO EMPRESARIAL)

References

[1] Anthony Jnr., B. (2022). 'Toward a collaborative governance model for distributed ledger technology adoption in organizations'. *Environ. Syst. Decis.,* 42: 2, 276–294.

[2] Soltani, R., Zaman, M., Joshi, R. and Sampalli, S. (2022). 'Distributed ledger technologies and their applications: A review'. *Appl. Sci. (Basel),* 12: 15, 7898.

[3] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[4] Monrat, A.A. and Schel´en, O., and Andersson, K. (2022). Applicability analysis of blockchain technology.

[5] Sunyaev, A. (2020). 'Distributed ledger technology. Internet computing: Principles of distributed systems and emerging internet-based technologies'. 265–299.

[6] Thakur, A. (2022). 'A comprehensive study of the trends and analysis of distributed ledger technology and blockchain technology in the healthcare industry'. *Frontiers in Blockchain,* 5, 844834.

[7] Ben Fekih, R. and Lahami, M. (2020). 'Application of blockchain technology in healthcare: A comprehensive study'. 268–276.

[8] Sarkis-Onofre, R., Catal´a-L´opez, F., Aromataris, E. and Lockwood, C. (2021). 'How to properly use the prisma statement'. *Systematic Reviews,* 10, 1–3.

[9] Welch, V., Petticrew, M., Petkovic, J., Moher, D., Waters, E., White, H., Tugwell, P., Atun, R., Awasthi, S., Barbour, V., *et al.* (2016). 'Extending the prisma statement to equity-focused systematic reviews (prisma-e 2012): explanation and elaboration'. *Journal of Clinical Epidemiology,* 70, 68–89.

[10] Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. and PRISMA Group*, t. (2009). 'Preferred reporting items for systematic reviews and meta-analyses: the prisma statement'. *Annals of internal medicine,* 151: 4, 264–269.

[11] Briner, R.B. and Denyer, D. (2012). 'Systematic review and evidence synthesis as a practice and scholarship tool'.

[12] Page, M.J., McKenzie, J.E., Bossuyt, P., and Boutron, I. (2021). 'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews'. *J. Clin. Epidemiol,* 134, 178–189.

[13] Alzahrani, S., Daim, T. and Choo, K.-K.R. (2023). 'Assessment of the blockchain technology adoption for the management of the electronic health record systems. IEEE Trans'. *Eng. Manage,* 70: 8, 2846–2863.

[14] Sonkamble, R.G., Phansalkar, S.P., Potdar, V.M. and Bongale, A.M. (2021). 'Survey of inter-operability in electronic health records management and proposed blockchain-based framework: MyBlockEHR'. *IEEE Access,* 9, 158367–158401.

[15] Zukaib, U., Cui, X., Hassan, M., Harris, S., Hadi, H.J. and Zheng, C. (2023). 'Blockchain and machine learning in ehr security: A systematic review'. *IEEE Access,* 11, 130230–130256.

[16] Andrew, J., Isravel, D.P., Sagayam, K.M., Bhushan, B., Sei, Y. and Eunice, J. (2023). 'Blockchain for healthcare systems: Architecture, security challenges, trends and future directions'. *Journal of Network and Computer Applications,* 103633.

[17] Elghoul, M.K., Bahgat, S.F., Hussein, A.S. and Hamad, S.H. 'Securing patient medical records with blockchain technology in cloud-based healthcare systems'. *International Journal of Advanced Computer Science and Applications,* 14: 11.

[18] Zhang, P., Kelley, A., Schmidt, D.C. and White, J. (2023). 'Design pattern recommendations for building decentralized healthcare applications'. *Frontiers in Blockchain,* 6, 1006058.

[19] Karmakar, R. and Dutta, S. (2022). 'Formal verification of a medical insurance system prototype: The event-b modeling approach'. *Journal of Information Assurance & Security,* 17: 1.

[20] Pillai, A., Ramachandran, A.V. and Saraswat, V. (2022). 'Design considerations for protection of blockchain based digital identity ecosystem'. *Journal of Information Assurance & Security,* 17: 3.

[21] Samanta, S., Sarkar, A., Singh, P. and Singh, P. (2021). 'Blockchain and iot based secured future city architecture'. *Journal of Information Assurance & Security,* 16: 4.

[22] Mills, D., Wang, K., Malone, B., Ravi, A., Marquardt, J., Chen, C., Badev, A., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M., Ng, W. and Baird, M. (2016). 'Distributed ledger technology in payments, clearing, and settlement'. *Fin. Econ. Discuss. Ser.,* 2016: 095.

[23] Deshpande, A., Stewart, K., Lepetit, L. and Gunashekar, S. (2017). 'Distributed ledger technologies/ blockchain: Challenges, opportunities and the prospects for standards'. *Overview report The British Standards Institution (BSI),* 40, 40.

[24] Mogavero, F., Visconti, I., Vitaletti, A. and Zecchini, M. (2021). 'The blockchain quadrilemma: When also computational effectiveness matters'. *2021 IEEE Symposium on Computers and Communications (ISCC),* 1–6.

[25] Trump, B.D., Florin, M.-V., Matthews, H.S., Sicker, D. and Linkov, I. (2018). 'Governing the use of blockchain and distributed ledger technologies: not one-size-fits-all'. *IEEE Engineering Management Review,* 46: 3, 56–62.

[26] Leekha, S. (2018). 'Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world'. *FIIB Business Review,* 7: 4, 275–276.

[27] Linkov, I., Trump, B.D., Poinsatte-Jones, K. and Florin, M.-V. (2018). 'Governance strategies for a sustainable digital world'. *Sustainability,* 10: 2, 440.

[28] Bouras, M.A., Lu, Q., Zhang, F., Wan, Y., Zhang, T. and Ning, H. (2020). 'Distributed ledger technology for ehealth identity privacy: State of the art and future perspective'. *Sensors,* 20: 2, 483.

[29] Underwood, S. (2016). 'Blockchain beyond bitcoin'. *Communications of the ACM,* 59: 11, 15–17.

[30] Sucharitha, G., Aditya, G.S., Varsha, J. and Nikhil, G.S. (2023). 'Electronic medical records using blockchain technology'. *EAI Endorsed Transactions on Pervasive Health and Technology,* 9.

[31] Abdelgalil, L. and Mejri, M. (2023). ‘Healthblock: A framework for a collaborative sharing of electronic health records based on blockchain’. *Future Internet,* 15: 3, 87.

[32] Bigini, G., Zichichi, M., Lattanzi, E., Ferretti, S. and D’Angelo, G. (2022). ‘Decentralized health data distribution: A dlt-based architecture for data protection’. *2022 IEEE International Conference on Blockchain (Blockchain),* 97–104.

[33] Nagasubramanian, G., Sakthivel, R.K., Patan, R., Gandomi, A.H., Sankayya, M. and Balusamy, B. (2010). ‘Securing e-health records using keyless signature infrastructure blockchain technology in the cloud’. *Neural Computing and Applications,* 32, 639– 647.

[34] Hussain, S., Rahman, H., Abdulsaheb, G.M., Al-Khawaja, H. and Khalaf, O.I. (2023). ‘A blockchain-based approach for healthcare data interoperability’. *International Journal of Advances in Soft Computing & Its Applications,* 15: 2.

[35] Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E. and Ylianttila M. (2018). ‘Blockchain utilization in healthcare: Key requirements and challenges’. *IEEE,* 1–7.

[36] Zakzouk, A., El-Sayed, A. and Hemdan, E.-D. (2023). ‘A blockchain-based electronic medical records management framework in smart healthcare infrastructure’. *Multimed Tools Appl,* 82, 35419–35437.

[37] Pilares, I., Azam, S., Akbulut, S., *et al.* (2022). ‘Addressing the challenges of electronic health records using blockchain and ipfs’. *Sensors,* 22: 11, 4032.

[38] Shahnaz, A., Qamar, U. and Khalid, A. (2019). ‘Using blockchain for electronic health records’. *IEEE ACCESS,* 7, 147782–147795.

[39] O’Donoghue, O., Vazirani, A., Brindley, D. and Meinert, E. (2019). ‘Design choices and trade-offs in health care blockchain implementations: Systematic review’. *J Med Internet Res,* 21.

[40] Puneeth, R. and Parthasarathy, G. (2023). ‘Survey on security and interoperability of electronic health record sharing using blockchain technology’. *Acta Informatica Pragensia,* 12, 160–178.

[41] Panigrahi, A., Nayak, A. and Paul, R.: (2022). ‘Healthcare ehr: A blockchain-based decentralized application’. *International Journal of Information Systems and Supply Chain Management,* 15.

[42] Rao, K. and Naganjaneyulu, S. (2021). ‘Permissioned healthcare blockchain system for securing the ehrs with privacy preservation. Ingenierie des Systemes d39’. *Information,* 26, 393–402.

[43] Lee, S., Kim, Y. and Cho, S. (2024). ‘Searchable blockchain-based healthcare information exchange system to enhance privacy preserving and data usability’. *Sensors,* 24: 5, 1582.

[44] Soni, P., Islam, S.H., Pal, A.K., Mishra, N., Samanta, D. (2024). ‘Blockchain-based user authentication and data-sharing framework for healthcare industries’. *IEEE Transactions on Network Science and Engineering.*

[45] Wang, T., Wu, Q., Chen, J., Chen, F., Xie, D. and Shen, H. (2024). ‘Health data security sharing method based on hybrid blockchain’. *Future Generation Computer Systems,* 153, 251–261.

[46] Manoj, T., Makkithaya, K. and Narendra, V. (2022). ‘A blockchain based decentralized identifiers for entity authentication in electronic health records’. *Cogent Engeneering,* 9: 1.

[47] Deepa, V., Thamotharan, B., Mahto, D., *et al.* (2023). ‘Smart embedded health monitoring system and secure electronic health record (ehr) transactions using blockchain technology’. *Soft computing, 27,* 12741–12756.

[48] Dubovitskaya, A., Baig, F., Xu, Z., *et al.* (2020). ‘Action-ehr: Patient-centric blockchain-based electronic health record data management for cancer care’. *J Med Internet Res,* 22.

[49] Yang, J., Onik, M., Lee, N.-Y., *et al.* (2019). ‘Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making’. *Applied Sciences (Switzerland),* 9.

[50] Lakshmanan, M. and Anandha Mala, G. (2024). ‘Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm’. *Knowledge and Information Systems,* 66: 1, 481–509.

[51] Barman, S., Chattopadhyay, S., Samanta, D. and Barman, S. (2022). ‘A blockchain-based approach to secure electronic health records using fuzzy commitment scheme’. *Security and Privacy,* 5: 4, 231.

[52] Patel, V. (2019). ‘A framework for secure and decentralized sharing of medical imaging data via blockchain consensus’. Health Informatics J, 25, 1398–1411.

[53] Preetha, A. and Kumar, T. (2023). ‘Securing iot-based healthcare systems from counterfeit medicine penetration using blockchain’. Applied Nanoscience, 13, 1263–1275.

[54] Gohar, A., Abdelmawgoud, S. and Farhan, M. (2022). ‘A patient-centric healthcare frame-work reference architecture for better semantic interoperability based on blockchain, cloud, and iot’. IEEE Access, 10, 92137–92157.

[55] Hylock, R. and Zeng, X. (2019). ‘A blockchain framework for patient-centered health records and exchange (healthchain): Evaluation and proof-of-concept study’. J Med Internet Res, 21: 8.

[56] Uddin, M., Memon, M. and Memon, I. (2021). ‘Hyperledger fabric blockchain: Secure and efficient solution for electronic health records’. Computers, Materials and Continua, 68, 2377–2397.

[57] Reegu, F.A., Abas, H., Jabbari, A., Akmam, R., Uddin, M., Wu, C.-M., Chen, C.-L., Khalaf, O.I., et al. (2022). ‘Interoperability requirements for blockchain-enabled electronic health records in healthcare: A systematic review and open research challenges’. Security and Communication Networks, 2022.

[58] Ekblaw, A. and Azaria, A. (2016). ‘Medrec: Medical data management on the blockchain’. Viral Communications.

[59] Shen, B., Guo, J., Yang, Y. (2019). ‘Medchain: Efficient healthcare data sharing via blockchain’. APPLIED SCIENCES-BASEL, 9.

[60] Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K. and Njilla, L. (2017). ‘Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability’, in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468–477.

[61] McFarlane, C., Beer, M., Brown, J. and Prendergast, N. (2017). Patientory: A healthcare peer-to-peer emr storage network v1. Entrust Inc., 3, 19.

[62] Panwar, A., Bhatnagar, V., Khari, M., Salehi, A.W., Gupta, G., et al. (2022). ‘A blockchain framework to secure personal health record (phr) in ibm cloud-based data lake’. Computational Intelligence and Neuroscience, 2022.

[63] Kim, J.Y. (2018). ‘A comparative study of block chain: Bitcoin· namecoin· medibloc’. Journal of Science and Technology Studies, 18: 3, 217–255.

[64] Grishin, D., Raisaro, J.L., Troncoso-Pastoriza, J.R., Obbad, K., Quinn, K., Misbach, M., Gollhardt, J., Sa, J., Fellay, J., Church, G.M., et al. (2021). ‘Citizen-centered, auditable and privacy-preserving population genomics’. Nature Computational Science, 1: 3, 192–198.

[65] Karmakar, A., Ghosh, P., Banerjee, P.S., De, D. and Pande, A. (2024). ‘Medichain: medical data fusion using blockchain integrated elastic storage’. Multimedia Tools and Applications, 83: 6, 17873–17895.

[66] Ivan D. Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

[67] Culver K. Blockchain Technologies: A whitepaper discussing how the claims process can be improved. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

[68] Kuo T-T, Hsu C-N, Ohno-Machado L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

[69] Goldwater J. The use of a blockchain to foster the development of patient-reported outcome measures. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

[70] 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(10):218.

[71] Attili S, Ladwa SK, Sharma U, Trenkle AF. Blockchain: the chain of trust and its potential to transform healthcare – our point of view. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.

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

[73] Blough D, Ahamad M, Liu L, Chopra P. MedVault: Ensuring security and privacy for electronic medical records. NSF CyberTrust Principal Investigators Meeting. 2008. http://www.cs.yale.edu/cybertrust08/posters/posters/158 medvault poster CT08. pdf. Accessed December 20, 2016.

[74] Vian K, Voto A, Haynes-Sanstead K. A blockchain profile for medicaid applicants and recipients. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/ NIST; 2016.

[75] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:25–30.

[76] Linn LA, Koo MB. Blockchain for health data and its potential use in health IT and health care related research. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST; 2016.