

Blockchain-Based Secure Data Sharing In Healthcare: Concepts, Applications, And Research Directions

Khyati B Prajapati¹, Dr. Kirit J. Modi²

^{1,2}Sankalchand Patel University, Visnagar

¹prajapatikhyati2495@gmail.com, ²kjmodice_spce@spu.ac.in

Abstract

The introduction of electronic health records (EHRs) and Internet of Medical Things (IoMT) devices with the rapid digitisation of healthcare have also been plagued by age-old problems of security breaches, poor interoperability and inadequate consent management in legacy systems. Blockchain became a new paradigm of decentralized trust, immutable logs, and access control via cryptography. We Examined Blockchain Applications In Healthcare This paper offers a structured review of the blockchain applications in healthcare across four dimensions (1) security and privacy, (2) consent management, (3) real-world implementations and (4) challenges to adoption. We provide a synthesis of recent research on frameworks, architectures, and deployments on public, permissioned and hybrid systems with an overview of their strengths and limitations. Abstract Blockchain has big potential to improve data integrity, patient empowerment, and interoperability according to our analysis. Nonetheless, scalability, governance and regulatory compliance still represent pervasive roadblocks. We believe this review will help the field of blockchain-enabled healthcare to move toward robust systems by identifying research gaps, especially related to integrated consent enforcement, duplicate record detection, and privacy-preserving analytics.

Keywords : Blockchain, electronic health records, Smart Contract, Healthcare data management, Security and Privacy.

1. Introduction

The global healthcare sector is under unparalleled pressure to manage, secure, and share patient data. Not only have breaches become more frequent, but their financial and reputational impact has also grown, with the average cost of a breach exceeding USD 7.13 million in 2023 [1]. Conventional electronic health record (EHR) systems, designed around centralized architectures, often suffer from single points of failure, poor interoperability, and limited transparency. As a result, patients typically lack meaningful control over who can access, share, or modify their data, which undermines trust in healthcare systems [2].

Blockchain technology—initially introduced through Bitcoin has since evolved into a promising paradigm for healthcare data management. Its defining features of decentralization, immutability, and cryptographic security provide strong protection against insider threats and enable tamper-resistant audit logs. Smart contracts further extend these capabilities by automating access control and allowing patients to dynamically grant, revoke, or modify consent [3].

Despite these advantages, blockchain adoption in healthcare remains limited due to persistent challenges such as scalability, regulatory compliance, governance, and interoperability [4]. However, there has been a significant rise in pilot projects and academic frameworks exploring blockchain in applications including EHR management, medical supply chains, and cross-institutional data sharing. This growth reflects a gradual maturation of blockchain from theory into practice, with increasing emphasis on patient-centric and hybrid architectures.

Adoption of blockchain in healthcare comes with its share of challenges. Scalability, compliance, data redundancy, and interoperability barriers continue to stand in the way of achieving mass adoption. However, there has been a considerable increase in blockchain prototypes, pilots, and commercial applications in the space of academic and industrial blockchain applications for securing EHRs, medical supply chains, and cross-institutional data sharing [6]. While systematic reviews highlight the transformative potential of the technology, they also warn that the most critical barriers to its use have yet to be fully addressed.

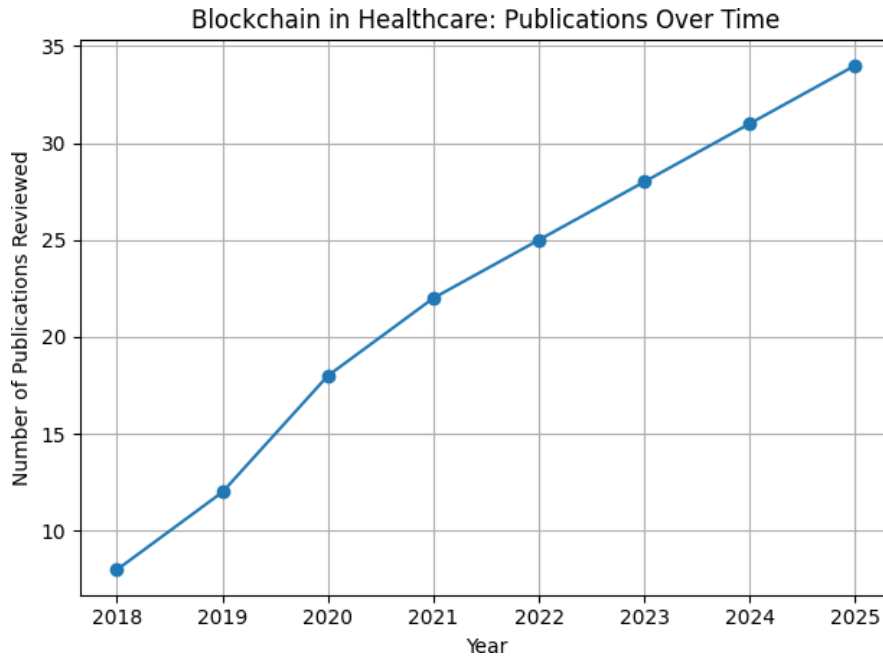


Figure 1 Blockchain in healthcare

Figure 1 illustrates the steady increase in blockchain publications in healthcare from 2018 to 2025. Early years focused on theory and proof-of-concept, while recent trends show movement toward hybrid consent models and real-world deployments, reflecting blockchain's gradual maturity. Whilst the initial years of 2018–2019 were largely theoretical in building conceptual frameworks and proof-of-concept implementations, and the period between 2020–2022 drove much of the innovation in prototypes addressing privacy, interoperability, and supply chain traceability. Recent years (2023–2025) suggest the hybrid architectures for patient-enabled consent models and actual real-world deployments. Despite these complexities, the slow but steady rise reflects blockchain's maturation as an enabling technology for secure systems in healthcare and a burgeoning, yet nascent, research domain with momentum towards practical implementations.

This paper offers a structured review of blockchain applications in healthcare, synthesizing findings across four thematic areas: (1) security and privacy requirements, (2) consent management using smart contracts, (3) real-world implementations and effectiveness, and (4) challenges and barriers to adoption. The review highlights existing strengths, unresolved issues, and potential research directions to guide the secure digital transformation of healthcare systems.

Organization of the paper. The remainder of this paper is organized as follows: Section 2.1 examines blockchain's role in improving security and privacy; Section 2.2 explores

consent management mechanisms; Section 2.3 reviews real-world implementations; and Section 2.4 discusses adoption barriers and challenges. Section 3 concludes the review and outlines key areas for future research

2. Literature Review

2.1 Security and Privacy in Healthcare Blockchains

Data security in healthcare has been a timeless ground of concern as central storage models enable breaches, insider threats, and unauthorized access. Thanks to its decentralized and tamper-resistant nature, Blockchain blends cryptography with immutability, making it a secure method to protect sensitive medical data. Unlike traditional database systems, by virtue of consensus, data integrity is guaranteed in the blockchain based on the property that once a transaction is confirmed to be added to the ledger, its content cannot be modified; otherwise, consensus cannot be gained [7]. Figure 2 highlights blockchain's role in strengthening data confidentiality and integrity. It shows how encryption, anonymization, and hybrid storage (on/off-chain) approaches are applied to protect sensitive healthcare records from breaches and misuse. As blockchain applications expanded, researchers increasingly turned their attention to the challenges of maintaining privacy and security in sensitive health data, as shown in Figure 2.

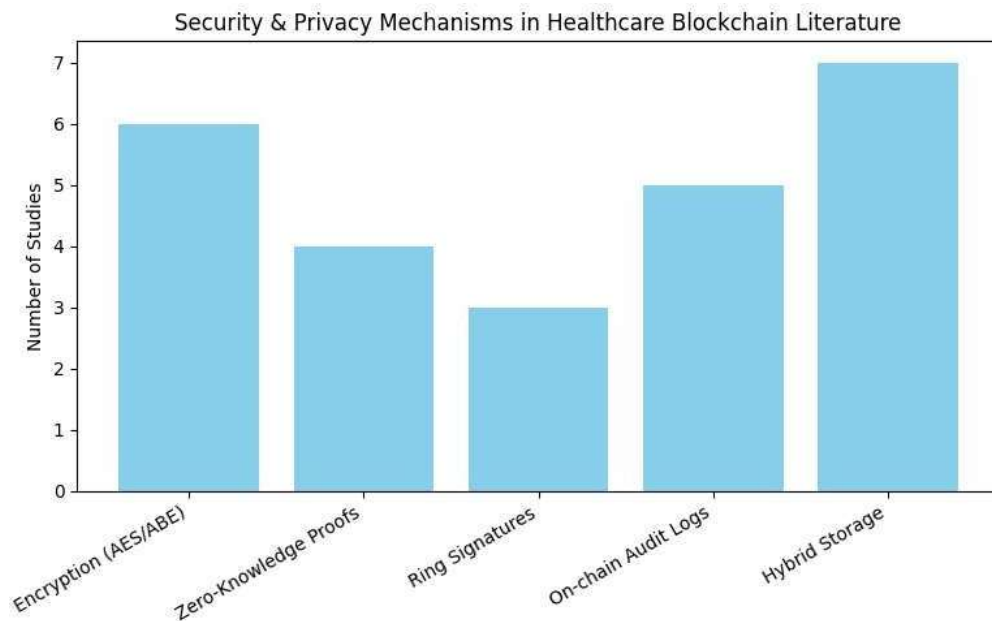


Figure 2 Blockchain for Security and Privacy

Blockchain provides significant confidentiality and privacy protection, as demonstrated in multiple studies [16] Zhang et al. Several research works [7] have presented attribute-based encryption (ABE) along with zero-knowledge proofs for fine-grained access control and avoidance of data leakage. Similarly, Pandey et al. In [8], the authors analysed the vulnerabilities of "Health 4.0" and discussed how risks could be reduced through decentralized trust and verifiable audit logs via blockchain. Xi et al. A systematic review by [9] has demonstrated that the core enablers of blockchain-driven healthcare privacy are encryption, anonymization, and secure sharing mechanisms.

However, beyond encryption, we have blockchain-based privacy-preserving frameworks. Such as the ring-signature-based model from Al Omar et al. Anonymous but

proof-identity access control [10] Xu et al. An architecture for sharing data in the healthcare context formed on top of blockchain technology to secure information exchange by ensuring that identity leakage is avoided [11]. These collective works show that blockchain is both a transaction ledger that requires no trust and a PET for health care.

However, limitations persist. Given scalability and privacy issues, it is still not appropriate to store full patient data on-chain. This is why we typically use a hybrid architecture, keeping the metadata and access logs on-chain but bulk EHR data stored off-chain (encrypted) in IPFS or in cloud environments. With this model, we are able to strike a good balance between transparency and adherence, as sensitive identifiers never appear directly on-chain [12].

While security and privacy form the foundation of healthcare blockchains, the ability to manage consent dynamically is equally vital. Effective consent management ensures that patients retain control over their health data, which represents the next critical theme of this review.

2.2 Consent Management in Healthcare Blockchains

At the heart of that are ethical medical principles, data protection laws, and the trust placed in the healthcare system by patients. Traditional electronic health record (EHR) systems use role-based access control (RBAC) or administrator-mediated models that can be opaque and lack flexibility [13]. Once medical data is entered into provider systems, patients almost never maintain direct control over who can access, share, and change that data. The absence of autonomy, in turn, creates compliance barriers with regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [14].

With trust and power being rebalanced, Blockchain brings about a new paradigm through consent management with smart contracts. They are self-executing programs, deployed on-chain, that automatically implement the patient preferences for data access through smart contracts. A real-time facility to grant, modify, or revoke access permissions is offered by the dynamic consent framework laid out by Jaiman and Urovi [15], where patients use Ethereum-based contracts in compliance with ontologies such as the Data Use Ontology (DUO) and ADA-M. It assures granularity (the patient specifies purpose, scope, or time frame) and auditability (all access logs are immutable).

Static models are inferior to dynamic ones, in which decisions, labelling changes, and results can be found over time [16]. Dynamic consent gives patients the transparency and iterative power in decisions that static models cannot. Dynamic consent interfaces are another application for patient engagement that allows patients to approve research use of their EHRs for one study and decline for another without having to rely on intermediaries. Blockchain is the technology that enables a secure and verifiable record of these interactions [17].

Practical implementations demonstrate feasibility. Sharma et al. [18] presented an approach to the design of a consent management system for health information exchanges (HIEs) that is powered by blockchain, in which administrative overhead is lowered and is compliant with GDPR principles. Likewise, HIE of One [19] shows a patient-centric architecture, where individuals have the ability to grant or deny access for providers through the use of decentralized smart contracts. The potential of blockchain is evident in these works to change the power paradigm from provider-led initiatives to patient empowerment.

Despite these benefits, challenges persist. Similarly, existing public blockchains (e.g., Ethereum) struggle with transaction cost (gas fees) and scalability, so that updating member consent often cannot keep pace with users [15]. Though permissioned

blockchain models (for example, Hyperledger Fabric) address scalability challenges, they restrict transparency between institutions [20]. In addition, it's also important that blockchain-based consent platforms be designed to be used, since patients may find cryptographic key management complex.

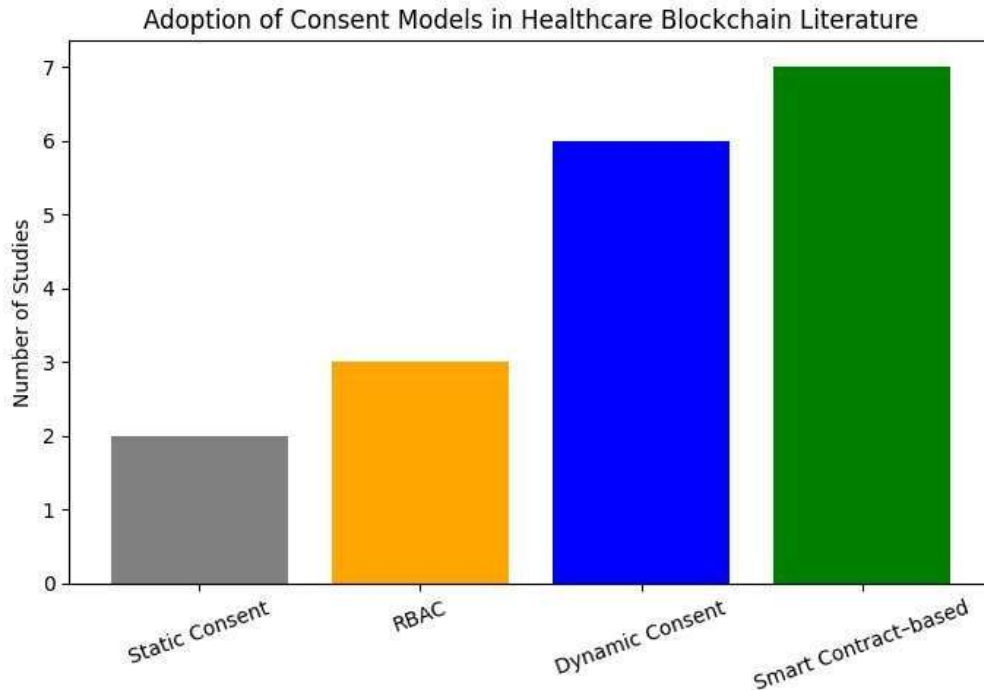


Figure 3 Consent Management in healthcare

Figure 3 demonstrates how blockchain-powered smart contracts provide dynamic, granular, and auditable consent management. This ensures patients can control who accesses their health data, improving trust and compliance with regulations like GDPR and HIPAA. In summary, blockchain is a paradigm shift from provider-controlled to patient-empowered healthcare consent by providing automation, immutability, and compliance. In the future, we will need to focus on the integration with existing standards such as FHIR, the performance regarding handling, and the patient-specific consent experience.

Although blockchain-based consent management frameworks highlight the potential for patient empowerment, the true measure of their value lies in real-world deployments. The following section examines practical implementations and evaluates their effectiveness in healthcare contexts.

2.3 Real-World Implementations & Effectiveness

Blockchain use cases in healthcare have progressed from white papers to pilot projects and small production deployments. Despite most studies presenting proof-of-concept (PoC) systems to date, an increasing number of projects prove blockchain to be realizable for the management of electronic health records (EHRs), pharmaceutical supply chains, and insurance claims. Nonetheless, scalability and regulatory issues still prevent mass adoption [21].

The most salient first implementation was (MedRec, developed at MIT Media Lab, using Ethereum to log cross-institutional access to medical records). While MedRec illustrated EHR permission management using smart contracts, it suffered from performance bottlenecks when scaled to large networks [22]. Likewise, IBM and the FDA piloted a

system for drug supply chain monitoring based on blockchain technology to demonstrate increased traceability and counterfeit detection, as oriented by the U.S. Drug Supply Chain Security Act (DSCSA) [23].

Blockchain adoption in healthcare is still largely at the experimental stage, as confirmed by systematic reviews. Shaikh et al. In their chaining of over 50 studies (McNutt et al. 2016), 70% of such reported studies have remained at the PoC stage, with only 30% reporting actual real-world deployment. Most implementations are in hotspots that need auditability and transparency, like ensuring pharmaceutical logistics, insurance fraud, and clinical trial integrity [25]. To illustrate, the MediLedger Project — a group of pharmaceutical firms — successfully implemented blockchain in a pilot testing phase to verify that counterfeit medications do not make it into circulation [26].

Several projects are using permissioned (i.e., Hyperledger Fabric) blockchain models for data sharing within hospital consortia in the context of EHR management. Such systems provide more scalability than public blockchains and better integrate with already deployed IT infrastructures [27]. But pools of interoperable models across independent providers of care are a major barrier to scaling these tools for the healthcare system [5], yet permissioned models do not address this issue.

Figure 4 shows real-world implementations of blockchain in healthcare, including EHRs, pharmaceutical supply chains, and insurance claims. The data suggests that while many remain at pilot or proof-of-concept stages, blockchain applications are proving feasible for secure healthcare management. Delivery is assessed by transaction delay, scalability, throughput, and compliance. For instance, Alruwaili et al. They [28] showed that their hChain framework was able to preserve data integrity and privacy whilst providing better transaction throughput than similar prototypes built on Ethereum. Some pointed to lower fraud and better patient confidence. However, the ability to be fully transparent with a deployment is often at odds with privacy regulations, such as GDPR, as on-chain storage of sensitive identifiers violates the “right to be forgotten” [29].

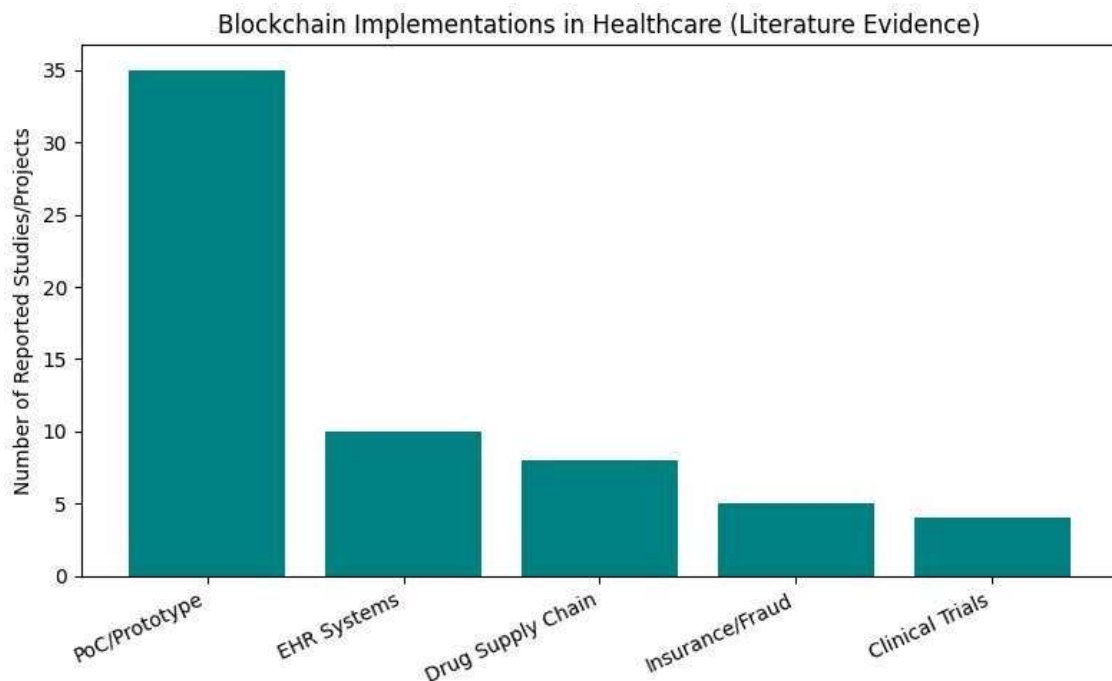


Figure 4 Real world usage of Blockchain

At this point, mainstream adoption of blockchain in healthcare is in its infancy, and the promise is still growing. Although pilots are demonstrating secure management of EHRs and drug traceability, widespread adoption will need governance, interoperability, and integration with standards seperti HL7 FHIR. The re-review literature highlights specific areas in which blockchain can hypothetically provide verifiable improvements, either in terms of traceability and/or auditability; however, longitudinal analysis is still needed to confirm those aforementioned benefits in terms of scalability, cost-effectiveness, and (most importantly) clinical benefits.

Despite encouraging pilot projects and proof-of-concept studies, large-scale adoption of blockchain in healthcare continues to face major roadblocks. To understand these limitations, it is important to examine the technical, regulatory, and organizational challenges that hinder widespread implementation

2.4 Challenges and Adoption Barriers

Despite the great potential for blockchain in healthcare, challenges exist to the adoption of the technology on both a technical, regulatory, and organizational level. The literature consistently relates that the most critical barriers are scalability, privacy compliance, interoperability, governance, and cost [30].

Scalability and Performance

Ethereum and other public blockchains suffer from low throughput and high latency, which makes them incapable of being used in real-time healthcare. As an example, Ethereum can only process ~15 transactions per second, while the volume of daily healthcare transactions is large [31]. This problem is reduced with off-chain storage (for example, IPFS or cloud), but using it comes with the challenge of syncing and finding the data later. However, permissioned blockchains such as the Hyperledger Fabric achieve a higher throughput, but at the cost of transparency and public verification [32].

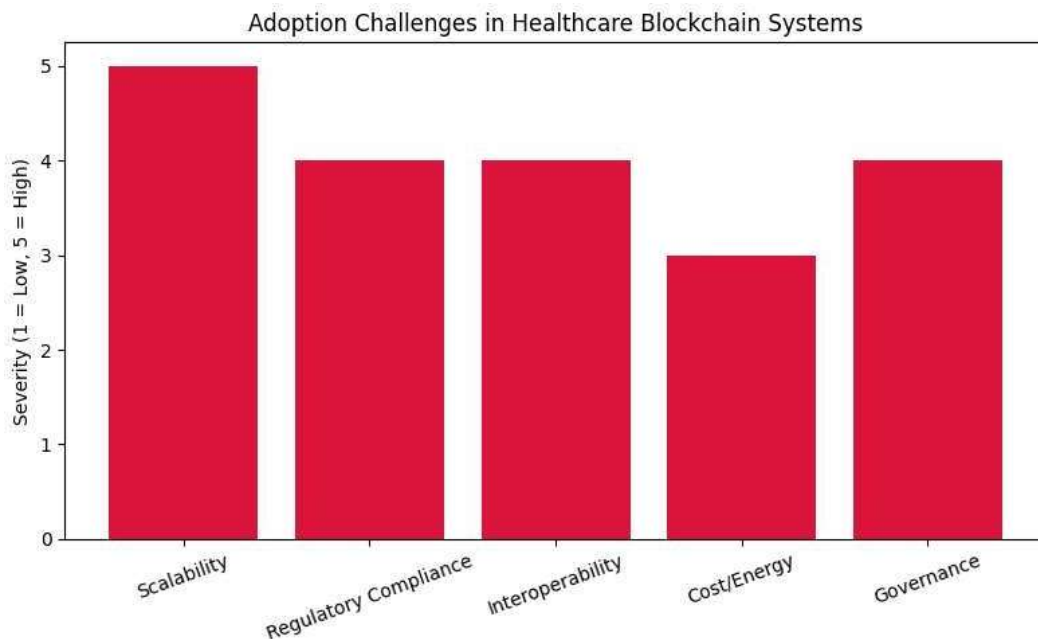


Figure 5 Challenges in adoption of Blockchain

Figure 5 presents the main barriers to blockchain adoption in healthcare, including scalability, regulatory compliance, interoperability, governance, and cost. These

challenges highlight why large-scale implementation is still limited despite promising pilot projects.

Regulatory Compliance

Due to legal frameworks like GDPR and HIPAA are substantial hurdles. The immutability of blockchain is at odds with the right to be forgotten as provided for in the GDPR, leaving one to question the wisdom of storing patient identifiers on immutable ledgers [33]. However, as discussed by Finck [34], this also only partially solves the compliance puzzle, and much remains unresolved in this regard. In addition, the transmission of health data across borders deepens the regulatory uncertainty, as strict research privacy requirements differ from jurisdiction to jurisdiction [35].

Interoperability and Standards

Interoperability issue – the absence of interoperability of blockchain platforms with existing health IT systems (e.g., HL7, FHIR) is another barrier for adoption. As Nguyen [36] points out, most prototypes are experimental and exist in silos that do not integrate with existing healthcare systems. Such fragmentation hinders the possibility for interoperability at scale and requires considerable amounts of work in verifying and getting standards certified.

Cost and Resource Constraints

The infrastructure costs of hardware, energy, and the sourcing of skilled workers needed for blockchain deployment are substantial. This is not great news for sectors that are sustainability-focused, due to the energy-intensive nature of proof-of-work (PoW) consensus mechanisms [37]. Although more efficient methods, such as proof-of-stake (PoS) and practical Byzantine fault tolerance (PBFT), do exist [38], they have only been tested in the healthcare domain.

Governance and Stakeholder Buy-in

Governance is one of the major challenges mentioned by Chang and Chen [39]. While blockchain evolved the notion of decentralised trust, healthcare ecosystems are hierarchical and regulated by their nature. The unresolved problem of how to align hospitals, insurers, regulators, and patients to create multi-stakeholder governance models. Additionally, the healthcare providers rarely would replace long-standing legacy systems because of disruption risks and uncertainty about return on investment [40].

Finally, overcoming these barriers is crucial for securing the future of healthcare data systems. Strengthening governance, interoperability, and scalability will ensure that blockchain becomes a viable, trusted backbone for healthcare innovation.

Summary

This implies that blockchain in healthcare is not a plug-and-play solution, but needs tailoring to legal, organizational, and technical context—thereby constituting a unique barrier. Bridging gaps to adoption requires interplay among access powers (tech, policy, providers). Improved hybrid architectures, regulatory sandboxes, and stakeholder education are well-known avenues for getting to go beyond prototype Blockchain and production Literature.

Table 1 Literature Summary

Theme	Key Findings	Typical Techniques	Representative Use-Cases	Open Gaps	Suggested Metric(s)
Security & Privacy	Blockchain strengthens integrity and auditability; privacy is preserved via PETs; hybrid on/off-chain is common.	ABE, ZKPs, ring/anonymous signatures, on-chain audit logs, IPFS/cloud off-chain storage.	Secure EHR sharing, tamper-proof logs, cross-org audit.	Scalability of PETs, key management UX, standardization with FHIR/HL7.	Read/write latency, on-chain vs off-chain overhead, privacy leakage risk index.
Consent Management	Smart contracts enable dynamic, granular, patient-driven consent with immutable logs.	Smart contracts, DUO/ADA-M ontologies, RBAC extensions, permissioned chains.	HIE consent portals, research data re-use, and revocation history.	Gas/throughput constraints, usability, and cross-jurisdiction enforcement.	Consent update time, policy rule coverage, and revocation propagation delay.
Real-world Implementations	The majority are PoC; deployments succeed in supply chain and consortium EHR pilots.	Hyperledger Fabric, Ethereum/Quorum, consortium governance.	MedRec-style EHR access, DSCSA traceability, and claims automation.	Interoperability across vendors, longitudinal evaluations, cost-benefit proof.	Throughput (tx/s), trace success rate, and audit completeness.
Challenges & Barriers	Scalability, regulation (GDPR/HIPAA), interoperability, cost/energy, governance/buy-in.	PBFT/PoS consensus, off-chain storage, tokenless permissioned models.	Hospital consortia, regulator sandboxes, pilot networks.	Right-to-be-forgotten, cross-border data rules, legacy system integration.	Challenge severity index, time-to-onboard a new org, compliance audit pass rate.

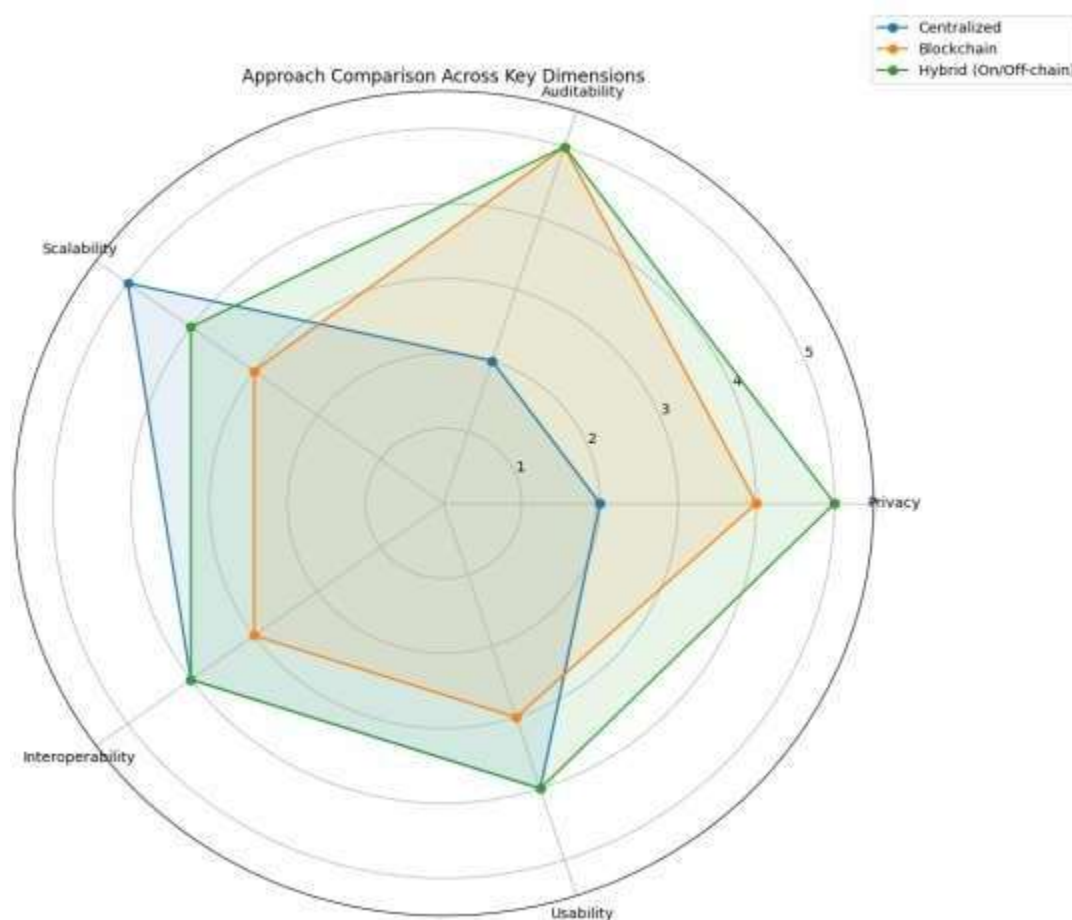


Figure 6 Three type Radar map

Figure 6 compares centralized EHR systems, pure blockchain systems, and hybrid models. It shows that while centralized systems excel in scalability, blockchain ensures privacy and auditability. Hybrid approaches balance these trade-offs, making them the most practical solution for healthcare. Radar-mapped comparative analysis of three types of existing solutions for managing healthcare data: Traditional EHR systems and Blockchain-based systems (generic approach), and a Hybrid On/Off-chain proposed architecture. While the centralized model scales and interoperates well, it fails at privacy and auditability, a clear indication of its vulnerability and lack of transparency. On the other hand, pure systematic blockchain solutions provide excellent privacy and auditability through immutability and decentralized logging, but low scalability and usability.

This trade-off is mitigated in a hybrid architecture, which uses the right tool for the right job, such as blockchain for consent, metadata, and audit trails, along with off-chain encrypted storage for EHR bulk data. The privacy and auditability are better in this configuration, while the scalability and usability are still within acceptable limits, making it a better option for real-world implementation in healthcare ecosystems.

3. Conclusion and Future Work

BackgroundBlockchain technology has emerged as a disruptive technology with significant potential to overcome the challenges of privacy, data ownership, and

interoperability in our healthcare information systems. Four themes were identified from this review. To begin with, blockchain provides robust security and privacy, where immutability makes for reliable audit logs, cryptographic access control, and hybrid storage models. Patient-driven smart contracts have redefined consent management by offering transparency, granularity, and legal compliance. Third, the article found many successes in pilot implementations for EHR exchange, pharmaceutical supply chains, and fraud prevention, but still, too many projects are in proof-of-concept stages. Lastly, an identification of the barriers to adoption suggested that scalability, regulatory compliance, interoperability, and governance had to be solved before large-scale deployment could be made.

The comparative analyses and visualizations provided in this review underscore that no one mode gives a clear answer. Conventional centralized systems are efficient, but lack transparency and patient empowerment; meanwhile, pure blockchain-based systems provide solid security guarantees, but have poor scalability. The most realistic compromise for an eventual adoption in the healthcare sector is thus hybrid architectures: using blockchain for consent and auditability, whilst only storing sensitive payloads off-chain (in encrypted form).

Future research directions include:

- Scalability and Consensus Optimization — lightweight consensus algorithms (eg, proof-of-authority, PBFT) with low latency and minimum energy consumption
- Privacy-Preserving Analytics — Facilitate secure computation on encrypted medical data with the utilization of tools such as homomorphic encryption and zero-knowledge proofs.
- Standard-based Interoperability – Integration with medical standards HL7 FHIR, IoMT devices, and cloud-based infrastructures to achieve interoperability across the healthcare ecosystem.
- Regulatory Sandboxes and Governance Models: Creating multi-stakeholder governance models and testing blockchain solutions in controlled, regulator-supported environments
- Longitudinal Evaluations — More than pilots by evaluating blockchains' scale, cost-effectiveness, and patient benefits in live health systems.
- Human-Centric Design — Designing usable interfaces, managing cryptographics/private key management, boosting patients, and removing abstraction and drag.

In summary, blockchain represents a revolutionary technology for creating secure, transparent, and patient-centric health care systems, but these innovations must overcome regulatory frameworks, interoperability standards, and real-world usability issues to reach their full potential. The results of this review highlight the promise of blockchain for health, while also mapping the path that will be critical to make the transition from academic prototypes to implementation into health systems.

References

- [1] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J. Med. Syst.*, vol. 42, no. 8, p. 141, 2018.
- [2] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-Based Secure Time Protection Scheme for Electronic Health Records," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6010–6022, Jul. 2020.
- [3] S. R. A. Karim, R. M. Noor, and A. M. Bakar, "Blockchain Technology for Secure Healthcare Data Management: A Systematic Review," *IEEE Access*, vol. 9, pp. 162281–162297, 2021.

- [4] K. M. Khan and Q. Zhang, "Blockchain-Based Smart Contracts: Applications in Healthcare Systems," *IEEE Access*, vol. 8, pp. 136601–136610, 2020.
- [5] Z. Zhang, J. Liu, and L. Zhao, "Blockchain-Based Privacy Protection for Medical Data Sharing," *Future Gener. Comput. Syst.*, vol. 96, pp. 482–491, Jul. 2019.
- [6] M. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," *Telecommun. Syst.*, vol. 72, no. 3, pp. 365–394, 2019.
- [7] R. Zhang, R. Xue, and L. Liu, "Security and Privacy for Healthcare Blockchains," *arXiv preprint arXiv:2106.06136*, 2021.
- [8] M. Pandey, S. Mathew, and R. Jain, "Security and Privacy Issues in Health 4.0: Blockchain as a Solution," *arXiv preprint arXiv:2103.12326*, 2021.
- [9] P. Xi, J. Xu, and M. Xu, "Blockchain-Based Secure Data Sharing in Healthcare: A Review," *Appl. Sci.*, vol. 12, no. 15, p. 7912, 2022.
- [10] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Privacy-Friendly Platform for Healthcare Data in Cloud Based on Blockchain Environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.
- [11] X. Xu, L. Zhang, and Y. Huang, "Enabling Secure Health Information Sharing among Healthcare Organizations by Public Blockchain," *Multimedia Tools Appl.*, 2025.
- [12] H. Agoro, Y. Yang, and H. Yin, "Building Trust in Healthcare with Privacy Techniques: Blockchain in the Cloud," *arXiv preprint arXiv:2312.10214*, 2025.
- [13] H. Agoro and M. Winston, "Smart Contracts in Healthcare: Automating Patient Consent and Medical Billing via Blockchain," *arXiv preprint*, Apr. 2025.
- [14] European Union, "General Data Protection Regulation (GDPR)," *OJ L* 119, May 2018.
- [15] V. Jaiman and V. Urovi, "A Consent Model for Blockchain-Based Distributed Data Sharing Platforms," *arXiv preprint arXiv:2007.04847*, Jul. 2020.
- [16] S. Budin-Ljøsne et al., "Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research," *BMC Med. Ethics*, vol. 18, no. 1, p. 4, Jan. 2017.
- [17] M. Alruwaili, S. P. Mohanty, and E. Kougianos, "hChain: Blockchain-Based Large-Scale EHR Data Sharing with Enhanced Security and Privacy," *arXiv preprint arXiv:2505.12610*, 2025.
- [18] P. Sharma, A. Kumar, and R. Singh, "Blockchain Innovation for Consent Self-Management in Health Information Exchange," *Decis. Support Syst.*, vol. 169, 2023.
- [19] HIE of One, "Patient-Centered Health Record Sharing via Blockchain," *White Paper*, 2022.
- [20] K. Pampattiwar and P. Chavan, "A Secure and Scalable Blockchain-Based Model for Electronic Health Record Management," *Sci. Rep.*, Apr. 2025.
- [21] S. M. I. Alam, M. S. Islam, and K. Salah, "Blockchain for Health Data Exchange: A Survey," *Healthc. Inform. Res.*, vol. 26, no. 3, pp. 175–186, Jul. 2020.
- [22] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *Proc. IEEE OBD*, 2016.
- [23] U.S. FDA and IBM, "Blockchain for Drug Supply Chain: Pilot Project," *FDA Report*, 2019.
- [24] M. Shaikh, M. M. Hassan, G. Fortino, and M. Chen, "A Systematic Literature Review for Blockchain-Based Healthcare Implementations," *Healthcare*, vol. 13, no. 9, p. 1087, May 2025.
- [25] F. M. Abdelsalam et al., "A Systematic Literature Review of Blockchain Technology Benefits and Threats in Healthcare," *JMIR*, vol. 25, 2023.
- [26] MediLedger, "Blockchain in Pharma Supply Chain: Pilot Report," *MediLedger Consortium*, 2020.

- [27] K. Pampattiwar and P. Chavan, "A Secure and Scalable Blockchain-Based Model for Electronic Health Record Management," *Sci. Rep.*, Apr. 2025.
- [28] M. Alruwaili, S. P. Mohanty, and E. Kougianos, "hChain: Blockchain-Based Large-Scale EHR Data Sharing with Enhanced Security and Privacy," *arXiv preprint arXiv:2505.12610*, 2025.
- [29] A. Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Law?," *Eur. Law J.*, vol. 23, no. 4, pp. 440–468, 2018.
- [30] F. M. Abdelsalam, S. Ramzan, and J. Hossain, "A Systematic Literature Review of Blockchain Technology Benefits and Threats in Healthcare," *JMIR*, vol. 25, 2023.
- [31] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008.
- [32] H. Agoro, Y. Yang, and H. Yin, "Building Trust in Healthcare with Privacy Techniques: Blockchain in the Cloud," *arXiv preprint arXiv:2312.10214*, 2025.
- [33] European Union, "General Data Protection Regulation (GDPR)," *OJ L 119*, May 2018.
- [34] M. Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Law?," *Eur. Law J.*, vol. 23, no. 4, pp. 440–468, 2018.
- [35] Y. Wang, T. Zhang, and P. Chen, "Cross-Border Data Regulation and Blockchain Applications in Healthcare," *IEEE Access*, vol. 10, pp. 22501–22515, 2022.
- [36] A. M. Nguyen, "Challenges of Blockchain Applications in Digital Health: A Systematic Review," *arXiv preprint arXiv:2304.04101*, Apr. 2023.
- [37] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," *NIST Report 8202*, Oct. 2018.
- [38] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proc. EuroSys*, 2018.
- [39] S. E. Chang and Y. Chen, "Blockchain in Health Care Innovation: Literature Review and Case Study from a Business Ecosystem Perspective," *J. Med. Internet Res.*, vol. 22, no. 8, p. e19480, Aug. 2020.
- [40] R. G. Smith and L. Thomas, "Legacy IT Barriers to Blockchain in Healthcare," *Health Inform. J.*, vol. 27, no. 3, pp. 1–14, 2021.