BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

NARRATIVE/SYSTEMATIC REVIEWS/META-ANALYSIS

Blockchain Technology to Enhance Clinical Data Management in Healthcare: A Systematic Literature Review

Khaoula Chafik, MS Computer Science, PhD(c)[1], Mohamed Hanine, PhD[1], Abdellah Ouaguid, PhD, ENSET (École Normale Supérieure de l'Enseignement Technique)[2,3] and Sulieman Alshuhri, PhD[4]

[1]Information Technology Laboratory, National School of Applied Sciences, Chouaib Doukkali University of El Jadida, El Jadida, Morocco; [2]University Hassan II of Casablanca, Casablanca, Morocco; [3]Laboratory of Precision Medicine and One Health (MedPreOne), School of Medicine, Mohammed VI University of Sciences and Health, Casablanca, Morocco; [4]Information Technology Department, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia

Corresponding Author: Khaoula Chafik, Email: khchafik99@gmail.com

DOI: https://doi.org/10.30953/bhty.v8.471

Keywords: audit trail, blockchain, clinical data management, consent management, healthcare, HL7 FHIR interoperability, smart contracts

Abstract

This systematic review examines how blockchain is applied in clinical data management (CDM) and what prevents its adoption in healthcare. A structured search in Scopus and Web of Science retrieved 554 records; after applying inclusion/exclusion criteria and quality assessment, 32 studies published between 2018 and 2024 were included. The analysis was guided by five research questions: (1) how blockchain supports clinical data workflows; (2) its role in data security and privacy; (3) key technical challenges and commonly used technologies; (4) integration with other healthcare technologies, and (5) how does blockchain technology integrate with and enhance other emerging healthcare technologies? Findings show that blockchain can support consent management, secure data sharing, traceability, and tamper-resistant audit trails using smart contracts and decentralized access control. It is also positioned as a trust layer for electronic health records, the Internet of Medical Things, artificial intelligence, and telemedicine by ensuring integrity and controlled access to sensitive clinical data. However, several barriers limit real-world deployment. Reported challenges include limited scalability and throughput, difficulty integrating with legacy electronic health record systems, heterogeneous regulatory requirements, and the complexity of encoding privacy, consent, and compliance into smart contracts. Ethereum and Hyperledger Fabric are the most frequently implemented platforms, often combined with off-chain storage and interoperability standards such as Fast Healthcare Interoperability Resources (FHIR)/Substitutable Medical Applications and Reusable Technologies on FHIR. Overall, blockchain shows strong potential to improve security, transparency, and cross-institution exchange in CDM, but its viability depends on addressing scalability, interoperability, and governance constraints. However, the evidence base remains heterogeneous, and only a minority of studies report quantitative benchmarks or real-world deployments, which limits cross-study comparability and generalizability.

Plain Language Summary

The authors investigate how blockchain can improve clinical data management. It explores standards-based data exchange, consent tracking, and audit trails in healthcare systems. After analyzing 32 studies from 2018 to 2024, key strengths were identified: transparent logging of access, better consent governance, and support for interoperable data sharing. The studies show that medical content usually stays off the blockchain. Instead, the ledger records pointers to the data along with consent status and access events, enabling auditability without storing sensitive clinical records on-chain. We found early pilots that demonstrate feasibility.

However, there is limited evidence on a large scale. Many reports lack common metrics, multi-site testing, and consistent performance results. Moreover, integrating legacy systems and managing identities remain challenging. These findings highlight the need for shared reference designs, privacy-preserving methods, and real-world evaluations. The goal is secure, reliable, and timely access to clinical data for patients and clinicians.

Received: November 2, 2025, Accepted: January 27, 2026, Published: March 11, 2026

Prior systematic reviews of blockchain in healthcare have largely emphasized broad health information systems and electronic health record use cases, particularly security, privacy, and general interoperability, rather than the end-to-end workflows of clinical data management (CDM).[1–7] This systematic literature review addresses that gap by focusing specifically on blockchain applications in CDM contexts. In addition, we interpret operational feasibility primarily through studies reporting quantitative evaluation metrics while treating the remaining works as conceptual architectures that motivate design directions but require further empirical validation.

In order to collect high-quality, reliable, and statistically valid data from trials, CDM is an essential component of any clinical research. Eliminating errors and data gaps is the primary goal of CDM, which enhances the integrity of clinical research-derived results.[8] The main activities involved in CDM include case report forms (CRFs) design, database development, data entry, data validation, discrepancy management, medical coding, data extraction, and database locking.[8] These activities are tightly coupled with regulatory expectations for data credibility and traceability in good clinical practice. The evolution of CDM into clinical data science reflects the growing emphasis on the measurement, acquisition, care, treatment, and inferencing of clinical research data, which requires advanced education and training to handle the complexities of modern clinical research.[9] With the volume and complexity of clinical data continuing to increase, CDM professionals will play an increasingly important role in ensuring the quality of the data and supporting the efficient commercialization of new therapeutics.[10]

The rapid evolution of healthcare technology has made the secure storage and exchange of clinical data more difficult. As health information systems expand and the use of the Internet of Medical Things (IoMT) grows, concerns about security, privacy, and governance have become more pressing. In this setting, blockchain, often characterized as a decentralized, tamper-evident ledger, has been examined as a possible approach to improve the reliability of CDM systems.[11,12]

From a technical perspective, blockchain is typically motivated by its ability to support transparency, accountability, and trust through distributed ledger technology (DLT). By maintaining an encrypted, tamper-evident record of transactions, blockchain-based designs aim to reduce dependence on centralized repositories and improve traceability in multi-stakeholder data exchange. These properties are frequently discussed in environments such as electronic health record (EHR) ecosystems, where information must be shared across institutions under stringent requirements.[13,14]

In addition, smart contracts are commonly incorporated to automate governance and policy enforcement, including consent management, access authorization, and billing-related checks.[15] Because these rules are executed programmatically, they can reduce manual intervention and support consistent enforcement of agreed conditions. Patient-centric models further emphasize cryptographic key control to support patient control over data access, which might strengthen trust.[16] Blockchain has also been explored within broader digital health architectures, where integrity and provenance mechanisms may improve confidence in datasets used for subsequent analysis.[17] For IoMT scenarios, tamper-evident logging is frequently proposed to strengthen data provenance for wearable and remote monitoring devices.[1,2] In telemedicine, blockchain-based mechanisms are proposed to secure data exchange and support consent and billing workflows.[3]

However, practical deployment remains constrained. Scalability is a recurring concern because many blockchain platforms face throughput and latency limitations under the transaction volumes typical of healthcare workflows; performance challenges have been reported for Ethereum and Hyperledger Fabric (HF) in relevant evaluations.[18,19] Energy consumption is also a consideration for some consensus mechanisms, particularly proof-of-work (PoW).[20]

Interoperability with existing infrastructures, particularly EHR systems, remains a practical obstacle and often requires substantial integration work, including new application programming interfaces (APIs) and compatible data-exchange interfaces.[21] Regulatory compliance adds another layer of difficulty because healthcare organizations must meet data-protection requirements that can differ across jurisdictions. While approaches such as zero-knowledge proofs and differential privacy are discussed as possible ways to manage these constraints, they have not yet seen broad uptake in routine deployments.[22]

The aim of this article is to provide a systematic analysis of current research regarding the application of blockchain in CDM. This review selected 32 articles from the

Citation: Blockchain in Healthcare Today 2026, 8: 471 - https://doi.org/10.30953/bhty.v8.471

databases Scopus and Web of Science (WoS), published between 2018 and 2024, and discusses the applications of blockchain, its challenges, and future developments in the area of healthcare. Some of the specific areas covered include how blockchain can improve data security, integrate with other standards, enhance interoperability, and combine with other technologies, including artificial intelligence (AI) and IoMT.[21,23]

This article is divided into sections to deliver a comprehensive and easy-to-understand discussion on the topic. Section 1 introduces the study context, outlines the motivation and research gap, and presents the objectives of the systematic review. Section 2 provides a literature review summarizing significant contributions from previous research and discussing areas where future work should focus. Section 3 highlights the study selection process, where the method used is clear, logical, and rigorous, enabling the process to be repeated by others. Section 4 presents responses to the research questions and insights, focusing on the utilization of blockchain, technological issues, and realization architectures. Section 5 discusses these findings as they relate to healthcare innovation more broadly, while Section 6 examines the limitations of this study and offers a discussion of future directions. Finally, Section 7 consolidates the findings and recommendations that can be useful for enhancing blockchain's application in CDM.

The findings of this study can also benefit various segments of society and stakeholders involved in the research and application of blockchain technology in the healthcare industry as follows: It describes not only how blockchain technology creates value for various industries but also the major challenges that need to be addressed to capitalize on its opportunities. In general, this synthesis provides a research and implementation plan for the potential evolution of a safer, more efficient, and patient-oriented health application environment.

Background

This systematic review of the literature attempts to identify the most relevant papers on blockchain use in electronic health. This article highlights the use of blockchain technology to improve data security and privacy with respect to data management. The evaluation approach is also comprehensive; all opportunities and challenges of applying blockchain technology to CDM are covered.

Moreover, Hölbl et al.[4] focus on the rarity of blockchain implementation in the healthcare industry, discussing the opportunities blockchain offers for sharing data combined with efficient access control. They argue that, even though blockchain has the potential to transform health systems, most studies are unclear and lack technical analysis and real-world applications.

In addition, the review by Attaran[5] outlines how blockchain works, how it can be used, and the potential problems that can arise when using it to solve critical issues in healthcare, such as data sharing and protection. Furthermore, this review highlights how blockchain could potentially help in discovering perhaps better architectures for storing data and how to better integrate them with healthcare systems.

Conversely, blockchain technology for healthcare is examined by Agbo et al.,[1] who provide an exhaustive analysis of the technology, and how it will revolutionize nearly every aspect of the healthcare system. They emphasize the need for conducting more beneficial research and fostering stakeholder collaboration so that no limitations prevent the full realization of blockchain's potential.

Additionally, the ability to optimize personal health records and data management is an essential component of the concept, including the advantages and disadvantages of using blockchain for healthcare, as described by Tandon et al.[6] The analysis also suggests that additional research is necessary to understand the policy and design aspects of integrating blockchain technology into other fields, such as medical diagnostics and other legal domains.

Similarly, Fang et al.[15] explored not only the construct but also the gap in blockchain solutions for personal health record (PHR) functionality. They observe that, while much can be made of the technology, most projects remain at the pilot phase. In order to make blockchain PHR models conform more closely to these systems and verify the correctness of the models, the authors proposed an empirical study.

Likewise, Saeed et al.[7] provide a brief description of the advantages of blockchain technology for patients' rights and data management issues in the context of the healthcare domain. In terms of security, system infrastructure, and compliance, they identify some of the limitations within empirical work, methodology, and regulation and recommend possible approaches for future research.

On the other hand, blockchain can enhance the protection and related privacy of EHRs. Kiania et al.[24] examine the limitations and propose efficient protocols in their article. Their analysis presents different applications of blockchain and cautions on the lack of empirical research done toward the real-life issues such as cost, scalability, and regulation.

Last but not least, the potential of these benefits is one of the major factors that have led to a heightened focus on blockchain technology for healthcare; however, it is often achieved at the cost of addressing the issues and questions that revolve around the best way to apply the technology. The present study aims to fill these gaps using an systematic literature reviews (SLRs) on the open issues and research questions related to the use of blockchain technology in improving CDM. This work will provide a framework for current applications of blockchain technology in healthcare, describe the problems of clinical information management, and pinpoint the key research areas that may address these problems.

The reviewed articles, published between 2018 and 2024, cover different applications of blockchain in healthcare. They analyze between 33 and 65 studies, drawing information from sources such as IEEE Xplore, ACM Digital Library, SpringerLink, Scopus, WoS, and PubMed. These papers cover topics such as data security, privacy, interoperability, and regulatory concerns. Some papers discuss the advantages of blockchain in providing secure and efficient health data exchange, while others address difficulties such as scalability, cost, and regulatory compliance. This study reviews 32 recent works from Scopus and WoS, providing an overview of current research and progress in the field. Unlike prior reviews that broadly emphasize healthcare data security or interoperability, this SLR targets CDM workflows (e.g., clinical trials, eCRF, and trial protocol data) and explicitly distinguishes between conceptual architectures and studies reporting quantitative performance or empirical evaluation metrics.

Methods

Review Questions

A review of the literature was conducted in a more structured way and built on the review systematically in support of research questions. They form the foundation in the systematic approaches to formulating the question and objectives of the SLR, the focus, and the direction of the study. In conducting this research, common guidelines for performing SLR have been strictly observed to guarantee the stringency and coverage of the methods.

From the beginning, when determining articles to include or exclude in the current study, to when we conducted a systematic search and screen for articles of interest, we followed a systematic procedure. This ensured that all research that would be conducted would be relevant to the core concepts being explored, including blockchain, healthcare, and CDM. Furthermore, to create our search strategy, we utilized Population, Intervention, Comparison, and Outcome (PICO),[25] a well-defined structure used to create sound search filters.

Moreover, we also followed a strict criterion through which we filtered the articles that must address the blockchain's application in CDM, the technical aspect of the subject, and evaluation. The systematic method we adopted facilitated selecting and reviewing a number of important articles that provided valuable insights into how blockchain might be used to improve CDM in the healthcare setting. This section focuses on the research questions that steer our SLR and explains the particular questions we wish to answer. These questions also form the framework of the review and present the reader with a clear vision of the major purposes and concepts that ground this research.

RQ (Research Question 1): How can blockchain improve the management of clinical data in healthcare systems? The objective of this question is to investigate the possible advantages of blockchain technology in enhancing the efficiency of CDM procedures. It evaluates the benefits of blockchain in terms of efficiency, data integrity, and overall process optimization as compared to older systems.

RQ2: What role does blockchain play in ensuring the security and privacy of clinical data? The purpose of this question is to better understand how blockchain technology might improve the security and privacy of clinical data. Its goal is to determine how blockchain technology, in contrast to current security methods, can offer better protection against unwanted access and data breaches.

RQ3: What are the key technical challenges in implementing blockchain technology for CDM? The goal of this question is to identify and understand the technical challenges associated with the integration of blockchain technology into CDM systems. It covers issues such as scalability, interoperability, and the complexity of implementation.

RQ4: What blockchain technologies are most commonly used in CDM? This question explores the specific blockchain platforms and technologies frequently implemented in CDM. It aims to assess how each technology addresses healthcare requirements, including data privacy, security, scalability, and interoperability.

RQ5: How does blockchain technology integrate with and enhance other emerging healthcare technologies? The objective of this question is to explore how blockchain may interact with other emerging technologies to boost healthcare outcomes, particularly in the context of CDM.

Each review question in this systematic literature study constitutes an essential component of a coherent narrative that methodically examines diverse facets of blockchain's incorporation into CDM within healthcare. The inquiry into how blockchain might improve CDM (RQ1) naturally leads to an analysis of its advantages in terms of efficiency, data integrity, and optimization compared to existing methods. Understanding these benefits affects the inquiry into blockchain's function in maintaining security and privacy (RQ2), as boosting efficiency goes hand in hand with strengthening defenses against data breaches and unauthorized access.

Similarly, the investigation of technical issues in deploying blockchain (RQ3) is strongly related to the practical implementation of these technologies. Identifying problems such as scalability, interoperability, and complexity of implementation gives context for understanding the limitations of blockchain. These insights are vital for examining the suitability of different blockchain technologies (RQ4) for CDM. These technical challenges will assist in deciding when to apply HF,[26] Ethereum,[27] or Corda[28] to fulfill healthcare requirements like data privacy, security, or integration.

Furthermore, there is a reasonable connection between applying new technologies (RQ5) and the overall picture

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

of technologies improvised with blockchain. It gives an understanding of how blockchain could integrate with AI and IoT to improve the work with clinical data with the help of smart automation and the network's view. This systematic review provides a clear map of the state and scope of blockchain in healthcare as well as future research directions within the field.

Inclusion/Exclusion Criteria

Systematic literature reviews have many important aspects, and one of those requirements is defining well-established inclusion and exclusion criteria. This type of predetermined inclusivity and exclusivity serves as the benchmark for a particular research scope by eliminating every other research not conforming to the previously established conventions. This section provides a clear explanation of the exact criteria as well as even the reasoning for each so that our review does adhere to the outlined criteria to the letter and can be replicated. The aim of these measures is to eliminate bias in our analysis of other studies and only include research that meets the specific objectives of the SLR analysis. This guarantees that the selected study is both relevant and of a high standard because it stems from the wide and systematic amalgamation of evidence that provides the conclusion and results.

Database Selection

The primary databases for this systematic literature review that we considered for inclusion are WoS and Scopus due to the following advantages. These databases are renowned for their extensive indexing of scholarly literature, encompassing journals, conference proceedings, and other intellectual outputs. These broad scopes are particularly helpful for interprofessional education, ensuring a wide number of relevant materials, which systematic literature reviews require. In addition, the multidisciplinary nature of WoS and Scopus is suitable for the study issues that necessarily involve concentration on many scientific disciplines, as it expands the spectrum of sources for assessment in the given fields. Furthermore, quality control standards upheld for the data fed into these databases guarantee that only materials subject to review by other professionals in the field are used. As for the quality assurance part, it is crucial to mention that the reliability of the research chosen to be included in the SLR is a priority. Furthermore, the applied databases offer such search parameters as Boolean operators and various filters that allow one to design precise search queries, thereby increasing the effectiveness and productivity of the procedure for identifying relevant research.

Search Query

The PICO criteria[29] provided the basis for our search query formulation. In the context of our study, these elements are delineated as follows:

Population: Blockchain's application to CDM and healthcare.

Intervention: Blockchain-based techniques, procedures, tools, or systems for processing clinical data.

Comparison: Research comparing blockchain technology with traditional approaches to CDM.

Outcomes: Improving clinical data governance, security, and efficiency in healthcare systems are the results.

This led to the formulation of the following search query: *("Blockchain*" OR "Blockchain" OR "Block chain" OR "Hyperledger" OR "Distributed Ledger" OR "DLT" OR "Smart Contracts" OR "Decentralized Applications" OR "Encryption" OR "Decentralized Data") AND ("Healthcare" OR "Health Care" OR "Health*" OR "Medical Research" OR "Medical Data" OR "E-Health" OR "Electronic Health" OR "Electronic Health Records" OR "EHR") AND ("Clinical Data" OR "Clinical trial*" OR "Trial Protocol" OR "Trial Management").*

We developed a thorough search strategy using Boolean operators to find publications that highlight the intersection of CDM, blockchain, and healthcare. This is a summary of the question:

("Blockchain" OR "Blockchain" OR "Block chain" OR "Hyperledger" OR "Distributed Ledger" OR "DLT" OR "Smart Contracts" OR "Decentralized Applications" OR "Encryption" OR "Decentralized Data"):* This part of the query allows for the capture of all pertinent variations of blockchain terms found in the work.

AND: This operator ensures that terms pertaining to blockchain and healthcare are present in the papers that are retrieved.

("Healthcare" OR "Health Care" OR "Health" OR "Medical Research" OR "Medical Data" OR "E-Health" OR "Electronic Health" OR "Electronic Health Records" OR "EHR"):* The OR operator is used to capture studies that may utilize different language by embracing a wide range of healthcare phrases.

("Clinical Data" OR "Clinical trial" OR "Trial Protocol" OR "Trial Management"):* This part of the query ensures that the search focuses on studies that are most pertinent to the research objectives by limiting the focus to CDM.

Focusing on security, efficiency, and improvements to governance, the combination of these elements helps obtain a wide collection of publications discussing the use of blockchain technology for CDM in the health sector.

Inclusion/Exclusion Steps

The selection workflow followed a sequential process: database retrieval using structured keyword queries, duplicate removal, proximity-based precision filtering, title/abstract screening, and full-text eligibility assessment

against predefined inclusion and exclusion criteria, resulting in the final set of included studies.

Three main phases—identification, screening, and inclusion—of the process are outlined in Figure 1, which shows how to find, evaluate, and choose articles for an SLR. During the Identification Phase, an initial search was made in both the WoS and Scopus databases. The search, which targeted the title, abstract, and keywords categories, generated 137 documents in WoS and 417 in Scopus, resulting in a total of 554 items. The search query includes a range of keywords and phrases relating to blockchain technology, healthcare, and CDM.

To increase the precision of the screening phase, we applied proximity operators to the title, abstract, and keywords fields, requiring that blockchain-related terms occur within 50 words of clinical-data-management terms (NEAR/50 in WoS and the equivalent W/50 operator in Scopus). This proximity filtering reduced the initial set to 265 records, which were then screened using the eligibility criteria described later.

In the final Inclusion Phase, 32 unique documents were included in the study after the final exclusion procedures. Documents that focused primarily on blockchain and e-health without relation to CDM were eliminated, amounting to 40 exclusions, along with 18 duplicates. This procedure made sure that the final collection of documents examined was unique and useful.

Quality Assessment

Assessment of the quality of included studies is a crucial factor for improving methodological quality and reliability for this SLR. This section provides an important foundation for the later integration of the studies presented through a detailed critical appraisal that focuses on the quality of the studies and the credibility of their findings. The aim of this section is to give the readers a

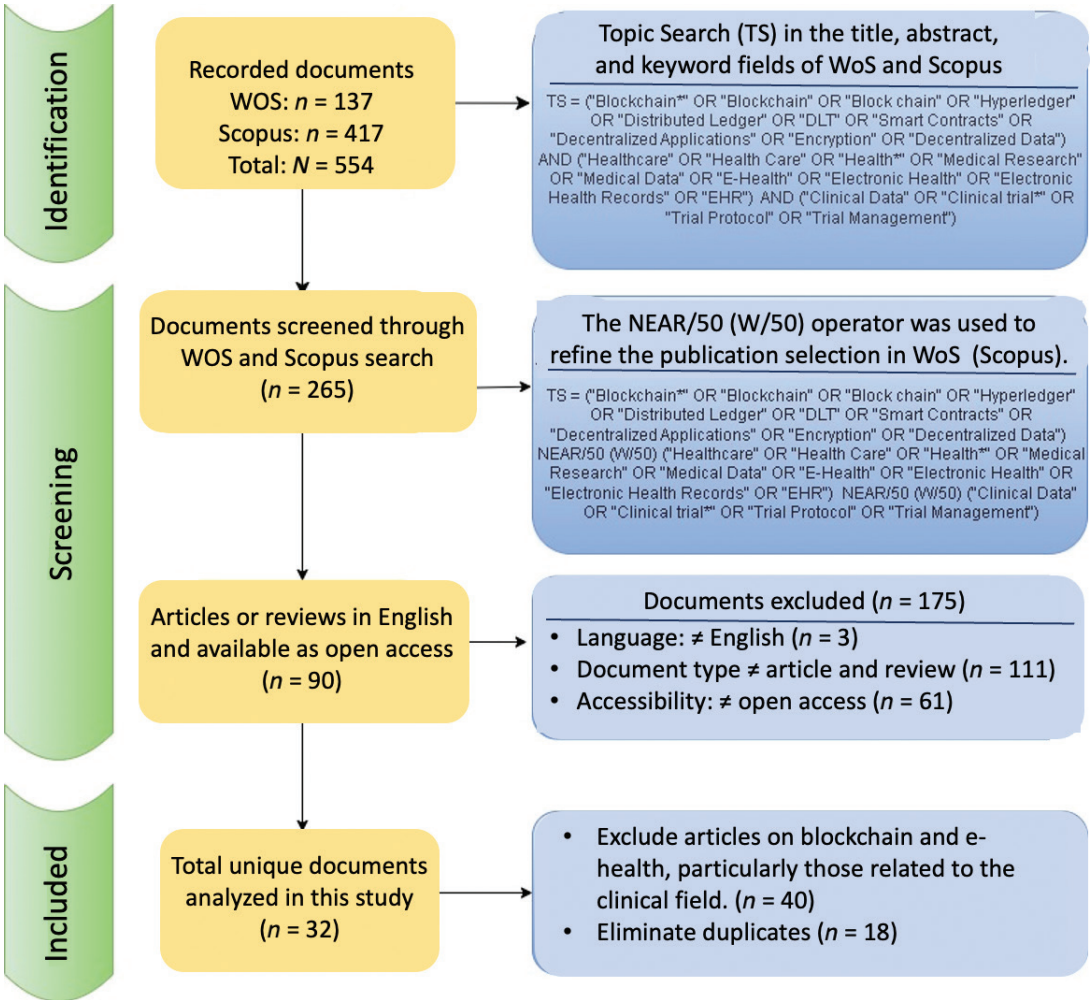

Fig. 1. Flow chart of the inclusion/exclusion criteria. TS: Topic Search performed on title, abstract, and keywords fields. NEAR/50 (Web of Science)/W/50 (Scopus): Proximity operator requiring search terms to appear within 50 words of each other, WoS: Web of Science.

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

clear assessment of the works reviewed in this paper without bias, so the findings reported are objective, well-conducted, and well-produced research studies. By using an assessment form that has established criteria, we want to understand the advantages and the limitations of each study so that their weight in answering our research objectives can be correctly evaluated. Besides, it will help readers and researchers to filter out the quality of synthesized evidence in this SLR and improve the validity and significance of the conclusions.

For the quality assessment, we focused on three essential questions to evaluate the primary studies:

Application of Blockchain: Does the article clearly demonstrate the application of blockchain technology in the management of clinical data in healthcare?

Methodology: Is the methodology for implementing blockchain technology in CDM explicitly defined (problem identification, blockchain techniques, and solution architecture)?

Evidence: Is there empirical evidence supporting the effectiveness of blockchain solutions, such as case studies, empirical results, or evaluation outcomes?

After the inclusion/exclusion criteria and quality assessment of papers were conducted, 32 articles were included for the current SLR. As this review could seem more selective compared with large-scale reviews, it is vital to underline that the focus was on the careful analysis of a limited sample of methodologically sound, full-implementation publications only. The collected literature revealed noteworthy discoveries and methodologies that pertain to blockchain technology use and CDM in healthcare. Therefore, by adhering to the strict methodological guidelines listed earlier, we established a solid basis that supported the synthesis of relevant studies as well as the identification of emerging trends and obstacles to the use of blockchain in healthcare systems for the optimization of clinical data. This strategy of sample selection helps to make well-justified findings, which will be valuable in increasing knowledge in the existing literature.

Final Article Dataset

As demonstrated in Figure 2, research on blockchain integration in e-health has fluctuated over the years. From 2018 to 2019, the field had low activity, with only a small number of selected articles.

Starting in 2020, the number of studies expanded gradually, suggesting an increasing interest in this subject. The year 2021 witnessed considerable growth, with a significant number of papers selected, and this trend continued into 2023, where research output peaked. Although there was a notable decrease in 2022, the increasing trend returned in 2023, reflecting a renewed interest in studying blockchain's possibilities in e-health. By August 2024, the selected articles had declined significantly, reaching a low count. This overall pattern reflects the cyclical attention toward blockchain's ability to enhance the security, privacy, and efficiency of e-health systems, highlighting its importance in the healthcare sector.

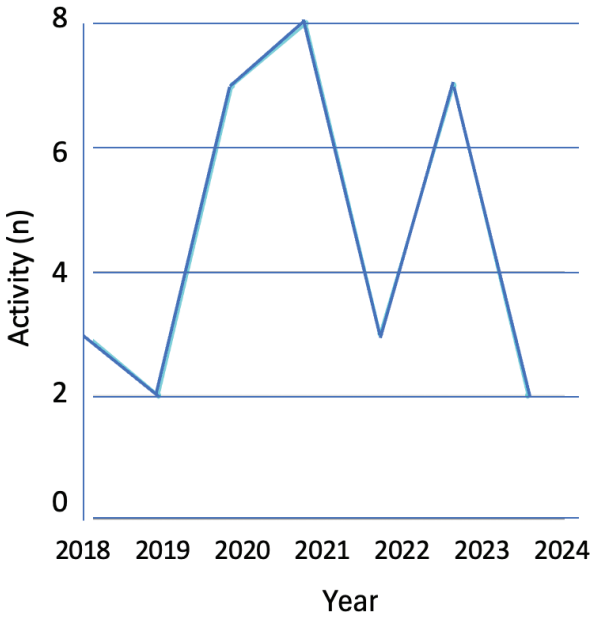

Fig. 2. Field growth since 2018.

Results

Corpus Overview

We extracted a standardized set of variables aligned with the review questions, including application context, security/privacy role, techniques, integration with emerging technologies, challenges, empirical results, and interoperability elements (Appendix A).

The evidence separates into studies with quantitative or operational evaluations and design-oriented studies without benchmark reporting. This distinction is used throughout the results when interpreting feasibility and maturity (Appendices B and C).

RQ1. How can blockchain improve the management of clinical data in healthcare systems? Blockchain technology, whose features include a distributed database and a trustworthy ledger for updated data, helps to satisfy the need to keep sensitive patient information and to respect compliance standards in regulatory regimes.[30] Its advantages in maintaining a decentralized structure, reinforced with cryptographic chains to enhance data integrity without relying on a governing body, make it ideal for clinical trials and mobile health applications.[31]

Because blockchain solutions provide synchronization of patient information across providers, blockchains might become essential tools to enable timely access to the latest information, particularly for critical emergency treatment.[32] Moreover, blockchain technology can be integrated with other systems to enable the sharing of patient

data effectively. Models like MediLinker[33] show that users can apply digital wallets to share data without compromising their anonymity because the blockchain technology is decentralized, which enhances data interoperability.[34]

Along with reducing the administrative load, smart contracts on blockchains allow providers to increase their focus on patient care by simplifying certain processes, such as data sharing and managing patient consent.[35] Blockchain also enables secure data sharing and distribution that is easy to trace, thereby maintaining data governance, enhancing record integrity, and preventing any unjustifiable alterations to records.[36,37]

Overall, the corpus frames blockchain's contribution to CDM around secure sharing, interoperability, decentralization, smart contract automation, and auditability (Table 1).

RQ2. What role does blockchain play in ensuring the security and privacy of clinical data? There is an inherent security associated with blockchain, which is extremely important for this technology to be used in healthcare since clinical information must be confidential and secured against unauthorized access. In the article,[48] the authors present the application of cryptographic encryption to secure clinical transactions; even if intercepted, the information is unreadable without the corresponding encryption keys.

The focus on the patient-centered nature of blockchain technology is expressed in this study,[40] noting that patients can use cryptographic keys to control access to their medical records. This configuration gives patients full control over who is allowed to either access or edit their medical data, thus better protecting privacy.

Additionally, as noted in this article,[47] the blockchain architecture is decentralized, hence removing the risks that arise from the conventional centralized healthcare databases. Because it is decentralized, cybercriminals have a difficult time trying to compromise the system as a whole.[49]

As the article by Khatoon[50] reports, blockchain technology produces unchangeable audit trails that record every interaction with clinical data. This characteristic promotes accountability because the healthcare professionals involved can be accountable for any access or changes not permitted in a patient's record. Moreover, Plebani et al.[43] point out the integration of multifactor authentication as an added layer of protection for sensitive medical information, reinforcing access security.

As stated in the study by Khatri et al.,[51] blockchain technology has inherent decentralization and immutability, properties that add up to better data privacy and protection against unauthorized access. Since every transaction is encrypted and then transparently recorded, blockchain assures data integrity and traceability. The application of blockchain technology in regulatory compliance enhancement was discussed by Aljaloud and Razzaq,[41] particularly in relation to privacy legislations such as the General Data Protection Regulation (GDPR). The traceability and transparency capabilities of blockchain enable healthcare businesses to demonstrate adherence to legal data protection standards and provide an auditable record of who accessed or changed patient data.[39]

Overall, the reviewed studies emphasize encryption, patient-controlled access, decentralization, immutable audit trails, and compliance support as key security enablers (Table 2).

In Aljaloud et al. (2023),[41] the proposed system (Figure 3) uses identity verification followed by smart

Table 1. Comparison of blockchain features in healthcare.

Features	Description	Articles (*n*)	References
Security & privacy	Ensures sensitive patient data are protected and compliant with regulations.	6	Kasyapa and Vanmathi,[16] Saeed and Malik,[7] Rahman and Hossain,[38] Hovorushchenko and Moskalenko,[30] European Society of Radiology,[39] Siyal and Junejo[40]
Interoperability	Synchronizes patient data across providers for timely access, especially in emergencies.	7	Aljaloud and Razzaq,[41] Zhang and White,[42] Harrell and Usman,[34] Plebani and Rossetto,[43] Ali and Al-Rimy,[44] Hirano and Motohashi,[36] Rana and Rana[45]
Decentralization	Maintains data integrity without a central authority through cryptographic chains.	8	Milone and Fusco,[20] Oakley and Worley,[46] Harrell and Usman,[34] Saleh and Shayor,[37] Motohashiand and Hirano,[31] Zhuang and Chen,[47] Rana SK Rana[45]
Smart contracts	Automates processes like data sharing, patient consent management, and enforcing healthcare policies.	4	Oakley and Worley,[46] Aljaloud and Razzaq,[41] Plebani and Rossetto,[43] Omar and Jayaraman[35]
Auditability	Provides secure, traceable data distribution that prevents unauthorized alterations.	4	Ali and Al-Rimy,[44] Hirano and Motohashi,[36] Saleh and Shayor[37]
Integration with other systems	Facilitates data sharing while preserving user anonymity using models like MediLinker.	6	Aljaloud and Razzaq,[41] Zhang and White,[42] Harrell and Usman,[34] Ali and Al-Rimy,[44] Bautista and Harrell,[33] Rana and Rana[45]

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

Table 2. Blockchain features ensuring clinical data security and privacy.

Security/privacy feature	Role in clinical data management	References
Cryptographic encryption	Secures clinical transactions, making intercepted data unreadable without the proper keys.	Zhuang and Sheets[48]
Patient-controlled access	Empowers patients with cryptographic keys to manage access/edit permissions to their records.	Siyal and Junejo[40]
Decentralization	Reduces centralized attack risks, enhances system resilience, and eliminates single points of failure.	Zhuang and Chen,[47] Chen and Cao,[49] Gordon and Catalini[32]
Immutable audit trails	Tracks every interaction with patient data to promote accountability and transparency.	Khatoon[50]
Multi-factor authentication	Adds another layer of protection for sensitive clinical information.	Plebani and Rossetto[43]
Data integrity and traceability	Ensures encrypted, tamper-proof transactions that can be transparently audited.	Khatri and Al Sulbi[51]
Regulatory compliance	Helps demonstrate adherence to legal standards with verifiable access/change logs.	Aljaloud and Razzaq,[41] European Society of Radiology[39]

contract policy enforcement to authorize access, and the clinical report is retrieved from a secure archive linked to blockchain records. In this workflow, the consent artifact (e.g., a signed consent form stored off-chain) can be managed separately from the consent state; the document may be stored in an external repository (e.g., Interplanetary File System [IPFS]), while the on-chain smart contract maintains a minimal consent status with time-stamped provenance and an immutable audit trail. This structure ensures data confidentiality, maintains the integrity of health records, and prevents unauthorized access, reinforcing the role of blockchain in protecting sensitive healthcare information.

RQ3. What are the key technical challenges in implementing blockchain technology for CDM? Despite its potential advantages, blockchain application in healthcare confronts many technological obstacles, especially with regard to scalability, interoperability, and regulatory compliance. According to two articles, Marbouh et al.[52] and Molli[53] reported that scalability is one of the main problems, with blockchain systems finding it difficult to manage the enormous amounts of medical data. In the healthcare industry, this difficulty is particularly noticeable because data must frequently be analyzed rapidly and in real time. In practice, these constraints push designs toward minimizing on-chain clinical content and prioritizing architectures that can sustain predictable performance under clinical workloads.

One of the significant challenges relates to energy consumption by these networks, due to the PoW-based consensus mechanism required for validating most public blockchain-related transactions.[54] At scale, these energy costs can become an operational barrier for healthcare organizations, affecting sustainability and deployment decisions. If blockchain use grows, healthcare organizations may find their high energy needs unsustainable. Furthermore, as mentioned in this study,[46] blockchain deployment for healthcare providers is made more difficult by the difficulty of developing smart contracts that adhere to strict healthcare laws.

Another significant barrier to blockchain technology's integration with current healthcare systems, such as EHR platforms, is interoperability. This challenge is a further major problem, as blockchain technology challenges the interaction with existing healthcare systems like EHR platforms. Hirano et al. showed that efficient data interchange requires building standard APIs and considerable upgrades to integrate blockchain with these legacy systems. Data storage limits, as demonstrated by Taloba et al.,[55] are other serious concerns since blockchain may lack the capability to manage the extensive datasets created in healthcare situations.

The problem of regulatory compliance is further underlined by Gonzales et al.,[56] especially considering the different data privacy rules between areas. Blockchain's decentralized structure may limit compliance with local privacy and data preservation rules, particularly in cross-border healthcare applications. Regulatory issues thus remain a hurdle to blockchain adoption, as healthcare providers may hesitate to employ technology that does not entirely comply with existing legal frameworks. As a result, even technically sound prototypes may remain at the pilot stage until compliance responsibilities and validation evidence are clearly established.

According to Rana et al.,[45] there are also problems with system throughput and processing speed because many blockchain systems—especially those that were first created for financial transactions—are not suited for managing complicated healthcare data. Finally, this study[44] highlights the trade-off between privacy and transparency in blockchain systems. Although one of blockchain's advantages is transparency, handling sensitive medical

data can make it difficult. The preservation of patient privacy and transparency must be balanced in healthcare organizations. These trade-offs influence design choices and often determine whether systems can progress beyond demonstrations to routine use.

Overall, the barriers cluster around scalability and throughput limits, integration/interoperability constraints, and compliance-driven design complexity (Table 3).

RQ4. What blockchain technologies are most commonly used in CDM? In CDM, blockchain technologies and related tools are frequently used to address security, privacy, and interoperability requirements. Across the reviewed studies, consensus choices, security strategies, permissioned designs, and implementation stacks varied across the corpus (Table 4). Ethereum-based implementations and HF were reported most frequently, while Corda appeared less often. However, throughput and latency are reported by only a subset of evaluation studies and are not directly comparable because workloads, network configurations, and measurement definitions differ; therefore, cross-platform performance conclusions should be interpreted as indicative rather than definitive.

First, restricted access is made possible by permissioned blockchain systems, which guarantee that only authorized users can handle sensitive data. Platforms like FHIR-Chain[42] and Quorum,[57] alongside Ethereum[38,48] and HF,[26] provide a strong emphasis on high transaction speed and interoperability—the critical attributes for applications such as clinical trials.[57,58] Moreover, tools like Hyperledger Sawtooth[49] and Hyperledger Caliper[19,49] facilitate assessment of scalability and performance, which allows for the efficient optimization of blockchain applications.[49]

It is important to implement security techniques that ensure the confidentiality and integrity of data. While zero-knowledge proofs and public key infrastructure give very reliable means for secure identity verification, smart contracts help in automating access rights and compliance.[32,42,50] Furthermore, technologies of audit trails, Merkle trees, and hash chains improve transparency, build trust, and raise resistance to tampering, while cryptographic algorithms will protect data from unauthorized access and ensure the reliability of the information concerning patients.[59]

Consensus mechanisms ensure consistency of the blockchain data, ensuring validation of transactions in a secure manner. Secure alternatives include PoW and proof of stake (PoS),[60] commonly known by the abbreviation PoS, while proof of authority[60] rests on trusted nodes to provide fast and effective validation.[61] Decentralized identifiers enable protection of patients' privacy; this also enhances compliance with laws in the area of healthcare by enabling greater control of the availability of information for both the patients and their providers.[62]

Finally, development tools and frameworks based on blockchain make scalability and integration easier.[60] Platforms like PFS[64] offer decentralized storage for handling big datasets, while tools like Node.js,[47] Web 3.js,[47] and Docker Containers[19] simplify the development and deployment of applications. Additional tools, including Solidity,[42] Remix IDE,[41] and Ganache,[41] help smart contract creation. Frameworks like blockchain-as-a-service (BaaS)[5] ease deployment, while MetaMask[23] and ReactJS[34] improve user interaction and front-end development.

Interoperability across the corpus leans on established standards rather than bespoke blockchain APIs (Table 5). Fast Healthcare Interoperability Resources / Substitutable Medical Applications and Reusable Technologies (FHIR/SMART) is the primary boundary: REST endpoints expose normalized resources and payloads stay off-chain, and only SHA-256 digests and consent pointers are anchored on-chain, with SMART scopes used where implemented.[34,42] Legacy Health Level Seven Version 2/Clinical Document Architecture (HL7 v2/CDA) feeds are extract, transform, and load (ETL)-mapped into FHIR with document hashes/URIs registered on the ledger[42,43]; cross-repository exchange often follows IHE XDS.b/XCA, with the chain acting as a registry for UUIDs, hashes, and policy pointers.[44,58] Digital

Table 3. Technical challenges in implementing blockchain for clinical data (RQ3).

Study	Challenge	Details
Marbouh and Abbasi (2020)[52]	Scalability	Blockchain struggles to handle large volumes of clinical data efficiently.
Milone and Fusco (2024)[20]	High energy consumption	Proof of Work consensus mechanisms are resource-intensive.
Oakley and Worley (2023)[46]	Smart contract complexity	Developing healthcare-compliant smart contracts is technically demanding.
Hirano and Motohashi (2020)[36]	Interoperability	Difficulty integrating with legacy EHR systems.
Taloba and Rayan (2021)[55]	Data storage limitations	Blockchain storage capacity is insufficient for massive healthcare datasets.
Gonzales and Smith (2021)[56]	Regulatory compliance	Complexities in complying with privacy regulations across regions.
Rana and Rana (2022)[45]	System throughput limitations	Blockchain systems are not optimized for complex healthcare data processing.
Ali and Al-Rimy (2023)[44]	Privacy–transparency trade-off	Managing privacy while maintaining transparency can be challenging.

EHR: electronic health record.

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

Table 4. Blockchain technologies commonly used in clinical data management.

Blockchain technologies	Articles (*n*)	References
Permissioned blockchain systems		
Ethereum	21	Kasyapa et al.,[16] Oakley et al.,[46] Aljaloud et al.,[41] Zhuang et al.,[57] Rahman et al.,[38] Zhang et al.,[42] Harrell et al.,[34] Plebani et al.,[43] Gordon et al.,[32] Hirano et al.,[36] Saleh et al.,[37] Omar et al.,[35] European Society of Radiology (ESR),[39] Zhuang et al.,[47] Taloba et al.,[55] Siyal et al.,[40] Rana et al.,[45] Zhuang et al.,[48] Khatoon et al.,[50] Marbouh et al.,[52] Zhuang et al.[63]
Hyperledger fabric	2	Brown et al.,[58] Chen et al.[49]
Hyperledger sawtooth	1	Chen et al.[49]
Hyperledger caliper	2	Zaabar et al.,[19] Chen et al.[49]
FHIRChain	2	Zhang et al.,[42] Omar et al.[35]
Quorum	1	Zhuang et al.[57]
Security techniques		
Smart contracts	23	Kasyapa et al.,[16] Brown et al.,[58] Aljaloud et al.,[41] Zhuang et al.,[57] Chen et al.,[49] Rahman et al.,[38] Zhang et al.,[42] Harrell et al.,[34] Plebani et al.,[43] Ali et al.,[44] Gordon et al.,[32] Saleh et al.,[37] Motohashi et al.,[31] Omar et al.,[35] Khatri et al.,[51] Zhuang et al.,[47] Taloba et al.,[55] Siyal et al.,[40] Rana et al.,[45] Zhuang et al.,[48] Khatoon et al.,[50] Marbouh et al.,[52] Zhuang et al.[63]
Public key infrastructure	2	Zhang et al.,[42] Gordon et al.[32]
Zero-knowledge proofs	2	Zhang et al.,[42] Gordon et al.[32]
Cryptographic algorithms	8	Oakley et al.,[46] Aljaloud et al.,[41] Zhang et al.,[42] Ali et al.,[44] Saleh et al.,[37] Omar et al.,[35] Taloba et al.,[55] Marbouh et al.[52]
Data sufficiency assessment	1	Hovorushchenko et al.[30]
Hashchain	3	Ali et al.,[44] Hirano et al.,[36] Motohashi et al.[31]
Audit trail	5	Zhang et al.,[42] Ali et al.,[44] Gordon et al.,[32] Saleh et al.,[37] Gonzales et al.[56]
Consensus mechanisms		
Proof of work	3	Zhang et al.,[42] Omar et al.,[35] Rana et al.[45]
Proof of stake	2	Omar et al.,[35] Zhuang et al.[48]
Proof of authority	3	Yaqoob et al.,[60] Arul et al.,[61] Rana et al.[45]
Blockchain-based frameworks and development tools		
JavaScript	4	Aljaloud et al.,[41] Zhang et al.,[42] Harrell et al.,[34] Zhuang et al.[47]
Solidity	2	Aljaloud et al.,[41] Zhang et al.[42]
Ganache	2	Oakley et al.,[46] Aljaloud et al.[41]
MetaMask	2	Aljaloud et al.,[41] Rahman et al.[38]
Docker containers	1	Chen et al.[49]
Visual studio code	1	Aljaloud et al.[41]
Remix IDE	2	Aljaloud et al.,[41] Zhuang et al.[57]
Blockchain-as-a-Service	4	Attaran et al.,[5] Zhang et al.,[42] Saleh et al.,[37] Hovorushchenko et al.[30]
InterPlanetary File System	5	Kasyapa et al.,[16] Milone et al.,[20] Rahman et al.,[38] Plebani et al.,[43] Khatoon et al.[50]

FHIR: fast health interoperability resources; IDE: integrated development environments

Imaging and Communications in Medicine (DICOM) remains in PACS/VNA, while Service-Object Pair (SOP) unique identifiers (UIDs) and checksums—sometimes with IPFS links—are committed on-chain,[38,64] and audit trails mirror ISO 27789 by immutably logging who/what/when/where events.[39,59]

Overall, PHI stays in systems of record, while the ledger provides integrity, provenance, and consent attestations.

RQ5. How does blockchain technology integrate with and enhance other emerging healthcare technologies? Blockchain technology improves healthcare technologies by offering a framework that is safe, compatible, and patient-focused (Table 6). It also supports innovation in clinical and administrative procedures and meets important demands across a range of healthcare applications.

The different areas in healthcare are slowly implementing blockchain technology in the promotion of patient-centered governance, data security, and interoperability.[47,58] With regard to interoperability issues found in EHR, blockchain efficiently allows the sharing of data from one provider to another without compromising the integrity of data, thus gives power to patients over their records, which may bring about effective care coordination and compliance with rules of privacy.[42,51]

In addition, IoMT benefits from the security features of blockchain because it protects data coming from

Table 5. Standards and interoperability patterns reported in included studies.

Standard	Interoperability goal	Typical integration pattern	Example in corpus
HL7 FHIR/ SMART-on-FHIR	Normalized resource exchange across EHR/HIE	Expose REST endpoints; keep payloads off-chain; persist SHA-256 of FHIR resources and consent refs on-chain; use SMART scopes for authorization	FHIRChain pattern[42]; patient wallet/ workflow[34]
HL7 v2 / CDA	Bridge legacy feeds/documents into modern APIs	ETL/mapping from v2/CDA → FHIR; anchor document hash/URI on-chain; originals remain in EHR	Legacy bridge discussed in[42]; policy/ authZ context[43]
IHE XDS.b/XCA	Cross-repository/community document sharing	Store documents in XDS repo; write doc UUID + hash + policy pointer on-chain; use XCA for federated query	Trial data/doc sharing context[58]; consent/audit pointers[44]
DICOM (imaging)	Imaging integrity and linkage to PACS/VNA	Keep DICOM off-chain (PACS/VNA); record SOP Instance UID + checksum and optional off-chain link (e.g., IPFS) on-chain	Hybrid on/off-chain storage[64]; IPFS pointer demo[38]
ISO 27789 (EHR audit)	Standards-aligned EHR audit trails	Mirror read/write/access events (who/ what/when/where) to ledger for immutable provenance; align fields to ISO audit model	Provenance/audit models[59]; compliance mapping[39]

API: application programming interface; Authz: authorization; CDA: clinical document architecture; DICOM: Digital Imaging and Communications in Medicine; EHR/ HIE: electronic health record/health information exchange; ETL: extract, transform, and load; FHIR: Fast Healthcare Interoperability Resources; HL7 FHIR/SMART-on-FHIR: Health Level Seven Fast Healthcare Interoperability Resources / Substitutable Medical Applications and Reusable Technologies on FHIR; HL7 v2/CDA: Health Level Seven Version 2/Clinical Document Architecture; IHE XDS.b: Integrating Healthcare Enterprise, Cross-Enterprise Document Sharing; IPNS: InterPlanetary Name System; IPS: Interplanetary File System; ISO: International Organization for Standardization; PACS: picture archiving and communication system; REST: representational state transfer; SHA-256: secure hash algorithm 256-bit; SMART: A self-executing, digital contract; SOP: service-object pair; SSHA: secure hashing algorithm; UID: unique identifiers; UUID: universally unique identifier; VNA: vendor neutral archive; XCA: cross-community access; XDS: cross enterprise document sharing.

connected devices, including wearables and remote monitors.[31,48,50] The blockchain ensures that the data produced by the patients remain tamper-proof and trustworthy, thus making sure that accurate, real-time monitoring is achieved in order to manage chronic diseases and preventive care effectively.[16,45]

Moreover, blockchain enhances the quality and integrity of data, which boosts AI. The training of AI models is based on secure, good-quality data, and the immutability of blockchain ensures that the data are reliable and consistent.[45,47] This linkage provides diagnostic and predictive analytics, resulting in improved, reliable clinical insight and decision-making.[16,51,57]

Another key area by controlling data access and confirming patient identities, blockchain technology in telemedicine protects data exchange during online consultations. Furthermore, blockchain-based smart contracts automate administrative tasks and ensure transparency through streamlined consent and billing processes.[42]

Table 6. Integration of blockchain with emerging healthcare technologies.

Healthcare technology	Blockchain integration	Description and enhancement
Electronic health records	Interoperability	Blockchain enables seamless data sharing across healthcare providers, ensuring data integrity and patient control over records, which enhances interoperability and care coordination.[42,58]
Internet of medical things	Data security	By securing data from IoMT devices, blockchain ensures tamper-proof and reliable data transmission, facilitating real-time patient monitoring.[31,48,50]
Artificial intelligence	Data quality	Blockchain provides a secure data source for AI training, ensuring high-quality data that enhance predictive analytics and clinical decision-making reliability.[45,47]
Telemedicine	Secure data exchange	Blockchain secures patient data in telemedicine, verifying patient identities, managing consent, and automating billing through smart contracts.[42]
Health information exchange	Interoperable data sharing	Blockchain improves HIE by securely enabling comprehensive data access across healthcare providers, supporting a unified patient record.[47,48]
Data analytics	Secure aggregation	Blockchain allows for secure data aggregation and analytics, enabling insights into patient outcomes and public health trends while maintaining privacy.[43,51,57]

EHR: electronic health record; IoMT: Internet of Medical Things; AI: artificial intelligence; HIE: health information exchange.

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

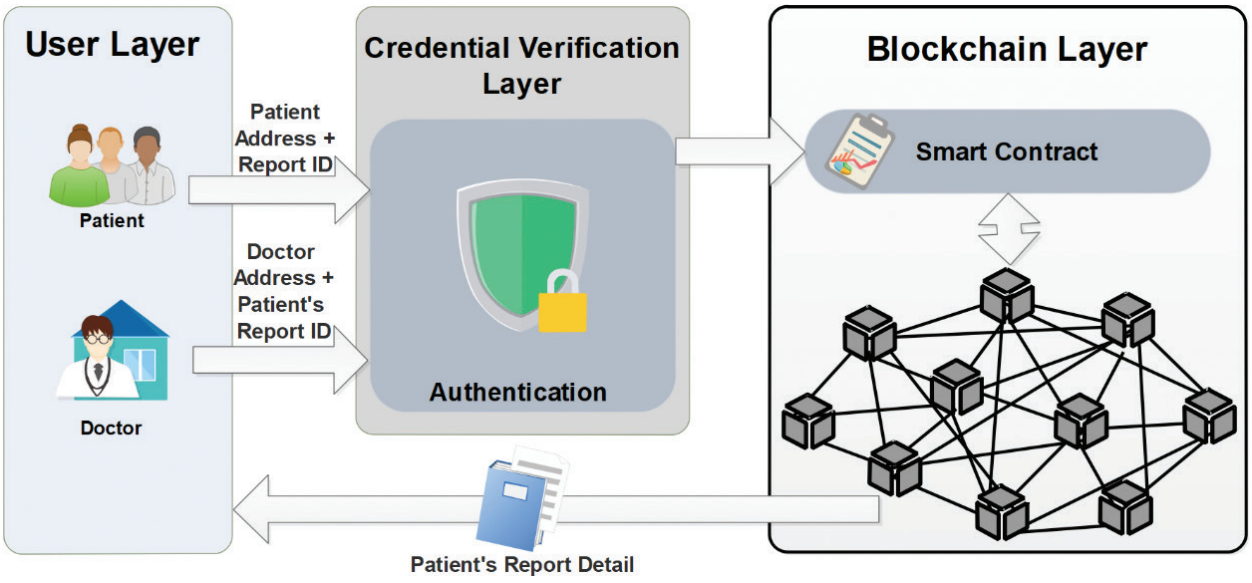

Fig. 3. Data accessing process (adapted from Aljaloud et al. [2023]) (41).

Furthermore, a strengthened and comprehensive patient record is made possible by the blockchain's capacity to support interoperable data sharing among healthcare providers, which facilitates health information exchange. By guaranteeing consistent data access, this capacity improves the standard and continuity of patient treatment.[47,48]

Finally, to draw conclusions about patient results and public health trends, data analytics in healthcare depends on safe aggregated data.[43,57] By enabling data aggregation that preserves privacy, the blockchain makes it possible to perform analytics on precise data while adhering to privacy regulations.[16,51]

Also, Figure 4 illustrates a conceptual architecture that demonstrates the synergistic integration of blockchain with key healthcare technologies—namely, AI, IoMT, and EHR. At the core of this architecture, blockchain acts as a secure and decentralized layer that ensures data immutability, traceability, and access control. Clinical data generated from IoMT devices—such as wearable monitors, sensors, and smart medical equipment—are transmitted in real time and securely stored via blockchain-enabled channels. Simultaneously, EHR systems interface with the blockchain to update and retrieve patient records while preserving data integrity and ensuring compliance with privacy regulations. AI modules interact with the blockchain to perform analytics, risk prediction, and decision support based on trusted and tamper-proof data inputs. Smart contracts orchestrate interactions between all components, automating tasks such as access permissions, billing, and consent management. This integrated flow supports a patient-centered, interoperable, and intelligent healthcare ecosystem, capable of responding to real-time clinical needs with enhanced security, transparency, and operational efficiency.

Discussion

This discussion focuses on implications for operational adoption of blockchain in CDM, rather than restating descriptive results. An important maturity gap emerges when contrasting narrative/architectural papers with metric-driven evaluations. In our corpus, only seven studies report quantitative performance or operational metrics (Appendix B), whereas 25 studies are primarily conceptual or design-oriented (Appendix C). Consequently, several claims regarding throughput, latency, and scalability remain difficult to compare across platforms because benchmarks, workloads, and reporting formats are not standardized.

Reported performance figures vary widely across prototypes and experiments, but comparisons are limited by non-harmonized workloads, baselines, and reporting practices (Appendix B).

From a regulatory perspective, our synthesis extends beyond GDPR-based considerations to include the U.S. framework for electronic records and electronic signatures (FDA 21 CFR Part 11). Part 11 emphasizes trustworthy and reliable electronic records, including secure, computer-generated, time-stamped audit trails, and controls for record changes. Blockchain's append-only data structure aligns naturally with auditability requirements; however, clinical workflows still require correction of data entry errors. In practice, such corrections can be implemented as new transactions that supersede prior entries while preserving an immutable history, thereby maintaining the audit trail expected by auditors.

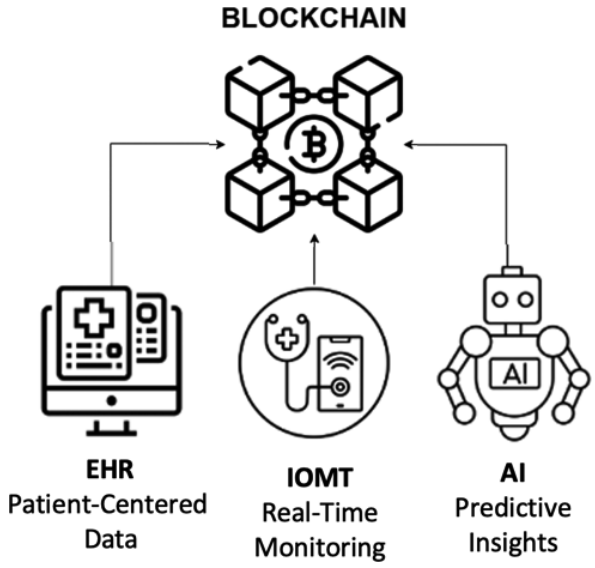

Fig. 4. Conceptual architecture showing the integration of blockchain with artificial intelligence (AI), Internet of Medical Things (IoMT), and electronic health records (EHRs) systems to enhance secure, interoperable, and intelligent clinical data management (CDM).

Most solutions rely on off-chain storage with on-chain anchoring, which is practical for limiting on-chain data exposure; however, this approach shifts engineering effort toward integration, key management, and operational governance of the off-chain components.

To avoid ambiguity in consent management, we distinguish between managing the consent document and managing the consent state. The consent document can be stored off-chain (e.g., as a PDF), while the consent state and policy logic (grant/revoke, expiry, role-based constraints) can be implemented on-chain via smart contracts and recorded in immutable logs. This separation supports both storage efficiency and transparent compliance reporting.

Although the review identifies multiple blockchain-enabled designs for CDM, practical validation remains limited relative to conceptual proposals. This imbalance reflects a broader "deployment maturity" challenge: the technical primitives may be well understood, but real-world uptake depends on socio-technical readiness in clinical environments.

First, integration burden remains a dominant barrier. Even when blockchain is used only as an audit/coordination layer, deployment typically requires tight integration with existing EHR/EDC (Electronic Data Capture) systems, identity and access management, and operational workflows. This integration cost and workflow disruption help explain why many contributions remain at prototype or pilot stage.

Second, governance and incentive alignment are non-trivial in multi-stakeholder settings (sites, sponsors, conversion rate optimizations, laboratories, regulators). Consortium decisions—who operates nodes, who is accountable for outages, how upgrades are governed, and how liabilities are allocated—often determine feasibility more than the ledger design itself.

Third, regulatory and validation burden shapes adoption. In addition to GDPR-oriented constraints (e.g., tensions between immutability and rights such as erasure/rectification, and ambiguity of data-controller roles), regulated clinical research requires validated systems and audit trail controls (e.g., Part 11 expectations for secure, computer-generated, time-stamped audit trails and controlled record changes). These requirements increase implementation effort and may slow production deployment even when conceptual compliance claims are strong.

Overall, operational readiness under realistic workloads remains uncertain because evaluation practices and reporting vary substantially across studies. As a result, it is difficult to translate prototype results into predictable service levels suitable for routine clinical operations.

Limitations and Future Work

This review followed the search, screening, and quality-assessment process described in Section 3 to support transparency and reproducibility.

Two challenges emerged during the selection process. First, a challenge faced was the different indexing of blockchain-related healthcare research articles, where the different databases sometimes failed to present continuous results, which could be due to the variability of the terminology used. Second, the wide array of uses of blockchain in the healthcare system created a problem for the authors in defining the area of coverage while including the studies.

Future research directions identified in the reviewed studies point to a variety of opportunities. Most effort will be put into optimizing blockchain scalability in clinical trials and healthcare data management frameworks, with a focus on improving the accuracy of privacy-preserving algorithms. Another strong emphasis will be on incorporating AI and machine learning for advanced data analytics. There will also be efforts toward advancing more efficient federated learning models, exploring hybrid methodologies that combine both centralized and decentralized strategies, and solving synchronization problems in cooperative healthcare environments. Also, it will involve IoT integration for real-time monitoring and the creation of emergency preparedness exercises that further improve the identity management of patients through advanced digital solutions.

Other research paths underline the application of blockchain in diverse contexts of healthcare, including infectious disease tracking, precision medicine, and neurotechnological applications. Scalability testing, formal verification of smart contracts, and frameworks ensuring regulatory compliance are needed to achieve

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

interoperability of the blockchain systems within the healthcare infrastructures globally. The other important proposals include the development of more integrated applications of blockchain technology for EHRs, enabling the safe sharing of data across borders and exploring new incentive structures, including the use of cryptocurrency for validation and compensation in clinical trials.

These directions aim to move blockchain-based CDM from conceptual designs toward validated, interoperable, and regulation-ready implementations.

Conclusion

This systematic review of existing literature aims to provide an overview of the research that has been conducted with regard to the use of blockchain in CDM within the medical field.

In the present study, several key findings regarding the capacity of blockchain to transform the clinical data handling process are identified, including improvements in data security, privacy, and integration. However, persistent issues associated with blockchain solutions remain, including scaling challenges, interaction with traditional systems, and sustainability in terms of energy resources. Addressing these technical and legal limitations is essential for broader adoption in healthcare.

Across the reviewed studies, Ethereum and HF are dominant platforms, commonly employed for reliable transactions and smart contract implementations. The trends also show growing integration with technologies such as AI and IoMT, highlighting applications in data protection, analysis, and live tracking, which suggests opportunities for more advanced clinical data workflows.

Finally, the literature remains limited in terms of deployment evidence and standardized evaluation, particularly for regulatory compliance and performance under realistic clinical workloads. Future work should prioritize comparable benchmarks and real-world validation to support translation of blockchain-based CDM designs into routine practice.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declare no competing financial or non-financial interests.

Contributors

Khaoula Chafik performed the systematic literature review, selected and analyzed the final set of studies, interpreted the findings on blockchain in CDM, and drafted the manuscript. Prof. Mohamed Hanine (supervisor) defined the research direction, refined the research questions and methodology, and provided critical review and supervision throughout the work. Prof. Abdellah Ouaguid (co-supervisor) contributed to validating the technical and regulatory interpretation of the results and revised the manuscript for clarity and rigor. Dr. Sulieman Alshuhri (expert reviewer) assessed the practical relevance of the work for real-world healthcare systems and provided critical feedback that informed the Discussion and Future Work sections. All authors approved the final manuscript and its submission.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

The data supporting the findings of this systematic review are derived from published studies indexed in Web of Science and Scopus. No new datasets were generated or analyzed beyond those included in the reviewed literature.

Additional details can be made available from the corresponding author upon reasonable request.

Application of AI-Generated Text or Related Technology

We used AI-assisted tools to support language editing/refining and restructuring of text for clarity (e.g., improving grammar, readability, and formatting). All content, interpretations, and conclusions were reviewed and verified by the authors, who take full responsibility for the manuscript.

Acknowledgments

The authors acknowledge the Laboratory of Information Technologies (LTI), National School of Applied Sciences (ENSA), Chouaib Doukkali University, El Jadida, Morocco, for institutional support. We also thank our supervisors for their guidance and expert feedback during this work.

References

1. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. Healthcare (Basel). 2019;7:56. https://doi.org/10.3390/healthcare7020056
2. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain technology in healthcare: a comprehensive review and directions for future research. Appl Sci (Basel). 2019;9(9):1736. https://doi.org/10.3390/app9091736
3. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—a scoping review. Int J Med Inform. 2020;134:104040. https://doi.org/10.1016/j.ijmedinf.2019.104040
4. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare. Symmetry (Basel). 2018;10(10):470. https://doi.org/10.3390/sym10100470
5. Attaran M. Blockchain technology in healthcare: challenges and opportunities. Int J Healthc Manag. 2022;15(1):70–83. https://doi.org/10.1080/20479700.2020.1843887

6. Tandon A, Dhir A, Islam AKMN, Mäntymäki M. Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. Comput Ind. 2020;122:103290. https://doi.org/10.1016/j.compind.2020.103290
7. Saeed H, Malik H, Bashir U, Ahmad A, Riaz S, Ilyas M, et al. Blockchain technology in healthcare: a systematic review. PLoS One. 2022;17(4):e0266462. https://doi.org/10.1371/journal.pone.0266462
8. Krishnankutty B, Bellary S, Kumar NB, Moodahadu LS. Data management in clinical research: an overview. Indian J Pharmacol. 2012;44(2):168–72. https://doi.org/10.4103/0253-7613.93842
9. Ittenbach RF. From clinical data management to clinical data science: time for a new educational model. Clin Transl Sci. 2023;16(8):1340–51. https://doi.org/10.1111/cts.13545
10. Banach MA, Fendt KH, Proeve J, Plummer D, Qureshi S, Limaye N. Clinical data management in the United States: where we have been and where we are going. J Soc Clin Data Manag. 2022;1(S1):61. https://doi.org/10.47912/jscdm.61
11. Treiblmaier H, Rejeb A, Gault M, Khurshid A, Norta A, Poteet J, et al. Harnessing blockchain to transform healthcare data management: a comprehensive research agenda. Blockchain Healthc Today. 2024;7:301. https://doi.org/10.30953/bhty.v7.301
12. Han Y, Zhang Y, Vermund SH. Blockchain technology for electronic health records. Int J Environ Res Public Health. 2022;19(23):15577. https://doi.org/10.3390/ijerph192315577
13. AbdelSalam FM. Blockchain revolutionizing healthcare industry: a systematic review of blockchain technology benefits and threats. Perspect Health Inf Manag [Internet]. 2023;20(3):1b. [cited 2025 Nov 01]. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC10701638/
14. Schmeelk S, Kanabar M, Peterson K, Pathak J. Electronic health records and blockchain interoperability requirements: a scoping review. JAMIA Open. 2022;5(3):ooac068. https://doi.org/10.1093/jamiaopen/ooac068
15. Fang HSA, Tan TH, Tan YFC, Tan CJM. Blockchain personal health records: systematic review. J Med Internet Res. 2021;23(4):e25094. https://doi.org/10.2196/25094
16. Kasyapa MSB, Vanmathi C. Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies. Front Digit Health. 2024;6:1359858. https://doi.org/10.3389/fdgth.2024.1359858
17. Tagde P, Tagde S, Bhattacharya T, Tagde P, Chopra H, Akter R, et al. Blockchain and artificial intelligence technology in e-health. Environ Sci Pollut Res Int. 2021;28:52810–31. https://doi.org/10.1007/s11356-021-16223-0
18. Dubovitskaya A, Baig F, Xu Z, Shukla R, Zambani PS, Swaminathan A, et al. Action-EHR: patient-centric blockchain-based electronic health record data management for cancer care. J Med Internet Res. 2020;22(8):e13598. https://doi.org/10.2196/13598
19. Zaabar B, Cheikhrouhou O, Jamil F, Ammi M, Abid M. HealthBlock: a secure blockchain-based healthcare data management system. Comput Netw. 2021;200:108500. https://doi.org/10.1016/j.comnet.2021.108500
20. Milone V, Fusco A, De Feo A, Tatullo M. Clinical impact of "real world data" and blockchain on public health: a scoping review. Int J Environ Res Public Health. 2024;21(1):95. https://doi.org/10.3390/ijerph21010095
21. Ouaguid A, Hanine M, Chiba Z, Abghour N, Ghazal H. Analysis of blockchain integration in the e-healthcare ecosystem. In: 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet). Rabat, Morocco; 11–13 Dec 2023. IEEE; 2023. pp. 1–8. https://doi.org/10.1109/CommNet60167.2023.10365182
22. Ouaguid A, Hanine M, Chiba Z, Abghour N, Ghazal H. Analysis of blockchain integration in the e-healthcare ecosystem. In: 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet). Rabat, Morocco; 11–13 Dec 2023. IEEE; 2023. pp. 1–8. https://doi.org/10.1109/CommNet60167.2023.10365182
23. Shruthi K, Poornima AS. Medical data asset management and an approach for disease prediction using blockchain and machine learning. Int J Eng Trends Technol. 2023;71(4):491–514. https://doi.org/10.14445/22315381/IJETT-V71I4P242
24. Kiania K, Jameii SM, Rahmani AM. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl. 2023;82(18):28493–519. https://doi.org/10.1007/s11042-023-14488-w
25. Eldawlatly A, Alshehri H, Alqahtani A, Ahmad A, Al-Dammas F, Marzouk A. Appearance of population, intervention, comparison, and outcome as research question in the title of articles of three different anesthesia journals: a pilot study. Saudi J Anaesth. 2018;12(2):283–6. https://doi.org/10.4103/sja.SJA_767_17
26. Wang Q, Qin S. A Hyperledger Fabric-based system framework for healthcare data management. Appl Sci (Basel). 2021;11(24):11693. https://doi.org/10.3390/app112411693
27. Wang H, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J Med Syst. 2018;42:152. https://doi.org/10.1007/s10916-018-0994-6
28. Hajela P, Pawar A, Phansalkar S. ITreatU: an effective privacy and security solution for healthcare data using the R3 Corda platform of blockchain technology. In: Data Protection and Privacy in Healthcare. Boca Raton, FL: CRC Press; 2021, pp. 165–179. https://doi.org/10.1201/9781003048848-9
29. Petersen K, Vakkalanka S, Kuzniarz L. Guidelines for conducting systematic mapping studies in software engineering: an update. Inf Softw Technol. 2015;64:1–18. https://doi.org/10.1016/j.infsof.2015.03.007
30. Hovorushchenko T, Moskalenko A, Osyadlyi V. Methods of medical data management based on blockchain technologies. J Reliab Intell Environ. 2023;9(1):5–16. https://doi.org/10.1007/s40860-022-00178-1
31. Motohashi T, Hirano T, Okumura K, Kashiyama M, Ichikawa D, Ueno T. Secure and scalable mHealth data management using blockchain combined with client hashchain: system design and validation. J Med Internet Res. 2019;21(5):e13385. https://doi.org/10.2196/13385
32. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J. 2018;16:224–30. https://doi.org/10.1016/j.csbj.2018.06.003
33. Bautista JR, Harrell DT, Hanson L, de Oliveira E, Abdul-Moheeth M, Meyer ET, et al. MediLinker: a blockchain-based decentralized health information management platform for patient-centric healthcare. Front Big Data. 2023;6:1146023. https://doi.org/10.3389/fdata.2023.1146023
34. Harrell DT, Usman M, Hanson L, Abdul-Moheeth M, Desai I, Shriram J, et al. Technical design and development of a self-sovereign identity management platform for patient-centric health care using blockchain technology. Blockchain Healthc Today. 2022;5:196. https://doi.org/10.30953/bhty.v5.196
35. Omar IA, Jayaraman R, Salah K, Yaqoob I, Ellahham S. Applications of blockchain technology in clinical trials: review and open challenges. Arab J Sci Eng. 2021;46(4):3001–15. https://doi.org/10.1007/s13369-020-04989-3
36. Hirano T, Motohashi T, Okumura K, Takajo K, Kuroki T, Ichikawa D, et al. Data validation and verification using

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

blockchain in a clinical trial for breast cancer: regulatory sandbox. J Med Internet Res. 2020;22(6):e18938. https://doi.org/10.2196/18938
37. Saleh S, Shayor F. High-level design and rapid implementation of a clinical and non-clinical blockchain-based data sharing platform for COVID-19 containment. Front Blockchain. 2020;3:553257. https://doi.org/10.3389/fbloc.2020.553257
38. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced Internet of Health Things framework: a blockchain managed federated learning approach. IEEE Access. 2020;8:205071–87. https://doi.org/10.1109/ACCESS.2020.3037474
39. European Society of Radiology (ESR). ESR white paper: blockchain and medical imaging. Insights Imaging. 2021;12(1):82. https://doi.org/10.1186/s13244-021-01029-y
40. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography. 2019;3(1):3. https://doi.org/10.3390/cryptography3010003
41. Aljaloud A, Razzaq A. Modernizing the legacy healthcare system to decentralize platform using blockchain technology. Technologies (Basel). 2023;11(4):84. https://doi.org/10.3390/technologies11040084
42. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J. 2018;16:267–78. https://doi.org/10.1016/j.csbj.2018.07.004
43. Plebani P, Rossetto D, Tiezzi F. Empowering trusted data sharing for data analytics in a federated environment: a blockchain-based approach. Front Blockchain. 2023;6:1141760. https://doi.org/10.3389/fbloc.2023.1141760
44. Ali A, Al-Rimy BAS, Tin TT, Altamimi SN, Qasem SN, Saeed F. Empowering precision medicine: unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. Sensors (Basel). 2023;23(17):7476. https://doi.org/10.3390/s23177476
45. Rana SK, Rana SK, Nisar K, Ag Ibrahim AA, Rana AK, Goyal N, et al. Blockchain technology and artificial intelligence-based decentralized access control model to enable secure interoperability for healthcare. Sustainability. 2022;14(15):9471. https://doi.org/10.3390/su14159471
46. Oakley J, Worley C, Yu L, Brooks RR, Özçelik İ, Skjellum A, et al. Scrybe: a secure audit trail for clinical trial data fusion. Digit Threat Res Pract. 2023;4(2):1–20. https://doi.org/10.1145/3491258
47. Zhuang Y, Chen Y-W, Shae Z-Y, Shyu C-R. Generalizable layered blockchain architecture for health care applications: development, case studies, and evaluation. J Med Internet Res. 2020;22(7):e19029. https://doi.org/10.2196/19029
48. Zhuang Y, Sheets L, Shae Z, Tsai JJP, Shyu CR. Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. AMIA Annu Symp Proc. 2018; 2018:1167–75.
49. Chen S, Cao Q, Cai Y. Blockchain for healthcare games management. Electronics (Basel). 2023;12(14):3195. https://doi.org/10.3390/electronics12143195
50. Khatoon A. A blockchain-based smart contract system for healthcare management. Electronics (Basel). 2020;9(1):94. https://doi.org/10.3390/electronics9010094
51. Khatri S, Al Sulbi K, Attaallah A, Ansari MTJ, Agrawal A, Kumar R. Enhancing healthcare management during COVID-19: a patient-centric architectural framework enabled by Hyperledger Fabric blockchain. Information (Basel). 2023;14(8):425. https://doi.org/10.3390/info14080425
52. Marbouh D, Abbasi T, Maasmi F, Omar IA, Debe MS, Salah K, et al. Blockchain for COVID-19: review, opportunities, and a trusted tracking system. Arab J Sci Eng. 2020;45:9895–911. https://doi.org/10.1007/s13369-020-04950-4
53. Molli VLP. Blockchain technology for secure and transparent health data management: opportunities and challenges. J Healthc AI ML [Internet]. 2023;10(10):1–15. [cited 2025 Nov 01]. Available from: https://journalpublication.wrcouncil.org/index.php/JHAM/article/view/9
54. Chang Y, Fang C, Sun W. A blockchain-based federated learning method for smart healthcare. Comput Intell Neurosci. 2021;2021:4376418. https://doi.org/10.1155/2021/4376418
55. Taloba AI, Rayan A, Elhadad A, Abozeid A, Shahin OR, Abd El-Aziz RM. A framework for secure healthcare data management using blockchain technology. Int J Adv Comput Sci Appl. 2021;12(12):951–61. https://doi.org/10.14569/IJACSA.2021.0121280
56. Gonzales A, Smith SR, Dullabh P, Hovey L, Heaney-Huls K, Robichaud M, et al. Potential uses of blockchain technology for outcomes research on opioids. JMIR Med Inform. 2021;9(8):e16293. https://doi.org/10.2196/16293
57. Zhuang Y, Zhang L, Gao X, Shae ZY, Tsai JJP, Li P, et al. Re-engineering a clinical trial management system using blockchain technology: system design, development, and case studies. J Med Internet Res. 2022;24(6):e36774. https://doi.org/10.2196/36774
58. Brown J, Bhatnagar M, Gordon H, Lutrick K, Goodner J, Blum J, et al. Clinical data extraction during public health emergencies: a blockchain technology assessment. Biomed Instrum Technol. 2021;55(3):103–11. https://doi.org/10.2345/0899-8205-55.3.103
59. Velmovitsky PE, Bublitz FM, Fadrique LX, Morita PP. Blockchain applications in health care and public health: increased transparency. JMIR Med Inform. 2021;9(6):e20713. https://doi.org/10.2196/20713
60. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Appl. 2022;34(14):11475–90. https://doi.org/10.1007/s00521-020-05519-w
61. Arul P, Renuka S. Blockchain technology using consensus mechanism for IoT-based e-healthcare system. IOP Conf Ser Mater Sci Eng. 2021;1055:012106. https://doi.org/10.1088/1757-899X/1055/1/012106
62. Javed IT, Alharbi F, Bellaj B, Margaria T, Crespi N, Qureshi KN. Health-ID: a blockchain-based decentralized identity management for remote healthcare. Healthcare (Basel). 2021;9:712. https://doi.org/10.3390/healthcare9060712
63. Zhuang Y, Sheets L, Gao X, Shen Y, Shae ZY, Tsai JJP, et al. Development of a blockchain framework for virtual clinical trials. AMIA Annu Symp Proc. 2021; Jan 25;2020:1412–20.
64. Al Mamun A, Jahangir MUF, Azam S, Kaiser MS, Karim A. A combined framework of Interplanetary File System and blockchain to securely manage electronic medical records. In: Proceedings of the International Conference on Trends in Computational and Cognitive Engineering (TCCE 2020: 17–18 Dec 2020). Singapore: Springer; 2021, pp. 501–11. https://doi.org/10.1007/978-981-33-4673-4_40

Appendix A. Extracted variables and mapping to RQ1–RQ5.

Information	Review question(s)
Blockchain application context	RQ1
Blockchain role in security and privacy	RQ2
Blockchain techniques	RQ1, RQ4
Integration with emerging technologies (AI, IoT)	RQ5
Key technical challenges	RQ3
Common blockchain technologies for clinical data management	RQ4
Datasets used	RQ1, RQ3
Limitations	RQ3, RQ4
Open challenges	RQ3
Empirical results	RQ2, RQ3
Blockchain frameworks	RQ1
Interoperability with healthcare systems	RQ5

AI: artificial intelligence; IoT: Internet of Things; RQ: research questions.

Appendix B. Evaluation datasets and metrics studies with reported metrics/observations.

Study	Domain	Dataset type	Data items (examples)	Metrics	Tooling
Brown and Bhatnagar (2021)[58]	Clinical trials (breast cancer RCT)	Real-world	ePRO entries; consent	Operational continuity (zero downtime during AWS outage); tamper-evidence (qualitative)	Hyperledger Fabric (on AWS)
Oakley, and Worley C (2023)[46]	EDC/REDCap integration	Demon-strator	REDCap forms; survey submissions	~13 tx/s prototype; qualitative latency	Ethereum test net (Ganache); REDCap connector
Aljaloud, and Razzaq (2023)[41]	EHR/secure storage	Demonstrator	Patient file(s) to IPFS + on-chain pointer	Qualitative demo (upload/con-firm); no TPS	Ethereum (Remix/ Solidity/MetaMask); IPFS
Zhuang and Zhang L (2022)[57]	Clinical trials (eCRF + IPFS)	Synthetic at scale	eCRF submissions; consent/provenance events	Throughput and latency at scale; approximately 1.2 million transactions completed	Smart contracts; IPFS; blockchain network
Chen S and Cao Q (2023)[49]	EHR data sharing (patient-centric)	Synthetic (Caliper)	EHR tx & query workloads; consent logs	TPS, latency, CPU util. (Caliper reports)	Hyperledger Fabric; Caliper; Docker
Rahman and Hossain (2020)[38]	Medical data storage	Demonstrator	On-chain refs; file upload to IPFS	Upload time; gas/tx cost	Ethereum (Ganache/ MetaMask); IPFS
Zaabar, and Cheikhrouhou (2021)[19]	Permissioned chain benchmarking (healthcare)	Synthetic (Cali-per)	Invoke/query workloads; block sizes; chaincode ops	TPS, latency, resource utilization under varying peers/orderers	Hyperledger Fabric; Caliper; Docker/K8s

AWS: Amazon Web Services; CPU: central processing unit ; EDC: Electronic Data Capture; ePRO: electronic Patient-Reported Outcomes; IPFS: Interplanetary File System; REDCap: Research Electronic Data Capture; K8s: Kubernetes; RCT: randomized clinical trial; TPS: Transactions Per Second; tx: transactions.

Citation: Blockchain in Healthcare Today 2026, **8**: 471 - https://doi.org/10.30953/bhty.v8.471

Appendix C. Content summary of narrative/architectural works.

Reference	Domain	Primary focus	Approach	Evaluation type
Zhang and White (2018)[42]	EHR/HIE (FHIR)	Interoperability; consent; privacy	FHIRChain pattern; consent registry; on-chain audit	Conceptual/ architecture
Harrell and Usman (2022)[34]	Patient wallet/identity	Patient-centric data sharing; trust	MediLinker workflow; verifiable sharing	Prototype/demo
Plebani and Rossetto (2023)[43]	Access control	MFA/authorization; accountability	Policy-driven access; audit trails	Conceptual
Ali and Al-Rimy (2023)[44]	Consent & audit	Consent lifecycle; provenance	Smart-contract policies; immutable logs	Conceptual
Kiania and Jameii (2023)[24]	EHR security	Privacy protocols; limitations	Protocol review; mitigation guidelines	Conceptual/synthesis
Gordon and Catalini (2018)[32]	Health records	Architecture; incentives and trust	Design primitives; governance considerations	Conceptual
Hirano and Motohashi (2020)[36]	Interop/provenance	Hash-chain for data lineage	Hash anchoring; reference architecture	Conceptual
Saleh and Shayor (2020)[37]	Secure sharing	Integrity; traceability; audit	Policy templates; auditability design	Conceptual
Motohashi and Hirano (2019)[31]	mHealth/IoMT	Tamper-evident logs	Hashchain-based auditing	Conceptual
Javed and Alharbi (2021)[62]	Identity/DIDs	Patient/provider identity	DIDs/VCs; trust registry	Conceptual
Attaran (2022)[5]	Review/survey	Landscape; use cases; issues	Narrative/system perspective	Review
Tandon and Dhir (2020)[6]	Review/survey	PHR/EHR; pros/cons	Taxonomy; design guidance	Review
Saeed and Malik (2022)[7]	Governance/rights	Patient rights; compliance	Policy analysis; patterns	Review/position
Kasyapa and Vanmathi (2024)[16]	Patient control	Key-based control; consent	Patient-centric access model	Conceptual
Hovorushchenko and Moskalenko (2023)[30]	Data quality	Data sufficiency/quality checks	Methodological framework	Conceptual/method
Milone and Fusco (2024)[20]	Sustainability	Energy, scalability, trade-offs	Comparative analysis	Conceptual/analysis
Omar and Jayaraman (2021)[35]	Smart contracts	Consent/billing automation	Policy smart contracts	Conceptual
European Society of Radiology (2021)[39]	Compliance	GDPR/ESR implications	Compliance mapping; auditability	Position/compliance
Khatri and Al Sulbi (2023)[51]	Integrity/traceability	Tamper-proof records; privacy	On-chain logs; access patterns	Conceptual
Velmovitsky and Bublitz (2021)[59]	Auditability	Provenance models in e-health	Merkle/audit schemes	Conceptual
Al Mamun and Jahangir (2021)[64]	Storage	Off-chain files (IPFS)	IPFS + on-chain references	Conceptual
Yaqoob and Salah (2022)[60]	Consensus	PoW/PoS/PoA trade-offs	Tech survey (health context)	Review/technology
Arul and Renuka (2021)[61]	Consensus/PoA	Validator trust; latency	PoA overview for apps	Review/technology
Zhuang and Chen (2020)[47]	Patient-centric EHR sharing	Generalizable blockchain pattern	Node.js/Web3.js stack; smart contracts; off-chain storage pattern	Prototype/design
Taloba and Rayan (2021)[55]	Data storage/access control	Hybrid on-/off-chain model; scalability	Cryptographic hashes + external storage; access control scheme	Conceptual framework

DIDs/VCs: decentralized identifiers/verifiable credentials; GDPR/ESR: General Data Protection Regulation; EHR: electronic health records; IPFS: Interplanetary File System; JS/Web3.js stack: JavaScript/Web3.js stack; MFA: multifactor authentication; PHR: personal health record; PoA: Proof of Authority; PoS: Proof of Stake; PoW: proof of work.