Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

# A Comprehensive Review of Blockchain-Enabled Open-Source Tools for Managing Electronic Health Records (EHR) in Hospitals

**Zahid Hussain Shaik[1], Kelapati poonia[2]**

[1]Research Scholar, [2]Assistant professor, Shri JJT University, Chudela, Rajasthan, India.

**Email:** [1]sah.ssk@gmail.com, [2]kelapatipoonia@gmail.com

**Abstract**

Currently, blockchain technology is becoming the potential innovation within a healthcare sector. This systematic review studies the literature regarding blockchain and blockchain adoption in healthcare with an emphasis on hospital Electronic Health Record (EHR) management. This study presents two objectives - identifying gaps in the current research pipeline and suggesting future research recommendations. The first task as part of the study is to analyze the opportunities and challenges associated with applying blockchain technology in the healthcare sector. To accomplish these objectives and assess the position of blockchain technology in the field, a systematic literature review was performed using credible scientific databases and conference papers. Some of the terms from the study glossary that were used as literature search terms included "Blockchain," "implementation," Of the relevant articles originally selected, 32 articles were deemed relevant of which 26 articles contained the elements necessary to conduct factor analysis. The authors of the selected articles presented the analysis of a framework for EHR management in 22 of these articles, that included classification, implementation forms and research gaps. This review shows that there are potential advantages to using blockchain technology in healthcare notable benefits include better data security, improved interoperability, and enhanced patient privacy. A transaction in Blockchain (Ethereum) cost 8 US cents. The evaluation of performance included a designed assessment and metrics that includes, 18.29 s execution time, throughput with 100 to 500 users for a period of 10 to 35, and a latency of 14ms. Among the very important contributions of this review was identifying existing research gaps and providing an exploratory analysis to inform future research efforts. By identifying these gaps, researchers can continue to investigate innovative blockchain applications in healthcare and apply its implementation across a range of clinical scenarios. As part of using blockchain technology to implement EHR management; this systematic review adds to existing scholarship on implementing blockchain technology in healthcare.

**Keywords:** Blockchain, Literature Analysis, Healthcare, EHR, Articles, Health Record Management.


*DOI: https://doi.org/10.36548/jtcsst.2025.3.011*
*Received: 15.07.2025, received in revised form: 16.08.2025, accepted: 01.09.2025, published: 12.09.2025*

## 1. Introduction

The popularity of blockchain technology has rapidly increased since Bitcoin launched in late 2009. A blockchain architecture does not require centralized authority but utilizes a distributed ledger [8], which adds a layer of security to the system. Blockchain has been proposed for use in several industries in the past decade, such as agriculture, e-currency, cyber security, banking, etc. Despite this, only a few healthcare papers discuss Electronic Health Record management, which is crucial for patients, hospitals, and insurance companies. The literature search was carried out using several academic library databases, including EBSCO, ProQuest Central, and Omren Masader. A complete empirical basis was used for the referenced and studied articles. The following factors were considered merit when selecting articles: the complete text, the article structure and direction, the impact, criticism and evaluation, and the conclusions [17]. The advantages and disadvantages of blockchain were compared to determine whether blockchain can be implemented in healthcare. The EHR strategy was reviewed, and performance factors were incorporated into its design and implementation. An in-depth literature review was conducted to determine the limitations, complex issues, and interventions in-hospital monitoring and management [9] reviews are either generic (Efendi et al. [11], Casino et al. [12]) or domain-limited; this paper uniquely classifies open-source blockchain EHR tools and evaluates them.

## 2. Literature Review

Healthcare is one of the industries with a high potential for using blockchain technology to manage safe medical data. This technology employs a decentralized approach to provide access control and clinical trials in a patient-centered manner. In terms of the literature collected, the author's comparison of the research identifies the obstacles and issues associated with blockchain privacy, as well as data security in the many application areas within distributed networks [18]. The studies that have been published tilt toward blockchain technology, and 80% of the study articles focus on electronic health record management applications with technological platforms for implementation, with the goal of increasing the impact of peer-to-peer devices [10].

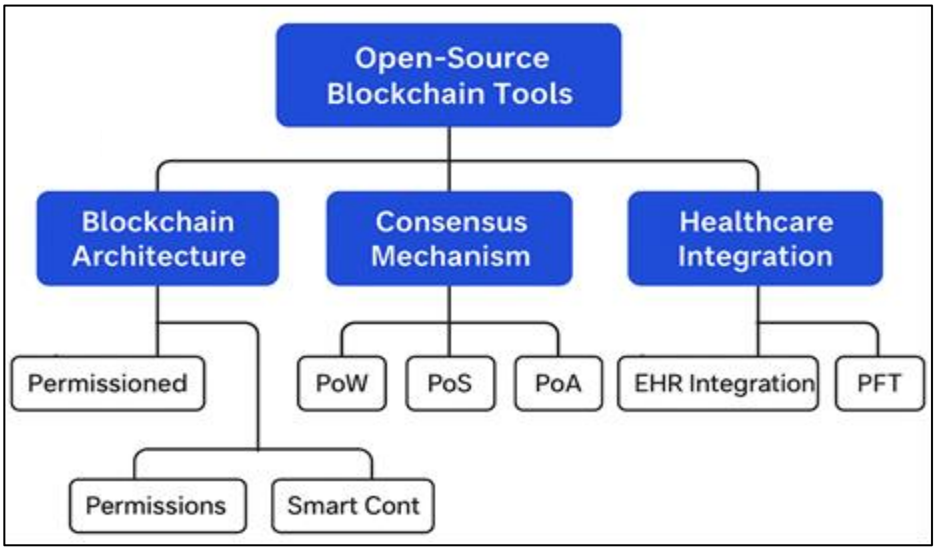


**Figure 1.** Open Source Blockchain Tools Classification

Furthermore, open-source blockchain tools can be broadly categorized into three categories, as shown in Figure 1. As a result, blockchain architecture emphasizes permissioned systems where only a small subset of participants can access and validate transactions. The taxonomy of open source blockchain tools can be classified into three categories: blockchain architecture, consensus mechanisms, and healthcare integration. Under blockchain architecture, permissioned systems are emphasized, where only authorized participants can access and validate transactions, ensuring security and controlled participation. In this respect, permissions assign roles and rights for participants and smart contracts; it is important to explain permissions in more detail. Importantly, smart contracts are self-executing protocols that automate rules and processes on the blockchain. Consensus mechanisms comprise the second category and are the means of achieving agreement on the validity of transactions on the blockchain between nodes on the network. There are a few consensus mechanisms associated with blockchains, such as, Proof of Work (PoW) which incentivizes nodes based on computational power and consumes a significant amount of energy, Proof of Stake (PoS) which incentivizes a validator who owns tokens in the network and consumes a fraction of the energy of PoW, and Proof of Authority (PoA) in which trusted authorities validate, creating speed but also limiting decentralization capabilities. The third category includes healthcare integrations where blockchain serves as a method to manage sensitive health data. This includes Electronic Health Record (EHR) which allows secured sharing and access to records for patients and organizations, and Privacy, Fairness, and Transparency (PFT) which ensures the confidentiality, ethical use and transparent treatment of healthcare data. These categories demonstrate how open-source blockchain tools can be organized around design, validation, and application to work from both technical and domain perspectives.

The first counterfeit involves the storage of medical data, which is more sensitive. The attacks and failure of medical data raise various problems regarding Wirst and Gervais' decision model [1]. The factors at play are data storage and access by several parties. Blockchain should be used in both public and private permissionless contexts to promote mutual trust and shared access. The literature review found that the blockchain order has evolved, and blockchain technology has substantial applications in healthcare [5].

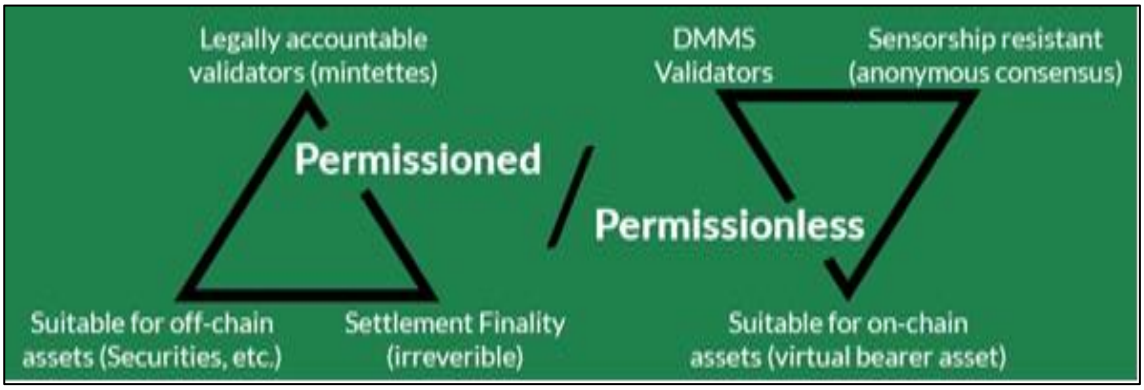


**Figure 2.** Blockchain Security (Source: www.engineerbabu.com)

Currently, blockchain has more relevance in the field, as the importance of blockchain has been infiltrating various sectors. The blockchain has an operational infrastructure relative to several healthcare startups. The care startup, Gem Health has great collaboration on promoting integrity, security, and easy transferral. Similarly, Cyph, MedRec, and Guardtime are delivering secure medical records using digital identities and management [2]. This technology also helps to lessen risk of security breaches in the healthcare industry, and provides a reliable way for trustworthy digital protection [7]. Figure 3. shows the Medical Organizational Structure.

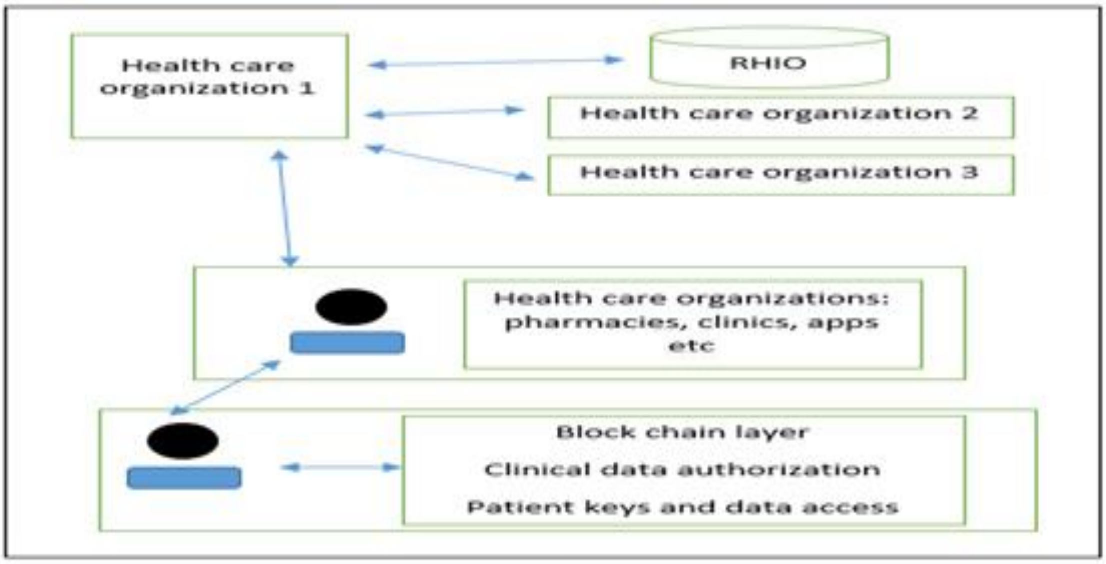


**Figure 3.** Medical Organizational Structure

According to William J. Gordon et al., [3] blockchain technology involves five different mechanisms, digital access, liquidity, patient identification, identity, and immutability of data [19]. Healthcare organizations should position themselves to become interoperable in order to provide an incentive for institutions and patients. This operability has a historical need, and organizations justify integration to preserve the medical data [6].

Some of the challenges examined in the existing work are:

1. Evolvability anywhere in the system packing of health support
2. Incompetent data access online [20]
3. Some apprehensions like privacy, data transparency, and applicable data recording events.

## 3. Research Methodology

Between January 2017 and July 2020, a literature search was conducted for journal articles and conferences. Scientific databases such as Scopus, Ebsco, PubMed, IEEE Transactions, IEEE Conferences, and Periodicals were used as master search criteria. The search terms included blockchain, electronic health record management [21], healthcare, and informatics [11]. Grey literature or unpublished work was not included in the review; only full publications with relevant titles were assessed for relevance.

**Evaluation and Selection:** We used distinct criteria for inclusion, taking into account language, area/theme, keyword, full article, year, respected publications, and download restrictions. The exclusion criteria included abstracts, unfinished articles, unpublished work, and articles with no relevance. Likewise, if any article did not belong in the group due to inappropriate detail, it was also subject to exclusion criteria.

**Synthesis:** The articles reviewed were analyzed appropriately to match the most recent trends and themes and were double-checked using qualitative analysis software (MAXQDA11). The authors reviewed and independently agreed on the content analysis by synthesizing the themes and sub-themes as well.

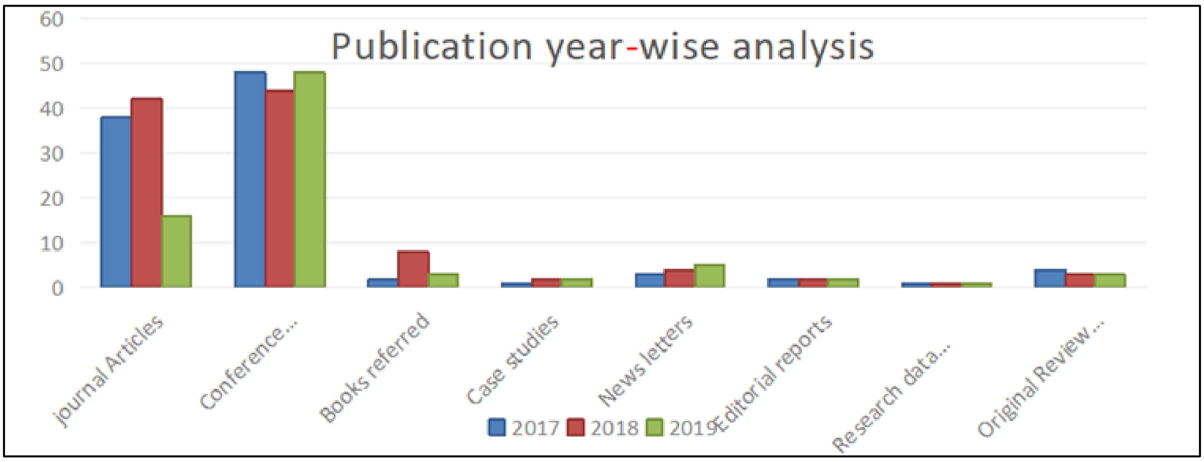


**Figure 4.** The Distribution of Publications Over Time for the Literature Review Performed

Subjective and Descriptive analysis: We analyzed 226 articles published from 2017 to 2020 and excluded gray literature to narrow the scope of this analysis. This analysis aims to provide insights and trends regarding current links with blockchain technology and how software connected to the blockchain is used as an implementation tool. The second purpose of this analysis was to establish the methods used in multidisciplinary applications. The final aspect of this analysis consisted of highlighting issues such as privacy, security, and interoperability for users of records. Every paper in this study is considered worthwhile in terms of quality literature over time.

The illustrations of the selected papers and the underlying blockchain have shown preferable solutions with structuring to provide governance for IoT, data management, and healthcare applications. Thus, this literature review has been conducted to devise and implement a novel mechanism for Electronic Health Records (EHRs) management using blockchain technology in hospitals in Oman. Blockchain applications are primarily focused on overall efficiencies and scalability. The literature studied focuses on single characteristics, scenarios, and datasets that align well with industry applications.

The methodology adopted in the literature review is articulated in the following steps:

1. **Investigation strategy:** The topics and questions related to the chosen technology.
2. **Searching:** Initially, renowned libraries are selected and explored to outline the findings.
3. **Selection of articles:** Criteria and topics as per the planned research study.
4. **Study and distribution:** Chronological order followed by suitable mapping.
5. **Extraction of data:** Medical record data storage and privacy with quality assessment.

## 4. Results and Discussion

The literature review aims to build on existing research and contribute to the growing interests in blockchain and electronic health record management in hospitals [24]. Electronic Medical Records Management provides security for human health records using a controlled, private blockchain system known as Hyperledger fabric [23] and provides patients complete control over their medical information management. In earlier research, blockchain platforms were created and experimented with to display medical data or control access [14]. In medical chain management, the blocks are differentiated as patient, doctor, hospital and insurance providers. Patients have the maximum access since they can appoint a doctor in any hospital [25].

**Table 1.** Summary of Literature

| Authors | Publisher & year | Objectives | Design methods | Limitations and strengths | Type of research | Improvements | Evaluation and performance Parameters |
|---|---|---|---|---|---|---|---|
| Lanxiang Chen et al. [1] | Elsevier & 2019 | The EHRs are encrypted to perform symmetric encryption and store in cloud server. | Data Owner uses complex Boolean expression to construct Index. The Index and the smart contracts will be stored in blockchain (Ethereum). The Proposed Scheme is Setup, Build Index, Enc, Trapdoor, Search) | The users (can be new hospital); this needs the index to obtain the EHRs for a patient. | Qualitative | The experiments are performed on a computing system; implementation of codes was in Python 2.7. | EHRs from the cloud provides a token, responsible person can access smart contracts. |
| Liehuang Zhu et al. [2] | Elsevier & 2018 | The proposed work is controllable blockchain data management (CBDM) model. | Bilinear Pairing and Threat Model<br>1. System initialization: System Setup (providing public key and private key)<br>2. Document Modification phase: (Request (Users), Verification (BS), Vote (TA), Count (TA)) | Introduced Trusted Authority (TA) as it is designed to prevent attacks and any modification in documents 3 phases in this proposed system. Here the EHRs are stored. | Qualitative | Trust Authority (TA), Cloud Server (CV), Blockchain System (BS) | The proposed model is effective and correct in terms of cost. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Sheng Cao et al. [3] | Elsevier & 2019 | A secure cloud-assisted eHealth system called TP-EHR is proposed. Consists of simply (Cloud Storage, and Block chain) | Setup: Creation of an account in Ethereum<br>Appointment: Key<br>Store: Hash value, C Language used for coding and MIRACL Library used for implementation | 1. Secured against modification attacks<br>2. Blockchain itself warranty the integrity secured against forgery<br>3. Secured against impersonation attacks (password guessing) | Qualitative | Investigation to enhance eHealth Systems using blockchain, especially to improve the Quality of service (QoS). | A transaction in Blockchain (Ethereum) that costed 8 US cents, which Authors claimed to be acceptable. |
| Kristen N. Griggs et al. [4] | Springer & 2018 | To implement Hyper ledger instead of Ethereum.<br>To improve privacy by introducing anonymizers.<br>Private blockchain. | Raw data (EHRs) sent to Smart devices (phone/tablet)<br>Smart Contracts receive the data and alert the patient and the hospital.<br>The data will be forwarded to storage database, using EHRs and APIs. | 1. Maintaining the security to every node.<br>2. Usage of any additional ciphering techniques. | Quantitive | Ethereum protocol-based smart contracts are used to provide security and manage access for the healthcare data records. | Performance evaluation is done in High level of availability as all records are duplicated. |
| Xiao Yue et al. [5] | Springer & 2016 | The proposed work is an Application of Healthcare Data Gateway based on Blockchain to enable patient to own, control and share | Data Organization Model: Indicator-Centric Schema (ICS) is a unified data schema. ICS stores the data in a table format to make it easy to gather the data under certain categories/type. There are 3 layers: Storage Layer: To keep data secure. Data Management Layer: | Blockchain used as storage system. Simple ICS model. MPC is used for securing the raw data, as the user is asked to process the | Qualitative | No 3rd party involvements<br>*Two types of Access; Raw Purpose, Process Purpose | No evaluation is done for the model. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | their own data. | This Layer has firewall. Data Usage Layer: This Layer consist of the users. | data in Blockchain. | | | |
| Peng Zhang et al. [6] | Elsevier & 2018 | An architecture "FHIR Chain" is presented. | 1. Model--> Block chain<br>2. Controller--> Server to facilitates the interaction between the User Interface and Blockchain | **Increased modularity<br>Each component is independent in FHIR system.<br>Scalable data integrity<br>**Access control<br>Enhanced trust. | Qualitative | Mentioned about the experiments and which software was used. | Simulation to evaluate the model performance.<br>** Comparison between different number of blockchain configurations |
| Abdullah Al Omar et al. [7] | Elsevier & 2018 | Graphical User Interface (GUI) designed with Blockchain and Cryptographic functions. | ** Entities:<br>*Data sender (Patient)<br>*Data receiver: Look for the data, and the data is provided after authentication. | **Set of privacy and security requirements | Qualitative | Interoperability between different entities handling key theft/lost and key distribution techniques | **Security and privacy evaluation (theoretically)<br>Pseudonymity, Privacy, Integrity, Accountability, Security |
| Rui Guo et al. [8] | IEEE Access & 2018 | Multiple Authorities-Attribute-Based Signature (MA-ABS) scheme | 1. EHRs server (cloud storage)<br>2. N authorities are the organizations that are involved in medical data exchange | MA-ABS model provides anonymity and immutability of the EHRs. The security protocol under CBDH | Qualitative | Supporting general non-monotone Predicates in blockchain | The proposed (MA-ABS) model shows better performance in term of cost and |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Goce Gavrilov et al. [9] | International Centre for Slavic Education & 2019 | Entities: *Users: patients, doctors, pharmacists. | 1. Users interact with Database and Authentication centre by application layer | Focused on authentication and authorization part. | Qualitative | Practicality of the application | No Evaluation is done |
| Tiago Quaini et al. [10] | IADIS International Journal & 2018 | UniRec (Unified Medical Records) | 1. Contract Layer: Smart contracts written for the Ethereum Blockchain using Solidity<br>2. Model Layer: Adds/remove/query EHRs in P2P network using "IPFS JavaScript API".<br>3. Control Layer: For users to be able to interact with the application (using REST services) | The implementation of the model and study was carried out in 7 test cases; they were tested as a model; effectiveness is observed. The study case was limited to one organization and one patient. | Quantitative | Adding cost Using UniRec model with "Hyper ledger" Blockchain platform, as in this study they used "Ethereum" | The response time of new data queries |
| Syahril Efendi et al. [11] | MICoMS 2017 | Review Paper on Concept Designs, to secure Healthcare records using Blockchain. | 1. The data should be encrypted before connecting Blockchain (to keep the data confidential)<br>2. The data is collected.<br>3. The data is then submitted to Blockchain. | * Easy to understand the concept<br>* Simple and very brief Review | Review | In Blockchain, to secure data delivery between nodes, encryption "SHA-256" is used. | No Evaluation. Finally, Healthcare records can be viewed as analytical materials by the user's patient, hospital, etc. |
| Fran Casino et al. [12] | Elsevier & 2018 | To know the characteristics which can revolutionize the present trend of business practices. | The approach towards literature review is systematic, transparent, and scientific. However, the PRISMA statement is used to establish features in the process. This | The work has revealed the results of blockchain technology as scalable, efficient, and durable. The review mechanisms | Review | It is observed that big data and AI can be added to blockchain-based applications to | No Evaluation. The blockchain concepts are selected from diverse sectors to match the emerging |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | work includes the below steps.<br>1. Identify, Importance and review of the protocol<br>2. Quality assessment and data extraction<br>3. Data synthesis and report results. | and features are addressed for different applications and diverse themes. | | augment the technologies for transparency, scalability, and efficiency. | key themes in business, healthcare and IoT. |
| AYESHA SHAHNAZ et al. [13] | IEEE Access & 2019 | Use block chain technology in Electronic Health Record (EHR) management. Secure storage of health records framework. | Consensus Algorithm and a block was designed to explain the architecture steps of transaction process of user over blockchain network. Similarly, the design framework was proposed as user layer, blockchain layer, and system implementation as smart contracts. | Scalability, off-chain storage and Health record management, decentralization, data transparency, security, and privacy. The major strength through this work is security measures. | Qualitative | Blockchain in decentralized system by complying with certain rules, principles, and policies in healthcare sectors. | The performance is evaluated with a designed setup and metrics which include 18.29 s execution time, throughput with 100 to 500 users for a period of 10 to 35 and latency is 14ms. |
| David N. Taylor et al. [14] | National University of Health sciences & 2017 | The work is intended to review the latest trends and challenges of Electronic Health Records (EHR). | Review paper to discuss barriers and challenges in Electronic Health Record management. The literature covered various sources, such as pubmed, chiropractic literature, and allied health databases from 2005 to 2015. | Barriers, benefits, challenges, and possible directions in chiropractic profession were studied within the scope. The relevant review was performed with one person and interpretation. | Qualitative | The major findings and challenges in implementation with EHR in chiropractic practice were considered. | 45 papers were considered for literature paper. All the governmental policies, past experiences, studies, insurance commentaries, financial burdens, software implementation |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Jiang Duan et al. [15] | MDPI & 2020 | The major aim of this work is to analyze the literature content and implementation of food supply chain management. | The literature review suggested that 57 papers of literature were reviewed for food supply chain management. The approach defined six stage refinement process, such as databases, synthesis, findings, criteria, reports, and literature related. All the papers chosen were from conference and peer reviewed papers. | The blockchain technology in food chain has eliminated risks and tested with positive benefits by considering its focus mostly on food supply chain and collected related papers from 2008 to 2019. | Review | Use of IoT & RFID technology with current state of Food chain management does improve the efficiency and traceability. | No Evaluation. The food chain management was discussed with four benefits, such as traceability, transparency, efficiency |

**Recent Contributions**

Blockchain is considered an efficient solution for the secure management of Electronic Health Records (EHRs). Authors in [28] presented a review on the role of blockchain in EHR systems, highlighting the role of decentralized networks, encryption, and smart contracts in enhancing privacy, security, and efficiency in the healthcare sector. Certain researchers [29] evaluated the use of blockchain in data security, suggesting a prototype smart contract to increase the reliability, security, and interoperability of EHRs. Safeguarding patient information and adherence to privacy legislation were prioritized the most within this research. In [30], a systematic review was performed to examine the state of the art in managing EHRs. This research examined global interoperability standards and suggested an end-to-end secure blockchain-based architecture with an integration of various healthcare systems. Husnain et al. [30] suggested HealthChain, which is a blockchain-based EHR architecture with strong encryption and consent management. The research yields 30% less data access time, 40% improved interoperability, 50% less data breach, and a 35% increase in patient satisfaction, highlighting the potential of blockchain in the real world. The authors in [31] enhanced the research by using a blockchain-based framework for healthcare on Ethereum. The analysis proved that decentralization was a viable, real-world solution that effectively solved problems with cost and performance while also improving security and privacy. Furthermore, Mole and Shaji (2024) suggested an Ethereum blockchain model to automatically and anonymously transfer medical data using smart contracts and the InterPlanetary File System (IPFS). Their investigation demonstrated that blockchain technology can exchange EHRs safely and rapidly with a minimum latency of 14 ms [32].

**Summary**

This review shows that blockchain technology enables better data security and interoperability in relation to healthcare. In order to guide future research, [26] also identified a number of gaps in the literature, some of which are related to scalability and regulatory issues. The researchers, practitioners, and policymakers who wish to comprehend or apply blockchain technology in the healthcare industry will find this systematic review to be a valuable resource. [27].

Ethereum has a transaction cost of about eight cents and additional time overhead when used in secure data frameworks, according to [1] and [3]. Although this overhead might not seem like much in isolated circumstances, it becomes more noticeable in large-scale scenarios involving frequent transactions, like continuous health monitoring or clinical data sharing. Ethereum's consensus system, which makes sure that every transaction is verified and safely recorded across several nodes, is the cause of the delay. In situations were having access to medical data in real time is critical, this invariably slows down the system and causes anxiety. However, the significant advantages that blockchain offers in terms of transparency, security, and data integrity must be weighed against this latency and cost. Ethereum increases trust and regulatory compliance in sensitive sectors like healthcare by reducing the risk of illegal access, interference, and data breaches through immutable and verifiable transactions. Therefore, the trade-off can be seen as one of efficiency versus reliability: blockchain increases accountability and resistance to security breaches by introducing latency. In the long run, improved transparency and data protection may make the marginal cost of longer transaction times and higher transaction costs worthwhile in the majority of medical applications. Abdullah Al Omar et al. [7] highlight that the smallest of imperfections can prove to be a doorway for malicious users, and the reliability of using immutable code in such a critical field is thus questioned. Over and above these security issues, Ethereum's scalability issues are a serious bottleneck as well. Kristen Griggs et al. [4] mention that the transaction rate of the system is limited, leading to delays and higher fees incurred during heavy usage. In the healthcare sector, where timely access to patient information can be the difference between life and death, such latency can have direct implications for patient outcomes. Additionally, the dependence on energy-hungry consensus protocols and volatile transaction fees introduces unpredictability to mass-scale adoption. Combining these risks highlights the necessity of extensive testing, hybrid implementations, and models of governance prior to the successful deployment of Ethereum for managing healthcare data.

A simple PRISMA flow diagram for all these recent studies is shown in Figure 5.

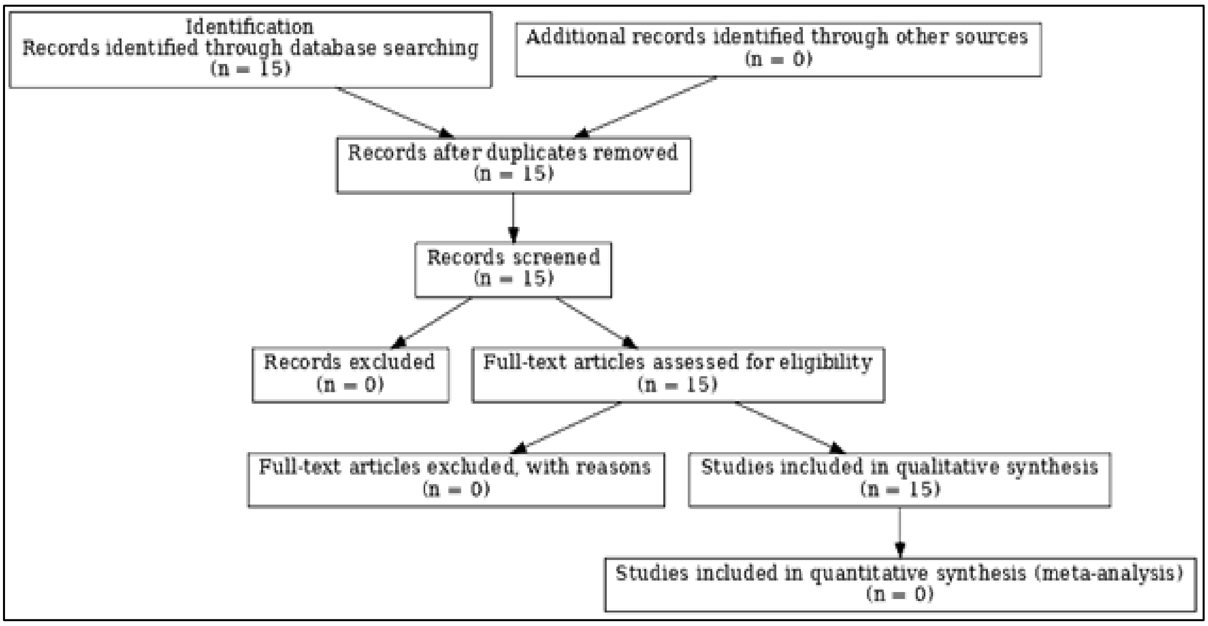


**Figure 5.** PRISMA Flow Diagram

## 5. Simulation Results

**Table 2.** Key Contributions and Result Parameters

| S.No | Reference (Year) | Framework / Method | Key Contributions | Result Parameters / Values |
|---|---|---|---|---|
| 1 | Sahu et al. (2024) | Blockchain-based review for EHR | Comprehensive review of decentralized blockchain framework for EHR | Enhanced privacy, security, and efficiency (qualitative) |
| 2 | Hamela et al. (2024) | Smart contract prototype for EHR | Improved data confidentiality, security, and interoperability | Improved reliability and compliance (qualitative) |
| 3 | *Journal of Angiotherapy* (2024) | Interoperable Blockchain-based EHR framework | Analysis of global EHR standards and interoperability | Proposed secure, interoperable blockchain framework (qualitative) |
| 4 | Husnain et al. (2024) – HealthChain | Blockchain with encryption & consent system | Secure and interoperable blockchain EHR framework | 30% reduction in access times, 40% higher interoperability, 50% fewer breaches, 35% ↑ patient satisfaction |
| 5 | Tahir et al. (2024) | Ethereum-based blockchain framework | Secure and private EHR system with cost-performance evaluation | Reasonable cost & performance feasibility (quantitative feasibility study) |
| 6 | Mole & Shaji (2024) | Ethereum + IPFS with smart contracts | Automated and anonymous secure medical record transfer | Minimum latency: 14 ms |

### Challenges

1. **Latency in Real-Time Access –** Ethereum-based frameworks (Chen et al. [1], Cao et al. [3]) show added time overhead due to consensus mechanisms, which limits usability in emergency or real-time healthcare scenarios.

2. **Transaction Costs** – Blockchain operations (e.g., ~8 cents per transaction) can accumulate significantly in large-scale hospital deployments, making cost-efficiency a challenge.
3. **Scalability Bottlenecks** – Ethereum's limited throughput causes delays and higher fees during peak usage (Griggs et al. [4]), restricting its use in large hospital networks.
4. **Private Key Vulnerabilities** – Loss or theft of private keys (Al Omar et al. [7]) compromises entire EHR datasets, posing catastrophic risks to healthcare security.
5. **Immutability of Errors** – Bugs in smart contracts cannot be reversed, raising safety concerns when managing sensitive and frequently updated medical data.
6. **Regulatory & Ethical Compliance** – Studies highlight difficulties aligning blockchain models with HIPAA, GDPR, and other privacy frameworks, slowing adoption.
7. **Energy and Resource Costs** – Energy-intensive consensus algorithms (e.g., Proof-of-Work) are unsustainable in large healthcare ecosystems.
8. **Lack of Standardization** – The absence of unified interoperability standards across frameworks hinders seamless exchange of EHRs among hospitals (Journal of Angiotherapy, 2024).
9. **Fault Tolerance in Node Failures** – Few studies have tested resilience when hospital nodes go offline, raising concerns for continuity of access.
10. **Limited Real-World Testing** – Many reviewed works present prototypes without long-term clinical deployment data, leaving uncertainty about real-world feasibility.

**Opportunities**

1. **Enhanced Data Privacy** – Blockchain ensures immutable and encrypted storage, protecting sensitive patient records from unauthorized access.
2. **Improved Security Against Attacks** – Mechanisms like Attribute-Based Signatures (Guo et al. [8]) and multi-authority systems strengthen authentication.
3. **Interoperability Gains** – Blockchain improves cross-platform data sharing (40% improvement reported by Husnain et al. [31]), critical for integrated hospital networks.
4. **Patient Empowerment** – Frameworks like Yue et al. [5] enable patients to own and control their records, increasing trust and transparency.
5. **Higher Resilience** – Decentralization ensures availability even when some nodes fail, improving the reliability of hospital IT systems.
6. **Cost Reduction in Data Breaches** – Studies (HealthChain [31]) report up to 50% fewer breaches, lowering compliance and recovery costs.

7. **Real-Time Efficiency Improvements –** Ethereum + IPFS (Mole & Shaji [32]) achieved latency as low as 14 ms, showing blockchain's potential for rapid secure data exchange.
8. **Integration with Emerging Tech –** Coupling blockchain with IoT and AI can enhance predictive healthcare, automated monitoring, and smart hospital management.
9. **Policy and Governance Potential –** Blockchain frameworks can embed compliance rules directly into smart contracts, aiding administrators in regulatory adherence.
10. **Scalable Future Architectures –** Modular systems like FHIR-Chain (Peng Zhang et al. [6]) provide pathways to scale blockchain in healthcare while maintaining trust and transparency.

**Recommendations for Future Research Directions**

Future studies can extend this work by validating MCUS-Net across larger, more diverse, and multi-institutional datasets to confirm its generalizability across populations with varying demographics and imaging protocols. Investigating the integration of multimodal data such as combining CT scans with genetic, histopathological, or clinical records may further enhance diagnostic accuracy and support personalized treatment planning. Additionally, explainable AI (XAI) techniques should be incorporated to improve interpretability for clinicians, fostering trust and transparency in decision-making. Future research may also explore lightweight and optimized versions of the model suitable for deployment in resource-constrained settings, including rural clinics and low-income countries. Finally, longitudinal studies assessing the impact of AI-assisted early detection on patient outcomes, cost-effectiveness, and overall healthcare system efficiency would provide critical evidence for policy-level adoption.

**Implications for Policymakers, Administrators, and IT Managers**

The findings of this research carry significant implications for multiple stakeholders in healthcare. Policymakers can leverage such AI-driven diagnostic frameworks to strengthen early detection programs for lung cancer, which may substantially reduce mortality and improve survival rates.

**Scalability limitations**

Another important challenge is storage overhead. High-resolution CT scans generate massive amounts of data, which not only require extensive storage capacity but also increase the burden of maintaining data security and compliance with regulatory standards. As datasets grow larger for both training and real-time use, hospitals face rising costs for cloud storage, data transfer, and secure backup systems, making large-scale deployment financially and logistically demanding.

## 6. Conclusion

The review has found that blockchain platforms based on hyper ledger and the Ethereum blockchain framework can serve as a suitable base for constructing an open-source platform for the healthcare industry. The benefits of the open-source software technology platform outlined will support the ongoing efficiencies of healthcare industry services to both save time, and even more importantly, lives. The study's primary milestone is determining the suitable software and blockchain technologies to achieve ambitious goals and revolutionize the way healthcare functions. Hyper Ledger is an open-source project that works to develop blockchain technology for various businesses. The Hyper Ledger Project is part of the Linux Foundation's Distributed Ledger Technology initiative. The Hyper Ledger project includes five frameworks (burrow, fabric, INDY, IROHA, and SAWTOOTH) as well as five tools (caliper, CELLO, COMPOSER, Explorer, and QUILT). Hyper Ledger Fabric-based applications can be used to create a business blockchain application. This project is an excellent fit for Hyper Ledger Fabric due to its four key features: permissioned network, secret transactions, no cryptocurrency, and programmability. In a permissioned network, participants' identities are known, and members have role-based access. Transactions are confidential and not accessible to all members, and any member can transact discreetly. Because of a lack of incentives and a scarcity of crypto tokens, cryptocurrency is no longer necessary. The chain code includes business logic and smart contracts for work execution. Each blockchain technology employs nodes, which link to form a network. A Hyperledger fabric member is a separate legal entity that transacts on the blockchain network. Many distributed ledgers are used by members. Each member hosts nodes. Throughout the organization, these nodes provide transactions and state information. The blockchain nodes are also called communication entities, and each node represents the identity of a certificate; even users in an ecosystem based on Hyperledger fabric receive certificates. A ledger manages the state of assets in a Hyperledger Fabric network. They represent anything from bonds to loans, to titles, to houses, and to anything that can be digitally represented.

## References

[1] Chen, Lanxiang, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, and Nan Zhang. "Blockchain based searchable encryption for electronic health record sharing." Future generation computer systems 95 (2019): 420-429.

[2] Zhu, Liehuang, Yulu Wu, Keke Gai, and Kim-Kwang Raymond Choo. "Controllable and trustworthy blockchain-based cloud data management." Future Generation Computer Systems 91 (2019): 527-535.

[3] Cao, Sheng, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and Ferrante Neri. "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain." Information Sciences 485 (2019): 427-440.

[4] Griggs, Kristen N., Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, and Thaier Hayajneh. "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring." Journal of medical systems 42, no. 7 (2018): 130.

[5] Yue, Xiao, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40, no. 10 (2016): 218.

[6] Zhang, Peng, Jules White, Douglas C. Schmidt, Gunther Lenz, and S. Trent Rosenbloom. "FHIRChain: applying blockchain to securely and scalably share clinical data." Computational and structural biotechnology journal 16 (2018): 267-278.

[7] Al Omar, Abdullah, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.

[8] Guo, Rui, Huixian Shi, Qinglan Zhao, and Dong Zheng. "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems." IEEE access 6 (2018): 11676-11686.

[9] Gavrilov, Goce, Sasho Manasov, and Orce Simov. "BLOCKCHAIN TECHNOLOGY FOR AUTHENTICATION, AUTHORIZATION AND IMMUTABILITY OF HEALTHCARE DATA IN PROCESS OF RECIPES PRESCRIPTIONS." International Dialogue: East-West 6, no. 1 (2019).

[10] Quaini, Tiago, Alex Roehrs, Cristiano André da Costa, and Rodrigo da Rosa Righi. "A MODEL FOR BLOCKCHAIN-BASED DISTRIBUTED ELECTRONIC HEALTH RECORDS." IADIS International Journal on WWW/Internet 16, no. 2 (2018).

[11] Efendi, Syahril, Baihaqi Siregar, and Heru Pranoto. "Concept designs of patient information security using e-health sensor shield platform on blockchain infrastructure." In Proceedings of MICoMS 2017, vol. 1, pp. 641-646. Emerald Publishing Limited, 2018.

[12] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues." Telematics and informatics 36 (2019): 55-81.

[13] Shahnaz, Ayesha, Usman Qamar, and Ayesha Khalid. "Using blockchain for electronic health records." IEEE access 7 (2019): 147782-147795.

[14] Taylor, David N. "A literature review of electronic health records in chiropractic practice: common challenges and solutions." Journal of chiropractic humanities 24, no. 1 (2017): 31-40.

[15] Duan, Jiang, Chen Zhang, Yu Gong, Steve Brown, and Zhi Li. "A content-analysis based literature review in blockchain adoption within food supply chain." International journal of environmental research and public health 17, no. 5 (2020): 1784.

[16] Badr, Shaimaa, Ibrahim Gomaa, and Emad Abd-Elrahman. "Multi-tier blockchain framework for IoT-EHRs systems." Procedia Computer Science 141 (2018): 159-166.

[17] Guo, Rui, Huixian Shi, Qinglan Zhao, and Dong Zheng. "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems." IEEE access 6 (2018): 11676-11686.

[18] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42, no. 8 (2018): 152.

[19] Efendi, Syahril, Baihaqi Siregar, and Heru Pranoto. "Concept designs of patient information security using e-health sensor shield platform on blockchain infrastructure." In Proceedings of MICoMS 2017, vol. 1, pp. 641-646. Emerald Publishing Limited, 2018.

[20] Al Omar, Abdullah, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.

[21] Liang, Xueping, Juan Zhao, Sachin Shetty, Jihong Liu, and Danyi Li. "Integrating blockchain for data sharing and collaboration in mobile healthcare applications." In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp. 1-5. IEEE, 2017.

[22] Hussain, Shaik Asif, and Sana Al Ghawi. "Sentiment Analysis of Real-Time Health Care Twitter Data Using Hadoop Ecosystem." In International Conference on Hybrid Intelligent Systems, pp. 453-463. Cham: Springer Nature Switzerland, 2022.

[23] Hosseini Sarkhosh, Seyyed Mahdi, and Peyman Akhavan. "Evaluating preparedness in using blockchains for electronic health record systems." The Electronic Library 41, no. 1 (2023): 87-110.

[24] Kiania, Kianoush, Seyed Mahdi Jameii, and Amir Masoud Rahmani. "Blockchain-based privacy and security preserving in electronic health: a systematic review." Multimedia Tools and Applications 82, no. 18 (2023): 28493-28519.

[25] Borade, Siddhi, Tanvi Paradkar, Prasad Takalkar, and Akash Trivedi. "Blockchain based electronic health record management system." Available at SSRN 4376765 (2023).

[26] Chelladurai, Usharani, and Seethalakshmi Pandian. "A novel blockchain based electronic health record automation system for healthcare." Journal of Ambient Intelligence and Humanized Computing 13, no. 1 (2022): 693-703.

[27] Hajian, Ava, Victor R. Prybutok, and Hsia-Ching Chang. "An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective." Computers in Human Behavior 138 (2023): 107471.

[28] Sahu, Dipansu, Namita Tiwari, and Meenu Chawla. "Blockchain as a solution for electronic health record management: A comprehensive review." In 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1-6. IEEE, 2024.

[29] Hamela, K., Gitanjali Shrivastava, Perikala Umapathi, Jayshri Sagar Bankar, Snehal Dipak Chaudhary, and Rajeshwari Kisan. "Enhancing Data Security and Privacy in Electronic Health Records with Blockchain Technology." In 2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS), pp. 1829-1835. IEEE, 2024.

[30] Husnain, Ghassan, Zia Ullah, Muhammad Ismail Mohmand, Mansoor Qadir, Khalid J. Alzahrani, Yazeed Yasin Ghadi, and Hend Khalid Alkahtani. "HealthChain: A

blockchain-based framework for secure and interoperable electronic health records (EHRs)." IET Communications 18, no. 19 (2024): 1451-1473.

[31] Husnain, Ghassan, Zia Ullah, Muhammad Ismail Mohmand, Mansoor Qadir, Khalid J. Alzahrani, Yazeed Yasin Ghadi, and Hend Khalid Alkahtani. "HealthChain: A blockchain-based framework for secure and interoperable electronic health records (EHRs)." IET Communications 18, no. 19 (2024): 1451-1473.

[32] Mole, JS Simi, and R. S. Shaji. "Ethereum blockchain for electronic health records: securing and streamlining patient management." Frontiers in Medicine 11 (2024): 1434474.