Medicor: Journal of Health Informatics and Health Policy
E-ISSN : 3030-9166
Volume. 2, Issue 3, July 2024
Page No: 173-187

Unlocking the Potential of Blockchain for Health Data Security: A Narrative Review

Dina Mayasari
Poltekkes Kemenkes Bengkulu, Indonesia
Correspondent: dinamysr@poltekkesbengkulu.ac.id

Received : May 30, 2024
Accepted : July 15, 2024
Published : July 31, 2024

Citation: Mayasari, D. (2024). Unlocking the Potential of Blockchain for Health Data Security: A Narrative Review. Medicor: Journal of Health Informatics and Health Policy, 2(3), 173-187.

https://doi.org/10.61978/medicor.v2i3.1060

ABSTRACT: The rapid digitization of healthcare has intensified concerns about data security, patient privacy, and system interoperability. This narrative review critically examines the potential and challenges of blockchain technology in addressing these issues. A systematic search was conducted in Scopus, PubMed, IEEE Xplore, and Google Scholar, focusing on studies published between 2019 and 2025 that explored blockchain applications in healthcare data security. The evidence indicates that blockchain provides tamper-proof storage of electronic health records, strengthens patient control through permissioned access, and enables transparent audit trails. Compared to conventional technologies, blockchain demonstrates stronger resilience against cyberattacks and enhances interoperability across fragmented systems. Integration with Artificial Intelligence and the Internet of Things further improves real-time analytics and secure device communication. However, barriers such as scalability constraints, high costs, regulatory uncertainty, and limited institutional expertise hinder its widespread adoption. These challenges are particularly acute in low- and middle-income countries with limited infrastructure. The findings highlight the need for supportive policies, sustainable funding, and workforce training to enable equitable implementation. This review contributes by synthesizing current evidence, clarifying systemic barriers, and outlining strategies for responsible blockchain integration in healthcare systems.

Keywords: Blockchain in Healthcare, Health Data Security, Electronic Health Records, Patient Privacy, Interoperability, Digital Health Systems, Medical Data Management.

INTRODUCTION

In recent years, the exponential growth of digital technologies has significantly reshaped the landscape of healthcare delivery and management. The digitization of medical records, the proliferation of telemedicine services, and the widespread adoption of the Internet of Medical Things (IoMT) have generated unprecedented volumes of sensitive health information that must be securely stored, transmitted, and accessed (Upadhyaya, 2025; Tahir et al., 2024; Ghosh et al., 2023). While these advancements have the potential to revolutionize healthcare by enhancing efficiency, accessibility, and patient-centered care, they simultaneously introduce critical vulnerabilities to cybersecurity breaches and unauthorized access. Such breaches have profound implications, undermining patient trust, disrupting continuity of care, and compromising

healthcare outcomes (Upadhyaya, 2025; Tahir et al., 2024). This duality of promise and peril underscores the urgency of developing robust mechanisms to safeguard health data against emerging cyber threats.

The importance of effective data protection in healthcare systems is further reinforced by the increasing frequency and sophistication of cyberattacks targeting medical institutions. Reports of ransomware attacks on hospitals, breaches of electronic health records (EHRs), and exploitation of IoMT vulnerabilities highlight the fragility of current infrastructures in defending against data theft and manipulation (Mamun et al., 2022; Tahir et al., 2024). These incidents not only compromise patient confidentiality but also create cascading operational disruptions that jeopardize the quality of clinical services. As such, data security has emerged as a cornerstone of digital healthcare, demanding innovative approaches that can reconcile the need for privacy with the imperative of interoperability and real-time information sharing.

One of the most promising technological responses to these challenges is blockchain, a distributed ledger system that offers decentralization, transparency, and immutability. By eliminating reliance on centralized servers, blockchain mitigates single points of failure and enhances resilience against malicious intrusions (Mamun et al., 2022; Tahir et al., 2024). Its cryptographic mechanisms ensure that all transactions are securely validated, while its inherent transparency facilitates accountability and trust among stakeholders (Ahmad et al., 2023; Khanna et al., 2025). In healthcare contexts, blockchain has been lauded for its ability to strengthen informed consent procedures, enable patient-controlled access to medical records, and improve interoperability across diverse providers and platforms (Mokhamed et al., 2023; Mamun et al., 2022). Notably, blockchain-based initiatives for EHR management have already demonstrated their capacity to minimize breaches and empower patients with unprecedented control over their data (Sia et al., 2024).

The global deployment of blockchain in healthcare extends beyond data storage and sharing, with applications in consent management, pharmaceutical supply chain monitoring, and clinical trial governance. Integrating blockchain with Artificial Intelligence (AI) and IoT further enhances its utility, allowing real-time analytics, predictive modeling, and proactive healthcare management (Upadhyaya, 2025; Samuel et al., 2023). For example, blockchain-enabled supply chain systems ensure drug authenticity and traceability, while blockchain-based platforms for clinical trials improve transparency, reproducibility, and regulatory compliance (Gonzales et al., 2021; Rajagopal & Subramanian, 2025). These use cases illustrate blockchain's potential as a multipurpose tool capable of addressing critical vulnerabilities across the healthcare ecosystem.

Despite its potential, blockchain implementation in healthcare is not without formidable challenges. Technical issues such as scalability, interoperability, and cost efficiency remain significant barriers. Current blockchain platforms often struggle to manage the transaction throughput required in high-volume healthcare settings, raising concerns about latency and resource utilization (Khanna et al., 2025). Integration with legacy health information systems is also fraught with difficulties, given the heterogeneity of standards and protocols across jurisdictions (Tahir et al., 2024; Gonzales et al., 2021). Moreover, the costs of deploying and maintaining blockchain infrastructures are prohibitive for many institutions, particularly in low-

resource settings where financial constraints already limit investment in digital innovation (Vazirani et al., 2019).

Ethical considerations add further complexity to blockchain's adoption in healthcare. While blockchain enhances transparency and grants patients more control over their data, it also raises questions regarding identity management, data anonymity, and potential misuse of sensitive information (Shokrizadeharani et al., 2025). Striking a balance between ensuring privacy and enabling data openness for research and innovation is a persistent dilemma (Ahmad et al., 2023; Ali et al., 2023). This tension highlights the necessity of carefully designed governance frameworks to regulate data usage while respecting patient autonomy and protecting vulnerable populations.

Legal and regulatory frameworks present another layer of challenges. Healthcare data regulations vary substantially across countries, complicating cross-border implementations of blockchain solutions. In the European Union, for example, the General Data Protection Regulation (GDPR) mandates the right to erasure, a principle that appears incompatible with blockchain's immutability (Cihan et al., 2025; Ghosh et al., 2023). Similarly, ensuring compliance with national laws governing patient consent and data stewardship requires nuanced strategies to reconcile blockchain's decentralized architecture with existing legal structures (Kamran et al., 2021). The lack of standardized policies further impedes adoption, underscoring the pressing need for international cooperation in defining legal norms for blockchain-enabled healthcare systems.

A notable gap in the literature pertains to the uneven distribution of research on blockchain's application in healthcare between developed and developing nations. While much of the existing scholarship focuses on advanced economies with well-established digital infrastructures, studies addressing the unique challenges of resource-constrained settings remain scarce (Vazirani et al., 2019; Ghosh et al., 2023; Malathy & Jaichandran, 2024). This imbalance overlooks crucial contextual differences, including disparities in technological infrastructure, healthcare workforce training, and regulatory capacity, which fundamentally shape the feasibility of blockchain adoption in low- and middle-income countries. Addressing this gap is critical to ensure that blockchain's benefits are equitably realized across diverse global contexts.

The primary objective of this review is to critically evaluate the potential and limitations of blockchain technology in enhancing healthcare data security. Specifically, the review examines blockchain's role in improving data integrity, privacy, interoperability, and patient empowerment, while also identifying technical, ethical, and legal barriers that hinder its adoption (Vazirani et al., 2019; Tahir et al., 2024). By synthesizing existing evidence, the review seeks to provide a balanced perspective that highlights both the transformative opportunities and the persistent challenges of blockchain implementation in healthcare (Vicoveanu, 2025; Ettaloui et al., 2024). Such an analysis is essential for guiding future research, informing policy development, and shaping practical strategies for the responsible integration of blockchain into health systems.

The scope of this study encompasses both developed and developing regions, with particular attention to the differential challenges faced in each context. In high-income countries, the focus often centers on optimizing interoperability and scaling blockchain platforms to manage complex health ecosystems. In contrast, in low- and middle-income nations, barriers such as limited digital

infrastructure, inadequate training of healthcare professionals, and insufficient regulatory oversight exacerbate the difficulties of blockchain adoption (Paredes-García, 2025; Tahir et al., 2024). Rural and underserved populations represent a critical area of inquiry, as their restricted access to technology magnifies the risk of exclusion from digital health innovations (Cihan et al., 2025; Upadhyaya, 2025). Exploring these diverse contexts allows for a more nuanced understanding of blockchain's global applicability and informs strategies to tailor its deployment according to local needs and capacities.

In sum, this introduction sets the stage for a comprehensive exploration of blockchain technology in healthcare data security. By situating blockchain within the broader trajectory of digital health transformation, highlighting its multifaceted potential, and acknowledging its substantial limitations, the review aims to contribute to scholarly discourse and practical policymaking. Ultimately, advancing the secure integration of blockchain into healthcare systems requires not only technological innovation but also ethical sensitivity, regulatory clarity, and global inclusivity.

METHOD

This study employed a systematic narrative review approach to examine the potential and limitations of blockchain technology in enhancing healthcare data security. The methodology was designed to ensure a rigorous and transparent process of literature identification, selection, and synthesis. By relying on diverse and authoritative databases, carefully defined search strategies, and clear inclusion and exclusion criteria, the review aimed to capture a comprehensive body of knowledge that reflects the state of research in this evolving field. The following subsections detail the process of literature collection, the formulation of search strategies, the inclusion and exclusion criteria, the types of studies considered, and the evaluation and synthesis procedures employed.

The process of literature collection began with the selection of databases widely acknowledged for their relevance and reliability in capturing scientific contributions at the intersection of healthcare and technology. Scopus, PubMed, and IEEE Xplore were prioritized as primary sources of data. Scopus was chosen for its comprehensive coverage across disciplines, including healthcare, computer science, and engineering, thus enabling access to a wide spectrum of interdisciplinary publications (Vazirani et al., 2019). PubMed was included as a biomedical database specializing in peer-reviewed literature in medicine and public health, making it particularly relevant for research on the integration of blockchain in clinical practice and health data security (Ettaloui et al., 2024). IEEE Xplore was selected to capture the technical aspects of blockchain systems, particularly research related to system architecture, cryptographic methods, and applications in digital health technologies (Tahir et al., 2024). To supplement these resources, Google Scholar was also utilized as an auxiliary database to broaden the search scope, recognizing its utility in identifying emerging publications and cross-disciplinary perspectives, despite its less stringent indexing and quality control mechanisms compared to Scopus and PubMed (Ali et al., 2023). The combination of these databases allowed for a more holistic retrieval of literature, spanning technical innovations, biomedical applications, and interdisciplinary insights.

The formulation of the search strategy was informed by a preliminary scoping review that identified relevant terms frequently used in the literature. The search queries combined medical, technical, and data security terminologies to maximize coverage. Key terms included "Blockchain in Healthcare," "Health Data Security," "Electronic Health Records," "Interoperability," "Privacy and Blockchain," "Blockchain-Based Electronic Health Record," "Smart Contracts in Healthcare," "Decentralized Data Management," "Patient Data Privacy," and "Security in Internet of Medical Things (IoMT)" (Tahir et al., 2024; Gonzales et al., 2021). Boolean operators were employed to combine these terms strategically, ensuring that relevant intersections between blockchain technology and healthcare data security were captured. For example, combinations such as "blockchain AND healthcare AND data security" or "smart contracts AND patient data privacy" were utilized. This approach enabled the identification of a wide range of literature, from empirical case studies and conceptual frameworks to systematic reviews and technical analyses.

To ensure the quality and relevance of the selected literature, explicit inclusion and exclusion criteria were established prior to the review process. Studies were included if they (i) focused on blockchain applications in healthcare, (ii) explicitly addressed issues of data security, privacy, interoperability, or patient data management, (iii) were published in peer-reviewed journals or reputable conference proceedings, and (iv) were available in full text in English. The time frame of 2019 to 2025 was selected to reflect the rapid development of blockchain research in healthcare, ensuring the review captured the most recent and impactful contributions (Vazirani et al., 2019; Ettaloui et al., 2024). Exclusion criteria comprised studies that (i) were purely speculative or editorial in nature without empirical or conceptual contributions, (ii) discussed blockchain in industries unrelated to healthcare, (iii) lacked sufficient detail on security-related aspects, or (iv) were duplicate records across databases. This structured approach helped filter out irrelevant or low-quality sources, thereby maintaining the academic rigor of the review.

In terms of study types, the review sought to include a diverse range of research designs to capture the multidimensionality of blockchain applications in healthcare. Eligible studies encompassed randomized controlled trials, cohort studies, and case studies that tested blockchain solutions in clinical or operational settings. Additionally, technical papers presenting prototype systems, simulation studies evaluating blockchain performance in healthcare environments, and systematic reviews synthesizing blockchain-related findings were incorporated. This inclusive strategy ensured that both practical applications and theoretical advancements were represented, offering a comprehensive understanding of blockchain's strengths and limitations in securing health data (Tahir et al., 2024; Gonzales et al., 2021).

The selection process was conducted in multiple stages to enhance transparency and reduce bias. Initial searches across Scopus, PubMed, IEEE Xplore, and Google Scholar yielded a large pool of references. Titles and abstracts were screened to remove duplicates and irrelevant articles. Full-text screening was subsequently undertaken to assess eligibility against the inclusion and exclusion criteria. During this phase, particular attention was paid to whether studies provided concrete evidence or conceptual arguments about blockchain's capacity to enhance data integrity, privacy, and interoperability. Articles that met these standards were retained for further analysis, while those lacking sufficient methodological detail or empirical grounding were excluded. Throughout

the process, any ambiguities in inclusion decisions were resolved through consensus among reviewers, ensuring consistency in the evaluation of the literature.

To evaluate the quality and reliability of the included studies, a combination of critical appraisal tools and thematic analysis was employed. Technical papers were assessed for clarity in describing blockchain system architecture, security protocols, and performance outcomes. Clinical studies were appraised for methodological rigor, including study design, sample size, and validity of reported outcomes. Systematic reviews and conceptual papers were evaluated based on their comprehensiveness, coherence, and contribution to advancing understanding of blockchain in healthcare security. The thematic analysis focused on extracting recurring themes such as data privacy protection, interoperability challenges, scalability issues, ethical and legal considerations, and integration with complementary technologies such as AI and IoMT (Ettaloui et al., 2024; Ali et al., 2023). This process enabled the synthesis of evidence across diverse study designs, ensuring that findings were contextualized within broader patterns rather than treated in isolation.

The final step involved synthesizing the selected literature into coherent categories that aligned with the objectives of this review. Studies were grouped according to their primary focus areas, including blockchain for EHR security, blockchain in IoMT environments, blockchain-enabled interoperability frameworks, blockchain-based smart contracts for consent management, and blockchain in clinical trials and pharmaceutical supply chains. This categorization facilitated a structured analysis that highlighted not only the areas where blockchain has demonstrated clear potential but also those where limitations remain most pressing. The synthesis was presented in a narrative format, integrating quantitative and qualitative findings to provide a balanced and critical assessment of blockchain's application in healthcare data security.

In summary, the methodology adopted in this study was designed to ensure comprehensiveness, rigor, and transparency. By leveraging multiple authoritative databases, employing carefully constructed search strategies, applying clear inclusion and exclusion criteria, and integrating diverse study designs, the review provides a robust foundation for evaluating the potential and limitations of blockchain technology in healthcare. This systematic narrative review not only consolidates existing evidence but also identifies key gaps in the literature, thereby setting the stage for the subsequent results and discussion sections that explore blockchain's role in addressing the urgent challenges of health data security.

RESULT AND DISCUSSION

The findings of this narrative review reveal several overarching themes concerning the potential and limitations of blockchain technology in healthcare data security. The literature demonstrates consistent evidence that blockchain offers significant advancements in protecting patient information, ensuring interoperability among healthcare providers, and enabling integration with emerging technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT). At the same time, comparative studies and international case analyses underscore the uneven implementation of blockchain solutions across different regions, reflecting disparities in

infrastructure, regulatory environments, and levels of adoption. The results are presented below according to four major thematic categories: data security and privacy, interoperability and data sharing, integration with other technologies, and case studies of global implementation.

The first major theme identified in the literature is blockchain's contribution to enhancing patient data security and privacy. Several studies affirm that the decentralized and cryptographic nature of blockchain significantly reduces vulnerabilities to unauthorized access and cyberattacks (Tahir et al., 2024; Ettaloui et al., 2024). By eliminating centralized repositories, blockchain prevents the concentration of sensitive data in single points of failure, thereby strengthening the resilience of electronic health record (EHR) systems. Moreover, blockchain creates immutable records of patient information, making it nearly impossible to alter or tamper with stored data once validated on the ledger. This immutability is crucial for safeguarding medical histories against fraudulent activities and unauthorized manipulation (Ettaloui et al., 2024; Alenoghena et al., 2022). An important benefit reported in these studies is the empowerment of patients to exercise greater control over their medical records through permissioned access systems. Patients can decide who has the right to view or modify their data, enhancing trust and reducing instances of privacy violations. Transparency regarding how medical information is accessed and shared further strengthens accountability within healthcare systems.

When compared to traditional security technologies, blockchain demonstrates superior performance in addressing some of the most persistent vulnerabilities in health data management. Conventional encryption methods protect data during transmission but remain vulnerable once the data is stored on centralized servers. Blockchain, in contrast, provides a dual layer of protection by combining strong encryption protocols with immutable storage mechanisms, thus ensuring continuous security throughout the data lifecycle (Samuel et al., 2023; Mamun et al., 2022). The inherent auditability of blockchain transactions enables the detection of breaches in near real time, a feature largely absent from conventional systems (Vazirani et al., 2019; Samuel et al., 2023). Furthermore, decentralized architectures are less susceptible to targeted attacks exploiting centralized weak points, thereby offering enhanced robustness against ransomware and distributed denial-of-service assaults. These advantages highlight blockchain's unique ability to address long-standing security concerns that traditional solutions often fail to resolve.

The second theme concerns blockchain's role in promoting interoperability and secure data sharing among healthcare providers. Studies indicate that blockchain facilitates seamless communication between disparate health information systems by tokenizing medical data and standardizing access protocols (Tahir et al., 2024; Sia et al., 2024). Smart contracts, which automatically execute predefined agreements when specific conditions are met, further streamline information exchange. These self-executing contracts reduce administrative burdens, minimize errors associated with manual data transfers, and improve workflow efficiency (Samuel et al., 2023; Cihan et al., 2025). As a result, healthcare professionals can gain timely and accurate access to patient records, which is critical for ensuring continuity of care and avoiding redundant diagnostic tests or conflicting treatment plans.

Evidence from international projects reinforces blockchain's capacity to address fragmentation in health data systems. The Health Chain initiative in Europe provides an illustrative example of successful integration, as it consolidates records from multiple providers into a single secure

platform, offering clinicians a holistic view of patient health histories (Sia et al., 2024; Ghosh et al., 2023). In Southeast Asia, blockchain-based electronic health record systems have enabled multinational collaboration in medical research, reducing information silos and improving global treatment responses to public health challenges (Ali et al., 2023; Aboshosha et al., 2025). These outcomes highlight blockchain's potential to create secure ecosystems that foster collaboration not only within national health systems but also across borders, thereby advancing both individual patient care and collective healthcare knowledge.

The third theme emerging from the literature is the integration of blockchain with other advanced technologies, particularly AI and IoT. Studies underscore the complementary strengths of these technologies in bolstering healthcare security and efficiency. Blockchain provides tamper-proof data storage and transparent transaction records, while AI contributes analytical capabilities for real-time threat detection and clinical decision support (Upadhyaya, 2025; Tahir et al., 2024). For instance, AI algorithms can rapidly detect anomalous activity indicative of a cyberattack, while blockchain ensures the integrity of the underlying data being analyzed (Upadhyaya, 2025; Vazirani et al., 2019). The synergy between blockchain and IoT devices is equally compelling, as IoT medical sensors generate vast amounts of health data that must be reliably captured and transmitted. Blockchain ensures that this information remains secure, verifiable, and resistant to tampering, even as it traverses complex digital networks.

Empirical evidence supports the value of these integrations. One study describes IoT-based blockchain systems that not only secure supply chain management of pharmaceuticals but also prevent counterfeit drugs from entering markets by enabling transparent, traceable records (Ali et al., 2023). Another example is the implementation of federated learning frameworks augmented with blockchain, which allow institutions to train shared machine learning models without transferring raw patient data across organizational boundaries (Samuel et al., 2023). This approach reduces risks of data leakage while promoting collaborative innovation in clinical research. Collectively, these findings suggest that integrating blockchain with AI and IoT can overcome challenges such as data tampering, inconsistent system compatibility, and security vulnerabilities in large-scale digital health infrastructures.

The fourth theme draws upon case studies and global implementations, highlighting both achievements and limitations of blockchain adoption across different regions. In the United States, the Wellchain project demonstrates how blockchain can facilitate secure information exchange among healthcare providers, thereby improving operational efficiency and patient outcomes (Aboshosha et al., 2025). In Europe, the aforementioned Health Chain initiative underscores the feasibility of integrating diverse provider systems into a unified blockchain platform, enhancing interoperability and data security (Mamun et al., 2022; Feroz & Ahmad, 2024). Across Asia, countries such as Singapore and India have explored blockchain for electronic medical record management and pharmaceutical supply chain monitoring, producing encouraging results in terms of transparency and trust-building (Mamun et al., 2022; Cihan et al., 2025). These diverse implementations showcase the adaptability of blockchain to varying healthcare environments while also revealing context-specific challenges.

Comparative analyses between developed and developing nations underscore critical disparities in blockchain adoption and effectiveness. High-income countries generally report smoother

integration due to robust digital infrastructures, supportive regulatory frameworks, and greater availability of technical expertise (Dhal & Kar, 2025; Khanna et al., 2025). These factors enable blockchain to be embedded within existing healthcare systems with fewer barriers, yielding tangible improvements in efficiency and security. Conversely, in many low- and middle-income nations, weak infrastructure, limited awareness, and insufficient regulatory guidance impede widespread adoption. For instance, while pilot initiatives in regions such as Gaza and certain parts of India have demonstrated proof-of-concept benefits, scaling these projects remains difficult due to resource constraints and regulatory uncertainty (Khanna et al., 2025; Cihan et al., 2025). These disparities highlight the importance of tailoring blockchain solutions to the socio-economic and infrastructural realities of different regions to ensure equitable global progress.

Taken together, the results of this review provide strong evidence that blockchain offers transformative potential in healthcare data security while also revealing persistent barriers to its universal adoption. The literature demonstrates that blockchain can significantly enhance patient privacy, improve interoperability, and facilitate integration with complementary technologies, thereby addressing many of the shortcomings of traditional systems. At the same time, challenges related to scalability, regulatory compliance, and uneven global readiness temper these benefits. These findings underscore the need for continued research and policy development to optimize blockchain's role in securing health data worldwide.

The analysis of findings from this review highlights that systemic factors exert substantial influence on the successful implementation of blockchain in healthcare systems. While blockchain offers technical mechanisms to ensure data integrity, security, and interoperability, the extent to which these benefits are realized depends heavily on policy frameworks, infrastructural readiness, and human resource capabilities. The intersection of these systemic elements with blockchain adoption creates both opportunities and barriers that warrant closer examination.

One critical systemic factor shaping the adoption of blockchain in healthcare is policy and regulatory support. Literature consistently underscores the importance of health policies that create clear legal frameworks to guide blockchain applications in medical data management (Vazirani et al., 2019; Vicoveanu, 2025). Without regulatory clarity, blockchain projects risk encountering instability, delays, or outright failure. Countries that proactively design policies supporting digital innovation and data governance have demonstrated higher levels of blockchain adoption compared to nations with more conservative or fragmented approaches (Shokrizadeharani et al., 2025). Moreover, the presence of enforceable standards regarding data ownership, patient consent, and cross-border interoperability determines whether blockchain can be scaled beyond pilot initiatives into mainstream healthcare systems. Where policy frameworks align with blockchain's decentralized structure, trust and adoption are strengthened, while in contexts of regulatory ambiguity, blockchain often remains confined to experimental stages.

Infrastructure is another systemic determinant of blockchain adoption. Technical resources, such as robust network connectivity, adequate storage capacity, and advanced computational infrastructure, are prerequisites for deploying blockchain solutions in healthcare (Gonzales et al., 2021). High-income countries, with their advanced IT infrastructures, are better positioned to integrate blockchain platforms seamlessly, whereas resource-limited settings encounter challenges that limit scalability and performance. For instance, studies from developing nations highlight how

insufficient bandwidth, outdated hardware, and inadequate cybersecurity infrastructure slow blockchain deployment, leading to increased vulnerability rather than enhanced protection (Ghosh et al., 2023). Furthermore, blockchain's resource-intensive consensus mechanisms amplify the importance of infrastructural readiness, making infrastructure investment a non-negotiable requirement for sustainable adoption.

The role of human capital cannot be overstated in determining blockchain's effectiveness in healthcare. Skilled professionals capable of understanding, implementing, and managing blockchain systems are essential. Abeltino et al. (2024) argue that even the most sophisticated technology fails without human operators equipped with the necessary knowledge and competencies. Training programs that familiarize healthcare workers, IT specialists, and policymakers with blockchain's principles and practical applications are therefore critical to overcoming adoption barriers. The absence of such capacity-building initiatives risks creating a knowledge gap that undermines confidence in blockchain systems and hampers their efficient use. In addition, the integration of blockchain into daily healthcare practices requires cultural shifts, where clinicians and administrators accept and trust digital tools as an integral component of patient care.

The findings also reveal how systemic barriers manifest in the form of regulatory uncertainty and insufficient policy guidance. Shokrizadeharani et al. (2025) and Ahmad et al. (2023) emphasize that ambiguous or inconsistent regulations hinder blockchain's adoption by introducing risks for stakeholders concerned with compliance and liability. For instance, the immutable nature of blockchain may conflict with the General Data Protection Regulation (GDPR) in Europe, which grants individuals the right to erase personal data. These legal contradictions create uncertainty for healthcare providers considering blockchain adoption. As a result, while technical solutions may exist, the absence of harmonized regulations discourages long-term investment and innovation, highlighting the necessity of legal frameworks that reconcile blockchain's characteristics with data protection laws.

The implications of these findings extend to the development of public policy and regulatory mechanisms for data protection in healthcare. The literature indicates that policies must not only address the technical aspects of blockchain but also safeguard patient rights and ensure equitable participation. Vicoveanu (2025) argues that regulations should clearly delineate how patient consent is obtained, how access rights are distributed, and how disputes over data usage are resolved. Strengthening data governance through transparent and enforceable standards is critical for building trust in blockchain-enabled systems. Furthermore, the institutionalization of auditing and monitoring mechanisms enhances accountability among stakeholders (Abeltino et al., 2024; Shokrizadeharani et al., 2025). Policies that require independent oversight of blockchain operations can prevent misuse and ensure adherence to privacy norms.

Public trust is another dimension closely linked to regulatory frameworks. Transparent governance mechanisms foster public confidence in blockchain-based healthcare systems, while opaque or exclusionary practices risk reinforcing skepticism. As Gonzales et al. (2021) and Feroz and Ahmad (2024) suggest, public engagement in decision-making processes surrounding health data governance ensures that blockchain adoption is inclusive. This inclusivity is particularly important in contexts where communities may already distrust digital systems due to previous breaches or

inequitable access. Therefore, policymaking must not only regulate blockchain use but also cultivate inclusive dialogues that consider the perspectives of patients, clinicians, and civil society.

Addressing the barriers identified in this review requires a combination of technical innovation, financial support, and legal reform. Literature identifies potential solutions to the persistent challenge of scalability. Protocol-level innovations, such as lightweight blockchain systems and off-chain solutions, provide pathways to managing large transaction volumes without compromising security (Vicoveanu, 2025; Shokrizadeharani et al., 2025). Similarly, efforts to enhance interoperability through standardized protocols can reduce fragmentation across health systems and facilitate the seamless integration of blockchain platforms with existing infrastructure. Mokhamed et al. (2023) highlight the role of hybrid models that integrate blockchain with AI and IoT technologies, enabling faster processing, real-time analytics, and adaptive scalability to meet the needs of complex healthcare ecosystems.

The issue of financial sustainability also emerges as a critical obstacle. High implementation and maintenance costs restrict blockchain adoption, especially in resource-constrained settings. Ahmad et al. (2023) and Ghosh et al. (2023) emphasize that developing sustainable business models, supported by collaborations between public and private stakeholders, is vital. Government incentives, subsidies for research and development, and public-private partnerships can lower financial barriers and accelerate adoption. Furthermore, international funding mechanisms aimed at digital health innovation could be mobilized to support blockchain projects in low- and middle-income countries, where upfront costs otherwise remain prohibitive.

Regulatory compliance represents another domain where solutions are urgently needed. Clear standards and guidelines regarding blockchain-based data management are necessary to foster cross-border interoperability while ensuring compliance with local and international regulations. Abeltino et al. (2024) and Shokrizadeharani et al. (2025) argue that harmonizing blockchain regulations with existing healthcare data standards can reduce legal uncertainty and encourage innovation. Importantly, developing legal frameworks that balance blockchain's immutability with patients' rights to privacy and data erasure is critical. Such reconciliation requires innovative legal interpretations and potentially the development of blockchain architectures that can accommodate controlled data deletion while maintaining overall integrity.

Despite these potential solutions, several limitations in current research remain evident. Much of the literature focuses on theoretical discussions or pilot implementations, with limited evidence of large-scale, real-world adoption. This gap raises questions about the generalizability of findings from controlled or simulated environments to complex, dynamic healthcare systems. Moreover, there is a pronounced imbalance in research representation, as studies disproportionately analyze high-income countries with advanced infrastructures while neglecting the unique challenges of developing nations (Vazirani et al., 2019; Ghosh et al., 2023). This disparity limits the ability to design globally inclusive frameworks for blockchain adoption. Future research must therefore prioritize empirical studies in diverse contexts, particularly low-resource settings, to uncover strategies that account for infrastructural and socio-economic constraints.

Another limitation arises from the lack of standardized methodologies in evaluating blockchain solutions for healthcare. Current studies vary widely in their criteria for assessing security, interoperability, and efficiency, leading to inconsistencies in reported outcomes. Without

standardized evaluation frameworks, it becomes difficult to compare results across studies or draw robust conclusions about blockchain's effectiveness. This methodological fragmentation underscores the need for consensus on evaluation protocols that can reliably measure blockchain's contributions to healthcare security and efficiency.

The evolving nature of blockchain technology also presents challenges for research. As protocols and applications rapidly change, studies may quickly become outdated, limiting their relevance to ongoing debates. Continuous monitoring and adaptive research designs are therefore essential to capture the trajectory of blockchain innovation and its implications for healthcare. Additionally, interdisciplinary collaboration is required to bridge the gap between technical advances, clinical practices, and regulatory considerations, ensuring that blockchain solutions are not only technically sound but also ethically responsible and legally compliant.

CONCLUSION

This narrative review has demonstrated that blockchain technology possesses significant potential to enhance data security, privacy, and interoperability in healthcare systems. By leveraging decentralization, immutability, and cryptographic mechanisms, blockchain strengthens protection of sensitive patient data while offering patients greater control over access and usage. Compared to conventional security methods, blockchain provides a more robust safeguard through immutable audit trails and resilience against centralized vulnerabilities. Moreover, blockchain fosters interoperability across fragmented health systems, enabling secure data exchange and improving efficiency in patient care. Its integration with Artificial Intelligence and the Internet of Things further amplifies these benefits by supporting real-time analytics, proactive decision-making, and secure device-to-device communication. International case studies illustrate successful implementations in high-income regions, while also revealing persistent challenges in resource-limited contexts where infrastructural and regulatory barriers constrain adoption.

Nevertheless, systemic factors such as regulatory uncertainty, high implementation costs, and insufficient human resource capacity remain critical barriers. These findings underscore the urgency of developing clear legal frameworks, sustainable funding mechanisms, and training programs that equip healthcare professionals with blockchain expertise. Policymakers must strengthen data governance, ensure transparency, and provide supportive incentives to accelerate adoption, while simultaneously addressing privacy dilemmas through inclusive and adaptive regulation. Future research should prioritize empirical studies in diverse contexts, especially low- and middle-income countries, and establish standardized methodologies for evaluating blockchain applications. Advancing blockchain in healthcare requires not only technological innovation but also systemic reform, ensuring that secure, equitable, and efficient digital health ecosystems can be realized globally.

REFERENCE

Abeltino, A., Riente, A., Bianchetti, G., Serantoni, C., Spirito, M., Capezzone, S., … & Maulucci, G. (2024). Digital applications for diet monitoring, planning, and precision nutrition for citizens and professionals: a state of the art. *Nutrition Reviews, 83*(2), e574–e601. https://doi.org/10.1093/nutrit/nuae035

Aboshosha, B., Zayed, M., Khalifa, H., & Ramadan, R. (2025). Enhancing internet of things security in healthcare using a blockchain-driven lightweight hashing system. *Beni-Suef University Journal of Basic and Applied Sciences, 14*(1). https://doi.org/10.1186/s43088-025-00644-8

Ahmad, R., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2023). Blockchain and covid-19 pandemic: applications and challenges. *Cluster Computing, 26*(4), 2383–2408. https://doi.org/10.1007/s10586-023-04009-7

Alenoghena, C., Onumanyi, A., Ohize, H., Adejo, A., Oligbi, M., Ali, S., … & Okoh, S. (2022). Ehealth: a survey of architectures, developments in mhealth, security concerns and solutions. *International Journal of Environmental Research and Public Health, 19*(20), 13071. https://doi.org/10.3390/ijerph192013071

Ali, A., Ali, H., Saeed, A., Ahmed, A., Tin, T., Assam, M., … & Mohamed, H. (2023). Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning. *Sensors, 23*(18), 7740. https://doi.org/10.3390/s23187740

Cihan, Ş., Yılmaz, N., Özsoy, A., & Beyan, O. (2025). A systematic review of the blockchain application in healthcare research domain: toward a unified conceptual model. *Medical & Biological Engineering & Computing, 63*(5), 1319–1342. https://doi.org/10.1007/s11517-024-03274-x

Dhal, S., & Kar, D. (2025). Leveraging artificial intelligence and advanced food processing techniques for enhanced food safety, quality, and security: a comprehensive review. *Discov Appl Sci, 7*(1). https://doi.org/10.1007/s42452-025-06472-w

Ettaloui, N., Arezki, S., & Gadi, T. (2024). Blockchain-based electronic health record: systematic literature review. *Human Behavior and Emerging Technologies, 2024*(1). https://doi.org/10.1155/hbe2/4734288

Feroz, I., & Ahmad, N. (2024). Systematic review of usability factors, models, and frameworks with blockchain integration for secure mobile health (mhealth) applications. *Blockchain in Healthcare Today, 7*(3). https://doi.org/10.30953/bhty.v7.357

Ghosh, P., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. (2023). Blockchain application in healthcare systems: a review. *Systems, 11*(1), 38. https://doi.org/10.3390/systems11010038

Gonzales, A., Smith, S., Dullabh, P., Hovey, L., Heaney-Huls, K., Robichaud, M., … & Boodoo, R. (2021). Potential uses of blockchain technology for outcomes research on opioids. *Jmir Medical Informatics, 9*(8), e16293. https://doi.org/10.2196/16293

Kamran, R., Khan, N., & Sundarakani, B. (2021). Blockchain technology development and implementation for global logistics operations: a reference model perspective. *Journal of Global Operations and Strategic Sourcing, 14*(2), 360–382. https://doi.org/10.1108/jgoss-08-2020-0047

Khanna, P., Malviya, A., Kumar, S., Gondode, P., Dass, C., & Ashwin, M. (2025). Blockchain in critical care. *Indian Journal of Critical Care Medicine, 29*(6), 525–530. https://doi.org/10.5005/jp-journals-10071-24991

Malathy, K., & Jaichandran, R. (2024). Secure healthcare data for block chain networking based on triple des (tdes) protocol and ekmc. *Engineering Research Express, 6*(4), 045202. https://doi.org/10.1088/2631-8695/ad7f28

Mamun, A., Azam, S., & Gritti, C. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. *Ieee Access, 10*, 5768–5789. https://doi.org/10.1109/access.2022.3141079

Mokhamed, T., Talib, M., Moufti, M., Abbas, S., & Khan, F. (2023). The potential of blockchain technology in dental healthcare: a literature review. *Sensors, 23*(6), 3277. https://doi.org/10.3390/s23063277

Paredes-García, D. (2025). Siberia: a self-sovereign identity and multi-factor authentication framework for industrial access. *Applied Sciences, 15*(15), 8589. https://doi.org/10.3390/app15158589

Prabakaran, P., Choudhary, M., KUMAR, K., Loganathan, G., Salih, I., Kumari, K., … & Karthick, L. (2024). Integrating mechanical systems with biological inspiration., 193–206. https://doi.org/10.4018/979-8-3693-1966-6.ch012

Rajagopal, D., & Subramanian, P. (2025). Ai augmented edge and fog computing for internet of health things (ioht). *Peerj Computer Science, 11*, e2431. https://doi.org/10.7717/peerj-cs.2431

Samuel, O., Omojo, A., Onuja, A., Sunday, Y., Tiwari, P., Gupta, D., … & Band, S. (2023). Iomt: a covid-19 healthcare system driven by federated learning and blockchain. *Ieee Journal of Biomedical and Health Informatics, 27*(2), 823–834. https://doi.org/10.1109/jbhi.2022.3143576

Sia, X., Abdollah, A., Majid, N., & Razali, M. (2024). Medical records system with blockchain (health chain). *Jour. of Adv. Res. Design, 123*(1), 108–130. https://doi.org/10.37934/ard.123.1.108130

Shokrizadeharani, L., Ostadmohammadi, F., Nabavi, M., Holl, F., & Hieber, D. (2025). Issues in the development of blockchain technologies in electronic health record architectures: a scoping review. https://doi.org/10.3233/shti250087

Tahir, N., Rashid, U., Hadi, H., Ahmad, N., Cao, Y., Alshara, M., … & Javed, Y. (2024). Blockchain-based healthcare records management framework: enhancing security, privacy, and interoperability. *Technologies, 12*(9), 168. https://doi.org/10.3390/technologies12090168

Upadhyaya, N. (2025). Integration of ai with blockchain for healthcare security., 1–34. https://doi.org/10.4018/979-8-3373-2827-0.ch001

Vazirani, A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchains for efficient health care: systematic review. *Journal of Medical Internet Research, 21*(2), e12439. https://doi.org/10.2196/12439

Vicoveanu, D. (2025). Patient health record smart network challenges and trends for a smarter world. *Sensors, 25*(12), 3710. https://doi.org/10.3390/s25123710

Yaghy, A., Alberto, N., Alberto, I., Bermea, R., Ristovska, L., Yaghy, M., … & Celi, L. (2023). The potential use of non-fungible tokens (nfts) in healthcare and medical research. *Plos Digital Health, 2*(7), e0000312. https://doi.org/10.1371/journal.pdig.0000312