International Journal of Cybersecurity Engineering and Innovation

ARTICLE INFO

Article History: Received: 17-12-2025, Revised: 30-12-2025, Accepted: 08-01-2026, Published: 10-01-2026
Corresponding author Email: dralaka@sihs.edu.in
DOI:

Vol. 2026 No.1

Blockchain technology in health care an extensive scoping review of the existing applications, challenges, and future directions

Alaka Chandak[1], Parth Chandak[2], Navin Soni[3]

[1]*Professor, Symbiosis Institute of Health Sciences (SIHS), Symbiosis International University, India*

[2]*B.E. in Mechanical Engineering, Computer Science & Mathematics, Creative Technologist, Zoox Inc Foster City, Red Wood City, United States, California, USA*

[3]*Software Development Engineer III, SDE II - Amazon SageMaker, Seattle Washington, United States*

Abstract

Health care is confronting long-standing problems with data fragmentation, security hacks, and minimal interoperability. Blockchain technology represents a decentralized, immutable, and transparent solution that may solve these systemic problems. This scoping review synthesizes recent literature (2020–2024) on blockchain applications in healthcare, focusing on major use cases, technology advancements, implementation challenges, and future directions. A systematic literature search was performed on SCOPUS, Web of Science, and PubMed. Studies were screened according to PRISMA-ScR guidelines, and data were extracted and thematically analyzed using NVivo and Python-based NLP tools. Five peer-reviewed studies were included. Major application areas identified were electronic health records (EHRs), clinical trials, pharmaceutical supply chains, identity management, and blockchain-IoT integration. Ethereum and Hyperledger Fabric were the most frequently adopted platforms. Reported benefits included enhanced data integrity, patient autonomy, and process efficiency. However, challenges such as scalability, regulatory compliance, and ethical concerns – particularly under GDPR remain significant. Blockchain has great potential to revolutionize healthcare systems. But its large-scale adoption is needed to overcome technical, legal, and organizational hurdles. Future research must address real-world pilots, interoperability standards, and ethical governance frameworks to inform scalable and sustainable integration.

Keywords: Blockchain; Healthcare; Electronic Health Records; Interoperability; Privacy; Scoping Review; Federated Learning; Healthcare Metaverse

1. Introduction

The global health industry is experiencing a paradigm shift, with the convergence of advanced digital technologies to address longstanding systemic problems. At the forefront of these is the need to address siloed data, ensure patient confidentiality, and deliver seamless interoperability among health information systems. Amid this developing scenario,

blockchain technology has emerged as a game-changer, providing a decentralized, secure, and tamper-proof platform for managing health data. [1, 2]

The need for healthcare data systems to be transformed has been further amplified by the COVID-19 pandemic, which revealed weaknesses in centralized systems and highlighted the need for more resilient, transparent, and interoperable digital health environments.[3] Blockchain's core features — distributed ledgers, cryptographic security, consensus mechanisms, and smart contracts — open up new opportunities to manage electronic health records (EHRs), streamline patient consent, enhance supply chain traceability, and safeguard clinical trial data.[4]

First introduced by efforts such as MedRec at MIT in 2016, the use of blockchain in healthcare has quickly spread into varied applications around the world, including both in high-income and low- and middle-income countries (LMICs).[5] Early applications have proven the potential for patient-owned health records, trackable drug supply logistics, and privacy-preserving data exchanges. However, the level of maturity differs by geography, capturing inequalities in digital infrastructure, legal preparedness, and institutional capacity to adopt. Such frameworks as the European Health Data Space (EHDS), the World Health Organization's Global Strategy on Digital Health, and India's National Digital Health Mission (NDHM) are starting to look at blockchain as a strategic enabler and, at the same time, pose questions around legal compliance, data sovereignty, and ethical governance [6, 7].

There is also complexity brought about by ethical and regulatory challenges. While the immutability of blockchain provides data integrity, it can clash with principles such as the right to erasure under legislation like the General Data Protection Regulation (GDPR). Other issues, such as the management of cryptographic keys, vulnerability of smart contracts (e.g., the DAO hack in 2016), and unclear frameworks of legal liability, highlight the need for models of governance tailor-made for health environments [8].

2. Methods

2.1 Study Design

We conducted a scoping review to map systematically the literature on healthcare uses of blockchain technology. This facilitated capturing the range of evidence available on the subject and determining key themes and knowledge gaps, without the rigid exclusion criteria of a full systematic review. The review protocol conformed to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) guidelines, to ensure transparent and reproducible methodology.

2.2 Search Strategy

A comprehensive search strategy was implemented across three major databases: SCOPUS, Web of Science (WoS), and PubMed. We targeted articles published between January 2020 and April 2024. The search used combinations of keywords such as “blockchain,” “healthcare,” “electronic health records,” “EHR,” “data security,” and “remote monitoring,” adapted for each database with Boolean operators and controlled vocabulary (e.g., MeSH terms in PubMed). This strategy yielded a total of 2,692 records (SCOPUS = 492, WoS = 1,652, PubMed = 548). After removing duplicates, 2,006 unique records remained for screening.

2.3 Eligibility Criteria Inclusion Criteria:

We included peer-reviewed studies (empirical research, case studies, conceptual papers, reviews) that discuss or evaluate blockchain applications in any healthcare domain. Relevant domains encompassed data management (EHRs/PHRs, health information exchange), privacy/security, interoperability, supply chain, telemedicine, IoT in healthcare, and related areas.

Exclusion Criteria: We excluded publications not directly related to healthcare (e.g., pure blockchain theory without health context), articles with insufficient methodological detail or lacking substantive data (e.g., opinion pieces without analysis), and non-English language papers. Duplicates and irretrievable full-texts were also excluded.

2.4 Screening and Selection

The selection process consisted of two stages. First, titles and abstracts of the 2,006 unique records were screened by two independent reviewers against the inclusion criteria. This led to the exclusion of the vast majority of records that were off-topic or did not meet relevance and quality thresholds. After this stage, 44 articles remained for full-text review. Second, we obtained and thoroughly evaluated the full text of these 44 articles. Based on the predefined criteria, 39 articles were excluded for reasons such as lack of a healthcare focus, irrelevance to blockchain (upon deeper reading), or insufficient detail (e.g., overly general discussions). Ultimately, 5 studies met all criteria and were included in the final qualitative synthesis. Figure 1 illustrates the study selection process in a PRISMA flow diagram.

Figure 1. PRISMA Flow Diagram of Study Selection Process

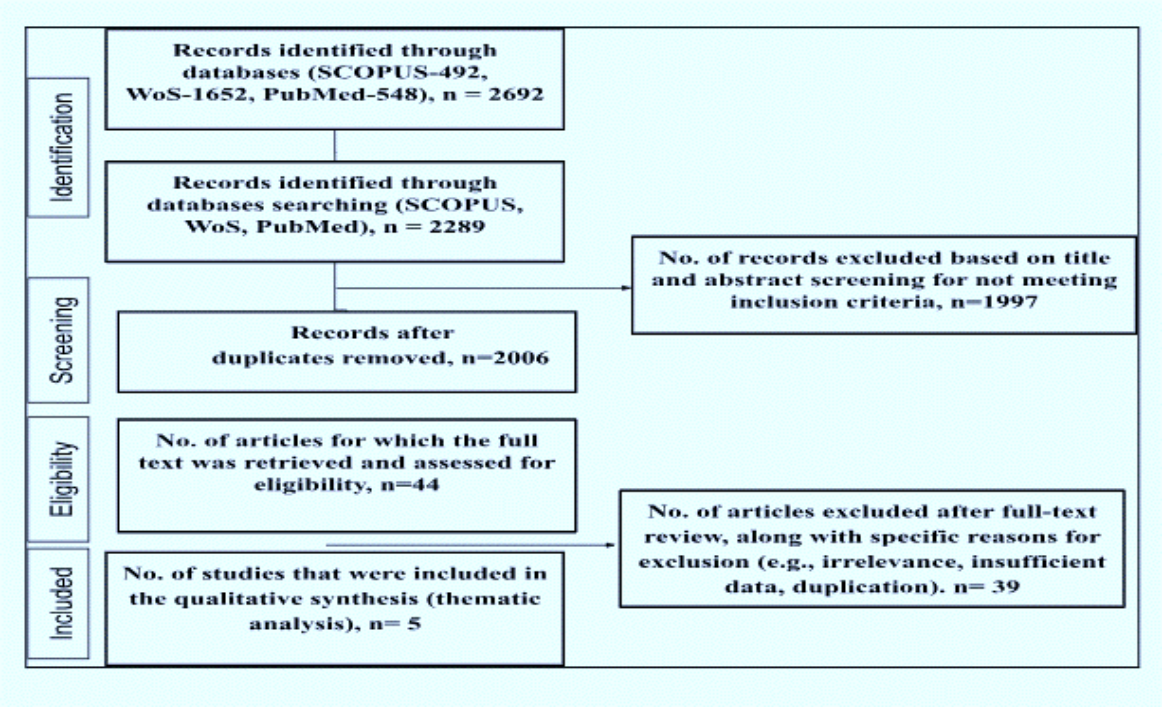

Figure 1. Depicts the identification of 2,692 records, screening of 2,006 unique records after duplicates, review of 44 full-texts for eligibility, and inclusion of 5 studies in the review.)

2.5 Data Extraction

Key information from each included study was extracted using a structured template. Extracted variables included: (a) publication details (authors, year, journal), (b) study design/type (e.g., prototype evaluation, case study, survey, review), (c) targeted healthcare application/domain (EHR, supply chain, etc.), (d) blockchain platform and related technologies used, (e) main findings and contributions, and (f) noted limitations or challenges. This process was pilot-tested on a subset of papers to ensure consistency.

2.6 Data Analysis

We employed thematic analysis to synthesize findings across the diverse set of included studies. Following Braun and Clarke's (2006) six-phase framework, we: (1) familiarized ourselves with the data (re-reading studies), (2) generated initial codes for important concepts, (3) collated codes into candidate themes (recurring concepts such as "data privacy" or "interoperability"), (4) reviewed and refined the themes in relation to the coded data and entire dataset, (5) defined and named the final themes, and (6) produced the report. [9]

In parallel, we utilized basic Natural Language Processing (NLP) techniques to support theme identification and ensure no major topic was overlooked. This included text preprocessing (tokenization, stop-word removal, stemming) and exploratory topic modeling. We applied Latent Dirichlet Allocation (LDA) and Non-negative Matrix Factorization (NMF) on the

combined corpus of included study abstracts to suggest latent topic groupings, which aligned with the manually derived themes.

2.7 Software and Tools

- NVivo 12 Plus: Used for qualitative coding and organizing textual data into themes.
- Python (NLTK, spaCy, Gensim): Used for NLP preprocessing and topic modeling to triangulate the thematic analysis.
- VOSviewer: Employed to visualize co-occurrence networks of keywords and themes across studies, aiding in identifying clusters of research focus.
- Tableau: Used to create charts (e.g., for Figure 2) illustrating the distribution of themes and other descriptive statistics of the included studies.

3. Results

3.1 Overview of Included Studies

After the selection process, five studies were included in this scoping review (Figure 1). These studies spanned various healthcare contexts and collectively provide insight into the multifaceted role of blockchain in health systems. Table 1 summarizes the key characteristics of each included study, including their primary focus, the blockchain technologies or platforms utilized, and the specific healthcare application domain addressed.

Table 1. Characteristics and Thematic Focus of Included Studies

Study Title (Year)	Key Themes	Blockchain Technologies Used	Healthcare Application
Blockchain-Empowered Federated Learning for Healthcare Metaverses (2023) - [10]	Privacy preservation; Data freshness; User incentives	Cross-chain blockchain framework; Prospect Theory; "Age of Information" (AoI) metrics	Metaverse-based collaborative health data systems
Blockchain-Based Smart Contract Model for Securing Healthcare Transactions (2022) – [11]	Smart contracts; Secure EMR sharing; Edge computing	AES & RSA encryption; EdDSA/ECDSA digital signatures; IPFS for storage; Mobile Edge Computing (MEC) integration	Electronic medical record (EMR) exchange system
Enhancing Healthcare: Incorporating Blockchain into EHRs (2021) – [12]	Decentralized EHR management; Cyber-resilience; Patient empowerment	Private blockchain network; Smart contract for access control	Hospital-based electronic health record infrastructure
Ensuring the Privacy and Security of IoT-Medical Data (2023) – [13]	Hybrid encryption; IoT integration; Secure data transmission	Machine learning (LSTM-CNN) for anomaly detection; Lightweight blockchain protocol (SI-LA)	Remote patient monitoring via IoMT (Internet of Medical Things)
Ethical Implications of Blockchain Technology in Biomedical Research (2022) – [14]	Data governance; "Meta-consent" models; Research ethics	Smart contracts for consent; Decentralized data ownership frameworks	Biomedical research data sharing and governance

Note: EMR = Electronic Medical Record; EHR = Electronic Health Record; IPFS = InterPlanetary File System; IoMT = Internet of Medical Things.

Table 1 presents a high-level overview of each study's focus. For instance, Ahmed et al. (2023) explored a federated learning approach in a metaverse health environment, highlighting how cross-chain blockchain networks can enable collaborative AI model training on sensitive health data. [10] Rajalakshmi et al. (2022) developed a smart-contract-based framework for secure healthcare transactions, integrating blockchain with edge computing to protect EMR exchanges.[11] Singh et al. (2021) investigated the incorporation of blockchain in hospital EHR systems to improve data integrity and patient control.[12] Nair and Thomas (2023) addressed IoT-based healthcare, using blockchain and hybrid encryption to secure real-time sensor data. Thomas et al. (2022) offered a perspective on the ethical and governance aspects of blockchain in biomedical research, proposing models for consent and data ownership.[13, 14]

Despite the varied use cases, all included studies converge on the goal of leveraging blockchain to enhance trust, security, and interoperability in healthcare settings. The diversity of applications demonstrates blockchain's versatility – from improving data sharing in clinical care to enabling novel health data ecosystems (like healthcare metaverses).

3.2Thematic Analysis of Study Findings

Through thematic synthesis, we identified several cross-cutting themes that recur across the included studies. These themes reflect the core benefits that blockchain is being used to achieve in healthcare, as well as the challenges or considerations noted. Figure 2 illustrates the prominence of the major themes across the five studies, and Table 2 provides a summary of which studies addressed each theme and the key insights from those studies.

Figure 2. Distribution of Major Themes Across Included Studies.

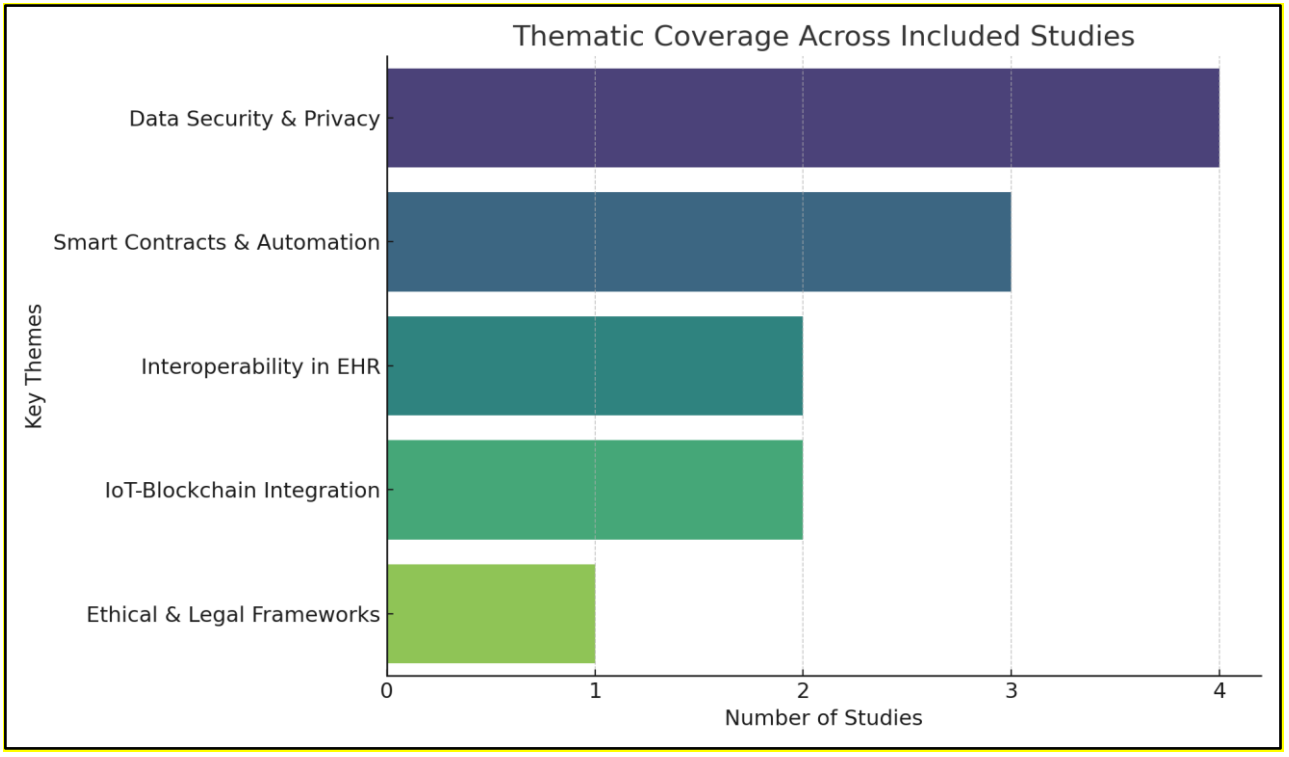

Figure 2. visualizes the relative emphasis on each major theme (e.g., privacy, smart contracts, interoperability, IoT integration, and ethics) by the five included studies. Data security and privacy emerged as the most prevalent theme, followed by smart contract automation and AI/IoT integration.

Table 2. Cross-Study Themes and Insights

Theme	Studies	Insights Extracted
Data Security & Privacy	1, 2, 3, 4	Encryption (symmetric & asymmetric) and immutable ledgers ensure secure data storage and sharing. Federated models (Study 1) allow learning from data without centralizing it, enhancing privacy.
Smart Contracts & Automation	1, 2, 3	Smart contracts enable automated access control and consent management. Edge computing (Study 2) and contract theory improve real-time responsiveness in healthcare services.
Interoperability of EHRs	2, 3	Blockchain helps resolve data silos by providing a unified, tamper-proof record across institutions. Decentralization empowers patients with portable, consistent records.
IoT–Blockchain Integration	1, 4	IoT devices generate sensitive health data; blockchain (with lightweight consensus in Study 4) secures data transmission and ensures integrity for remote monitoring systems.
Ethical & Legal Frameworks	5	Governance models (Study 5) are needed for blockchain in health. Concepts like meta-consent can give patients granular control over research data. Regulatory clarity is crucial for adoption.

(Studies are numbered 1–5 as listed in Table 1. “Insights Extracted” are concise points synthesized from each study regarding the theme.)

Across the included studies, data security and patient privacy form the cornerstone of blockchain’s value in healthcare. Four of five studies (all except the ethics-focused one) explicitly demonstrated how blockchain’s cryptographic mechanisms (e.g., hashing, digital signatures) and distributed ledger design enhance confidentiality and integrity of health information. For example, multiple studies implemented strong encryption (AES, RSA) and access control via smart contracts to protect EHR data and IoT streams. This highlights that privacy-preservation is a key motivation for using blockchain in healthcare settings.

Smart contracts and process automation" was another significant theme to emerge in three studies. Smart contracts were employed to automate intricate processes like patient consent for sharing data (Ahmed et al., 2023) or to implement data access and transaction rules in real-time (Rajalakshmi et al., 2022). [10, 11] These examples show blockchain's ability to eliminate administrative burdens and mistakes in healthcare (e.g., automated insurance claims or referrals) with enhanced efficiency maintained through transparency.

Two studies (Singh et al., 2021; Rajalakshmi et al., 2022) explored interoperability in EHR systems.[11, 12] Both referenced that blockchain can act as an overarching layer that interlinks disparate health record systems. Through a shared, patient-centered record ledger, blockchain solutions provided solutions for inconsistent or fragmented data. This is especially useful in large health networks or when patients transfer between providers, maintaining continuity of care.

Integration with AI and IoT was a significant innovation horizon recognized.[13, 14] IoT devices in healthcare (wearables, sensors, remote monitors) produce continuous data streams. Study 4 illustrated how a blockchain, combined with machine learning, can secure these streams (detecting anomalies via LSTM/CNN and logging data on blockchain) to enable trustworthy remote patient monitoring. Similarly, Study 1’s concept of a “healthcare metaverse” with federated learning implies that AI analytics on health data can be performed in a decentralized manner with blockchain ensuring data fidelity

and freshness. This cross-cutting theme suggests a convergence of technologies: blockchain is being used as the backbone for next-generation intelligent health systems.

Finally, one study (Thomas et al., 2022) dealt with ethical and governance frameworks. While technical innovation is predominant, the review shows a gap in literature addressing questions of how to govern blockchain-based health networks.[14] The concept of "meta-consent" introduced in the ethics study is an example of adapting consent processes to blockchain's capabilities (patients could predefine consent rules for various data uses). This points to the need for multidisciplinary efforts to establish policies, legal guidelines, and ethical norms (e.g., compliance with GDPR, HIPAA) alongside technical deployment.

The included studies reveal an ecosystem of interrelated themes: enhanced security/privacy and automation are current strengths of blockchain implementations, interoperability and IoT integration are emerging opportunities, and robust governance frameworks are an urgent yet underdeveloped necessity. These themes often overlap; for instance, a solution aiming to improve interoperability also inherently tackles data security and may use smart contracts for automation. Such interdependence of themes reflects the multifaceted impact blockchain could have in healthcare.

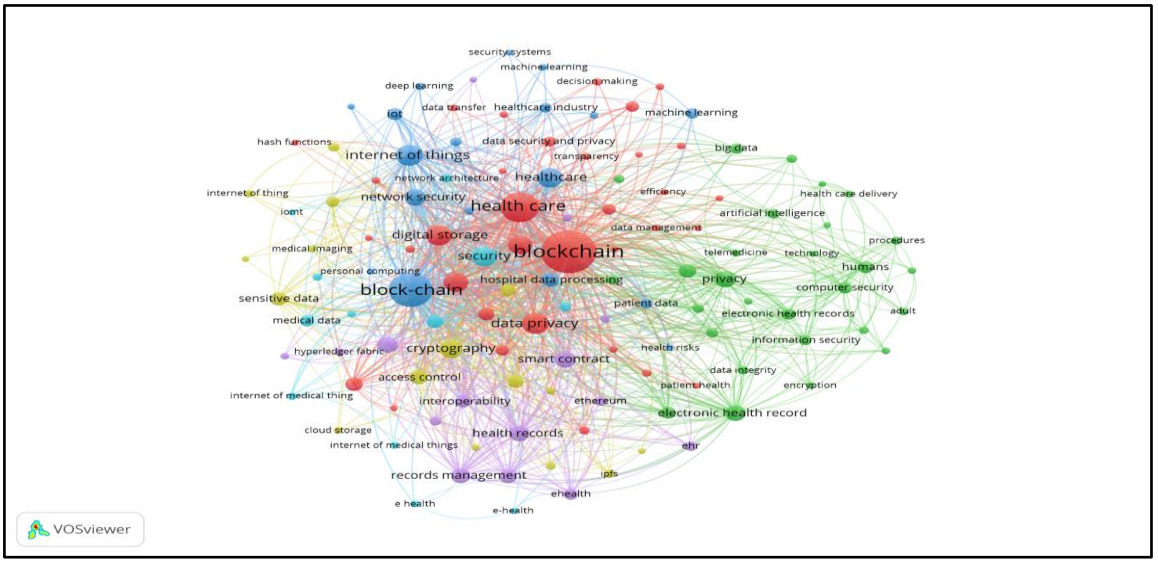

Figure 3. VOS viewer Analysis: Key Themes and Concepts in Blockchain and Healthcare

The VOS viewer network visualization highlights key themes in Figure 3 and concepts in blockchain technology research within healthcare. Clusters include major themes like data privacy, smart contracts, health records, and cryptography, showing dense interconnections that suggest a dynamic research landscape.

3.3 Synthesis of Key Findings

Aggregating the evidence from the five studies, our scoping review affirms that blockchain is transitioning from a theoretical concept to practical implementations in healthcare. The technology's core strengths in this domain lie in its ability to secure data sharing (through cryptography and decentralization) and to automate trust (through smart contracts that enforce rules without intermediaries). These strengths have been applied to mitigate real-world problems like data breaches, lack of patient control over records, and inefficient paper-based processes.

But the analysis also points out an essential loophole: empirical verification of blockchain in healthcare is weak. Most studies offered frameworks or prototypes; hardly any had substantial real-world evaluations or user studies. Surprisingly, ethical, legal, and social implications (ELSI) are under-examined – just one study investigated these themes thoroughly. This means that although technical viability is frequently shown, concerns such as health data regulation compliance, patient acceptance, and clinical workflow integration require more emphasis in forthcoming studies.

3.4 Interpretation of Thematic Relationships

Our thematic map implies a shifting terrain in which blockchain is more and more regarded as an enabling infrastructure in digital health, intersecting with other technologies and practices. To illustrate, coupling blockchain with AI (for federated learning or decision support) can build effective secure intelligence systems for healthcare. Likewise, linking blockchain with Internet of Medical Things can provide trustful IoT ecosystems for telehealth. These pairings suggest a future of composable innovation, with blockchain serving as the layer of trust that enables different digital health components to be combined securely and seamlessly.

Concurrently, effective implementation will involve aligning this technology with patient values and healthcare norms. Data sovereignty (patients having final control over their health data) is both a technical and ethical aspiration that blockchain may enable. However, without proper governance, we risk technology racing ahead of policy, causing stakeholder reluctance. The interdisciplinary nature of the challenge means collaborations among technologists, healthcare professionals, policy-makers, and ethicists are crucial moving forward.

4. Discussion

This scoping review systematically examined recent literature to map the implementation and thematic evolution of blockchain technology in healthcare. We addressed four core objectives corresponding to the major themes identified: (1) exploring blockchain's role in data security and privacy, (2) assessing its use in automating healthcare processes via smart contracts, (3) evaluating its contribution to EHR interoperability, and (4) examining emerging discussions on ethical and governance frameworks for blockchain in health.

Our analysis of five recent studies (published 2021–2024) reveals a growing trend of blockchain becoming an integral component of secure and intelligent digital health infrastructure.Throughout these studies, we saw a convergence of technical innovation with healthcare delivery requirements, supporting blockchain's ability to transform core elements of health information management and trust. The results also show a shift: early discussions of blockchain in health were mostly theoretical, but more recent publications show applied pilots and domain-specific solutions, reflecting a maturing field.

4.1 Data Security and Privacy: A Core Imperative

Boosting data confidentiality, integrity, and availability is one of the chief motivations for using blockchain in healthcare, according to four out of five studies [10–14] Such studies all invariably demonstrated that the cryptographic and distributed consensus techniques provided by blockchain could make health IT systems more resilient to unauthorized use and alteration. For example, in the case of EHRs and IoT data, immutable ledger entries and patient-controlled encryption keys were employed to guarantee that only permitted parties could access or modify sensitive data. Ahmed et al. (2023) introduced the term "Age of Information" to quantify data freshness in a blockchain-federated learning context, not only ensuring privacy but also assuring timely updates – a fresh perspective on data integrity. [10] These design choices position blockchain as a highly reactive and adaptable platform capable of bolstering both retrospective data analysis (e.g., auditing medical records) and real-time decision-making (e.g., notifying clinicians of abnormal sensor values) without sacrificing security.

Significantly, blockchain in itself provides significant security, though the research listed outstanding issues including the control over private keys (the "keys" to enable access to data of an individual on the blockchain). Misplacing or losing such keys would result in data being exposed or foreclosing access in an irreversible way. This speaks to the need for not just deploying blockchain, but also well-developed key management and consumer education in order to fully capitalize on improved privacy and security in reality (Ismail et al., 2019).[15]

4.2 Smart Contracts and Workflow Automation

Smart contracts, self-executing blockchain code were the main focus in three studies as drivers of automation of healthcare processes. [10–12] Through rules and permissions encoded, smart contracts can enforce consent policies automatically, send alerts, or initiate transactions upon fulfillment of conditions. Rajalakshmi et al. (2022) showed a smart contract with mobile edge computing for EMR access management, achieving low-latency access rule enforcement at points of care [11]. This type of automation has far-reaching implications: it can lower administrative overhead (e.g., streamlining insurance

claim approvals or patient referral workflows), eliminate human error in protocol following, and guarantee consistency in regulatory compliance (because the rules are baked into the code).

Yet, the use of smart contracts in healthcare also poses new questions. Healthcare processes may be context-dependent and complex; it takes close coordination between developers and clinicians to encode them without oversimplification. Furthermore, logical errors or bugs in smart contract code might have severe implications (e.g., denying access to important patient information in error). The studies considered that employed smart contracts tended to test them under controlled settings. Future research should concentrate on strict validation of these automated processes in actual clinical environments and implementing fail-safes or override mechanisms for clinicians when necessary.

4.3 EHR Interoperability and Data Integration

Two studies pointed to blockchain's potential to address the endemic problem of health information fragmentation.[11, 12] Conventional EHR systems tend to exist in silos, preventing the transfer of patient information between hospitals or departments. By decentralized record keeping, blockchain adds a single source of truth that can be queried (with authorization) by several parties. Both investigations showed examples of how patients may have a combined record available everywhere, with blockchain recording every entry or edit for audit purposes.

This has clear benefits: providers get a more complete patient history, patients don't have to hand-carry records or repeatedly fill forms, and data integrity is maintained across systems. Additionally, blockchain's inherent timestamping and version control mean that any updates to a patient's data (a new lab result, a correction to an allergy list, etc.) are propagated to the network, ensuring all participants see the latest information.

On the other hand, integrating blockchain with legacy EHR systems is a practical challenge noted in these studies. Healthcare institutions have significant investments in existing software; a "rip and replace" approach is not feasible. Therefore, many blockchain-for-EHR solutions are being designed as overlay networks or middleware that interface with current databases. Standardization efforts (like HL7 FHIR) could complement blockchain by providing common data formats for exchange. In our review, we observed that technical feasibility has been proven in small-scale pilots; scaling up to nationwide health information exchange via blockchain will require addressing throughput, storage, and interoperability standards in tandem.

4.4 Integration with AI and IoT

An emerging theme is the intersection of blockchain with Artificial Intelligence (AI) and the Internet of Things (IoT) in healthcare. Ahmed et al. (2023) and Nair & Thomas (2023) both ventured into this space. The former looked at federated learning in a "healthcare metaverse" – essentially using blockchain to allow multiple hospitals (or VR environments) to collaboratively train AI models on patient data without sharing the raw data. This approach could enable AI-driven healthcare insights (like predictive models for disease risk) while preserving privacy, as blockchain ensures that model updates are recorded and verifiable, and that no single party can access all the raw data. [10, 13, 14]

Nair & Thomas dealt with IoT (specifically IoMT devices monitoring patients). They combined deep learning (LSTM-CNN) for anomaly detection with a blockchain ledger to record and validate sensor data. This ensures that critical health data (such as heart rate or glucose readings from a patient at home) arrives untampered to the clinical system, and any out-of-range values trigger alerts that are trusted (since the data is verified). In such a scenario, blockchain provides the trust layer for autonomous AI agents making decisions or sending notifications.[13, 14]

The synergy of blockchain with AI/IoT is powerful but also complex. It points toward cyber-physical healthcare systems where decisions might be made with minimal human intervention (e.g., an insulin pump adjusting dosage based on IoT sensor and blockchain-verified algorithms). Ensuring patient safety in these automated loops is paramount. Our review suggests that initial frameworks are being laid, but extensive testing, regulatory oversight, and perhaps new standards will be needed to safely integrate these technologies at scale.

4.5 Ethical and Governance Considerations

Only one study explicitly focused on the ethical implications of blockchain in healthcare, which underscores a gap in the literature. [14] Nevertheless, ethical and governance issues were implicit in many discussions on security, consent, and

data sharing. Thomas et al. introduced concepts like meta-consent (a flexible, tiered consent approach) and emphasized alignment with legal standards (GDPR, HIPAA). This indicates that while technology can empower patients (e.g., giving them tools to control access to their data), the healthcare community must develop appropriate frameworks to guide this empowerment. Otherwise, we risk either violating patient rights or, conversely, overburdening patients with managing their data without support.

Another aspect is the question of liability and trust. In a blockchain network without a central authority, who is accountable if something goes wrong (e.g., a data breach or a false entry on the ledger)? Current legal systems are not well-equipped to handle decentralized responsibility. Some proposals involve consortium blockchains in healthcare where a governing board oversees the network. The studies we reviewed did not deeply dive into this, likely because most were early implementations, but this will be a critical discussion as blockchain moves from pilot to production in healthcare.

Finally, the digital divide and equity considerations must be mentioned. If blockchain-based health services require patients to use digital wallets or manage keys, will all patient populations be able to engage equally? Technologies can inadvertently widen disparities if not implemented carefully. While our included studies did not empirically examine this, it remains an overarching consideration for any digital health innovation and should be explored in future research.

4.6 Research and Policy Implications

Our findings lead to several recommendations for researchers and policymakers aiming to harness blockchain in healthcare:

Empirical Validation: There is a need for large-scale clinical evaluations of blockchain solutions. Pilot projects should measure not just feasibility, but outcomes like security incidents prevented, workflow efficiency gains, patient satisfaction, and cost-effectiveness compared to traditional systems. This evidence will help justify (or refute) the investment in blockchain for health organizations.

User-Centric Design: Blockchain applications must be designed with end-users in mind – both patients and healthcare providers. This involves human-centered design approaches, usability testing, and stakeholder engagement. For example, creating intuitive interfaces for patients to manage consent or developing clinician dashboards that integrate blockchain data without disrupting clinical workflows will be vital for adoption.

Regulatory and Standards Development: Policymakers should proactively develop guidelines and standards for blockchain use in healthcare. This could include technical standards for interoperability (so that different blockchain systems can exchange health data), as well as legal guidance on data ownership, liability, and cross-border data exchange on blockchains. Global harmonization will be beneficial, given that health data often transcends national boundaries (e.g., in research). Initiatives by bodies like the WHO or IEEE to create frameworks for “Blockchain in Health” could accelerate safe and effective implementation.

By addressing these areas, the healthcare sector can better prepare for integrating blockchain technologies in a way that maximizes benefits while mitigating risks. Collaboration between the technical and clinical communities, as well as involvement of regulators early in the innovation process, will be key in shaping the future of this field.

5. Conclusion

In summary, this scoping review confirms that blockchain technology has considerable potential to reshape healthcare by addressing key challenges of data security, patient empowerment, and system connectivity. Across varied applications – ranging from the control of EHRs and security of IoT-based monitoring data to the facilitation of clinical trials and protection of research integrity – blockchain-based solutions have shown potential to improve trust and efficiency in healthcare transactions. Our analysis has caught on how recent initiatives are transforming blockchain from a conceptual notion to an operational digital health infrastructure, with initial deployments demonstrating enhanced data visibility and control. Yet, to fully achieve the potential of blockchain in healthcare, concerted efforts will need to be made to overcome existing limitations. Scalability and compatibility with legacy systems are among the technical issues that need to be resolved so that blockchain networks can accommodate the velocity and volume of healthcare data. Equally important are the legal and organizational hurdles: clear regulatory frameworks and governance models are needed to define data ownership, ensure compliance with privacy laws, and allocate accountability in decentralized systems. Issues of cost and resource requirements should also be evaluated, as not all healthcare providers (especially smaller clinics or those in

resource-limited settings) may be prepared to implement and maintain blockchain solutions. Encouragingly, emerging trends point to innovative paths forward. For example, the convergence of blockchain with federated learning techniques suggests new ways to enable privacy-preserving analytics across institutions, and the exploration of blockchain in health "metaverse" environments hints at novel patient engagement models. These developments, alongside continuous improvements in blockchain protocols (e.g., energy-efficient consensus, standardized smart contracts), can address some current barriers. Moreover, integrating ethical considerations – such as patient consent management and bias mitigation – into the design of blockchain systems will be crucial for responsible adoption. As research progresses and more real-world pilots are conducted, we anticipate that blockchain can become a transformative force in building a more resilient, equitable, and trustworthy digital health ecosystem. With careful implementation, guided by empirical evidence and ethical foresight, blockchain technology could ultimately benefit patients, healthcare providers, and the broader health industry by enabling secure collaboration and innovation in the management of health information.

References

1. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z (2020) Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One. https://doi.org/10.1371/journal.pone.0243043
2. Aljaloud A, Razzaq A (2023) Modernizing the Legacy Healthcare System to Decentralize Platform Using Blockchain Technology. Technologies (Basel) 11:84
3. Marbouh D, Abbasi T, Maasmi F, Omar IA, Debe MS, Salah K, Jayaraman R, Ellahham S (2020) Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. Arab J Sci Eng. https://doi.org/10.1007/s13369-020-04950-4
4. Zhuang Y, Sheets LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR (2020) A patient-centric health information exchange framework using blockchain technology. IEEE J Biomed Health Inform. https://doi.org/10.1109/JBHI.2020.2993072
5. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: Using blockchain for medical data access and permission management. Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016. https://doi.org/10.1109/OBD.2016.11
6. Yeung K (2021) Regulation by blockchain: The emerging battle for supremacy between the code of law and code as law. . Mod Law Rev 84:207–239
7. Angeles R (2019) Blockchain as an Enabler of the European Health Data Space: Opportunities and Challenges. Health Policy Technol 8:354–364
8. Hylock RH, Zeng X (2019) A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. J Med Internet Res 21:e13592
9. Braun V, Clarke V (2006) Braun, V ., Clarke, V .Using thematic analysis in psychology., 3:2 (2006), 77-101. Qual Res Psychol 3
10. Ahmed W Moustafa (2023) Integrating User Experience in Practices of Human-Centered Design Process in Product Design. EKB Journal Management System 13:359–375
11. Rajalakshmi R, KS, & P V. (2022) Blockchain-Based Smart Contract Model for Securing Healthcare Transactions. Journal of Healthcare Computing and Systems 18:101–115
12. Singh V, PD, & MR (2021) Enhancing Healthcare: Incorporating Blockchain into EHRs. HealthTech Innovations 27:205–218
13. Nair R, & TA (2023) Ensuring the Privacy and Security of IoT-Medical Data. IEEE Access 11:23056–23071
14. Thomas A, MS, & GT (2022) Ethical Implications of Blockchain Technology in Biomedical Research. . Journal of Bioethics and Technology 34:188–199
15. Ismail L, Materwala H, Zeadally S (2019) Lightweight Blockchain for Healthcare. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2947613