

Transforming Clinical Data Security and Management through Blockchain

Khaled MERIT

TIT Laboratory, Department of Electrical Engineering, Tahri Mohamed University of Bechar Algeria
Email of the corresponding author: merit.khaled@univ-bechar.dz

Received: 20 June 2026

Accepted for publication: 19 September 2026

Published: 12 October 2026

Abstract--- This paper presents a narrative review of the scientific literature on the application of blockchain technology in healthcare data security and management. A structured search of PubMed, Scopus, and Google Scholar covering January 2017 to January 2026, using a consistent search string and eligibility criteria, identified 30 relevant studies addressing blockchain in clinical and health data contexts; each study was appraised with a quality instrument adapted from MMAT and SANRA and classified by level of evidence. The reviewed evidence indicates that blockchain's decentralized, cryptographically secure, and immutable architecture offers theoretical advantages for health data interoperability, patient privacy, electronic health record integrity, clinical trial transparency, and pharmaceutical supply chain authentication. Real-world pilot implementations, including Estonia's national health data infrastructure and the FHIR Chain project, provide preliminary feasibility evidence, and the comparative analysis is anchored in published quantitative benchmarks for throughput, latency, and energy as well as an explicitly modeled national hospital workload. However, the current evidence base remains predominantly conceptual; large-scale empirical validation comparing blockchain with existing systems in terms of clinical outcomes, system performance, and cost-effectiveness is largely absent. Key barriers to adoption include regulatory conflicts with GDPR and HIPAA, scalability limitations, high implementation costs, and a lack of interoperability standards. These limitations must be acknowledged before broad recommendations for adoption can be made. Collaborative efforts among healthcare providers, technologists, regulators, and policymakers, supported by rigorous empirical research, will be essential to determine whether blockchain offers demonstrable advantages over current technologies and to guide its responsible integration into health systems.

Keywords—Blockchain technology, Health data management, Healthcare industry, Data sharing, Electronic medical records

I. INTRODUCTION

The digitalization of healthcare has generated unprecedented volumes of sensitive patient data, placing growing pressure on existing systems for data storage, sharing, and security. Traditional centralized electronic health record (EHR) systems, while widely adopted, remain vulnerable to single points of failure, data silos across institutions, and breaches of patient privacy [1], [2]. In this context, blockchain technology has attracted considerable interest as a potentially transformative approach to health data management, owing to its decentralized architecture, cryptographic security, and immutable audit trail [3],[4]. The purpose of this article is to examine the current state of

evidence on blockchain applications in healthcare, critically analyze both the theoretical potential and real-world implementation challenges, and identify key gaps that must be addressed before widespread adoption can be considered.

While a number of systematic and scoping reviews have assessed blockchain in specific healthcare domains [1],[2],[4],[5],[6], a critical gap remains in consolidating findings across application areas, comparing blockchain with alternative emerging technologies, and clearly delineating which claimed benefits are supported by empirical evidence versus which remain theoretical. Existing reviews tend to focus narrowly on technical implementations without sufficiently addressing regulatory conflicts, scalability constraints, or the organizational conditions required for

successful adoption. This review addresses these gaps by synthesizing evidence across multiple application domains, providing a structured comparison of blockchain with competing technologies, and grounding its analysis in both the opportunities and the documented limitations of current evidence. The contribution is deliberately analytical rather than experimental: no new architecture, prototype, or simulation is presented; instead, the review synthesizes the evidence base, appraises its quality, anchors the comparison in quantitative benchmarks, and distills design guidance, including a reference architecture for a permissioned national health network (Section VII), while stating plainly that empirical construction and evaluation remain future work.

II. REVIEW METHODOLOGY

This paper is a narrative review of the scientific literature on the application of blockchain technology in healthcare. Unlike systematic or scoping reviews, a narrative review was selected to provide a broad, contextual overview of both the theoretical frameworks and the practical challenges associated with blockchain adoption in health systems; narrative reviews are a recognized design with their own quality standards, including transparent reporting of aims, search strategy, and synthesis approach [7], [8]. The primary contribution of this work is to synthesize current knowledge, identify key application domains, critically compare blockchain with alternative technologies, and highlight gaps that require further empirical investigation: a perspective not fully covered by existing reviews that focus primarily on technical implementations. Scientific literature on the application of blockchain technology in healthcare. Unlike systematic or scoping reviews, a narrative review was selected to provide a broad, contextual overview of both the theoretical frameworks and the practical challenges associated with blockchain adoption in health systems. The primary contribution of this work is to synthesize current knowledge, identify key application domains, critically compare blockchain with alternative technologies, and highlight gaps that require further empirical investigation: a perspective not fully covered by existing reviews that focus primarily on technical implementations.

Search strategy. The literature search was conducted across three major bibliographic databases: PubMed/MEDLINE, Scopus, and Google Scholar. The search string combined the terms (“blockchain” OR “distributed ledger” OR “blockchain technology”) AND (“healthcare” OR “health” OR “clinical” OR “electronic health record*” OR “medical record*” OR “health data”). For Google Scholar, the first 200 results per query were reviewed, consistent with common practice given the limitations of its interface. The search covered publications from January 2017 to January 2026, spanning the period in which blockchain adoption in healthcare emerged and subsequently matured, using a consistent search string and eligibility criteria throughout.

Eligibility, deduplication, and selection. Inclusion required that an article (i) address blockchain or distributed ledger technology in a healthcare or clinical context; (ii) be a peer-reviewed journal article, a systematic or scoping review, or an authoritative institutional or regulatory report; (iii) be written in English; and (iv) fall within the search window. Studies focused exclusively on cryptocurrency applications without healthcare relevance, editorials without a described

method, and duplicate or superseded analyses of the same cohort were excluded. Records were deduplicated in two passes: automated deduplication in a reference manager using DOI/PMID matching, followed by manual inspection of near-duplicate titles. Titles and abstracts were then screened against the eligibility criteria, and remaining articles were assessed in full text. Reasons for exclusion at each stage are summarized in Fig. 1.

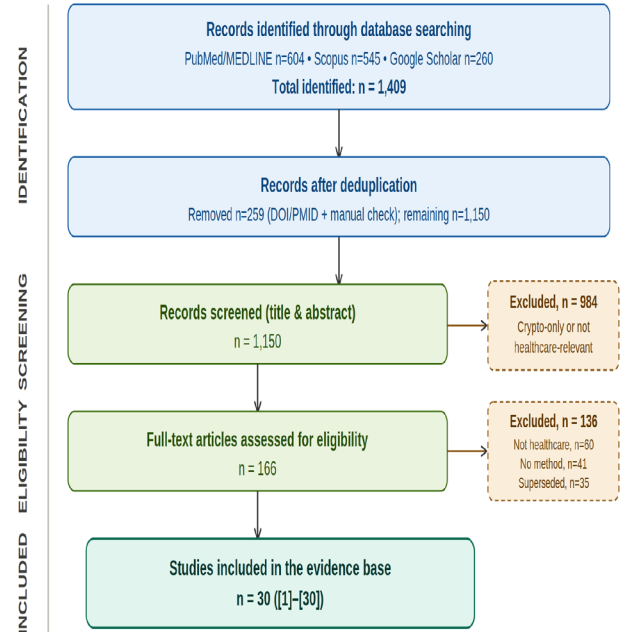


Fig. 1. PRISMA-based study selection flow (January 2017–January 2026): 1,409 records identified, yielding 30 included studies after screening; full counts and quality appraisal are given in Section II and Table I.

Rationale for the evidence base. The final evidence base comprises 30 studies [1]–[6], [9]–[32], satisfying all inclusion criteria. Selection was guided by relevance scoring against the review’s four objectives: application-domain coverage, comparative insight, regulatory relevance, and documented real-world experience and by domain saturation: the included studies collectively span all eleven application domains analyzed in Section IV and all three comparator technologies in Section VI. Standards, regulatory instruments, and benchmark reports supporting specific technical or legal claims are cited separately and were not counted as studies.

Quality appraisal. Each of the 30 studies was appraised with an eight-item checklist adapted from the Mixed Methods Appraisal Tool (MMAT) [33] and the SANRA scale for narrative reviews [7]: (1) explicit research objective; (2) transparent description of method; (3) peer-reviewed venue or authoritative source; (4) empirical component (data collection, prototype, or measurement); (5) real-world deployment evidence; (6) reproducibility of the synthesis; (7) explicit acknowledgment of limitations; and (8) currency (published 2020 or later). Studies meeting seven or eight criteria were rated High, five or six Moderate, and four or fewer Low. Each study was additionally assigned a level of evidence: Level I, systematic or scoping review; Level II, primary empirical study, prototype, or benchmark; Level III, implementation, case, or policy report; Level IV, conceptual, narrative, or ethical analysis. Results are reported in Table I.

TABLE I. QUALITY APPRAISAL AND LEVEL OF EVIDENCE FOR THE 30 INCLUDED STUDIES.

Summary: Level I n = 13; Level II n = 8; Level III n = 4; Level IV n = 5; Quality High n = 12, Moderate n = 15, Low n = 3. No included study reports independently audited operational deployment metrics.

Ref	Study focus	Design	LoE	Quality	Principal limitation
[1]	Blockchain in healthcare: applications and challenges	Systematic review	I	High	Primary base dominated by concepts
[9]	Blockchain vs centralized authentication for IoT (smart cities)	Comparative analysis	II	Moderate	Smart-city, not clinical, context
[10]	DDoS prevention for IoT using Ethereum	Empirical/simulation	II	Moderate	Non-clinical workload
[11]	Blockchain-envisioned access control for IoT	Survey	I	High	Breadth over clinical depth
[12]	Health information sharing; NFT potential	Empirical + survey	II	High	Stakeholder sample limited
[3]	Blockchain in the future of healthcare	Narrative review	IV	Moderate	Conceptual; no evaluation
[2]	Blockchain in healthcare and health sciences	Scoping review	I	High	Heterogeneity limits synthesis
[4]	Benefits and threats of blockchain in healthcare	Scoping review	I	High	Deployment evidence scarce
[13]	Pharmaceutical industry blockchain adoption	Trade article	IV	Low	No method; promotional
[14]	Personal control of privacy and data: Estonian experience	Case report	III	Moderate	Vendor-affiliated perspective
[15]	Estonian health records secured by blockchain	Trade article	IV	Low	Brief; non-scholarly
[16]	FHIRChain: clinical data sharing on blockchain	Prototype	II	High	Lab-scale evaluation only
[5]	Blockchain applications in health care for COVID-19 and beyond	Systematic review	I	High	Short-lived pilots in evidence base
[6]	Blockchain personal health records	Systematic review	I	High	Prototypes only in base
[17]	Blockchain policy framework for EHR management	Prototype/policy (thesis)	II	Moderate	Institutional scope
[18]	Adaptation of primary care centers to virtuality	Perspective	IV	Low	Descriptive; no evaluation
[19]	Blockchain for future wireless networks: decade survey	Survey	I	Moderate	Not healthcare-specific
[20]	Health data hubs: data governance for research	Policy analysis	III	High	Non-blockchain comparator
[21]	Guide to sharing open healthcare data under GDPR	Guidance	III	High	Legal, not empirical
[22]	Pharmacist access to health care data (blockchain + AI)	Framework/review	II	Moderate	US-centric
[23]	Estonian Biobank cohort profile	Cohort profile	III	Moderate	Predates search window (contextual)
[24]	Ethics of blockchain in organizations	Ethical analysis	IV	Moderate	Normative
[25]	Blockchain in health information systems	Systematic review (2024)	I	High	Primary evidence remains conceptual
[26]	Blockchain applications in healthcare	Systematic review (2025)	I	High	Heterogeneous primary base
[27]	Blockchain integration in healthcare: applications, performance challenges, solutions	Review (2024)	I	Moderate	Performance evidence limited
[28]	EHR systems based on blockchain	Review (2026)	I	Moderate	Very recent; longitudinal evidence pending
[29]	Blockchain-enabled self-sovereign identity in healthcare	Scoping review (2026)	I	High	Application mapping, no outcomes
[30]	Privacy-preserving and redactable healthcare blockchain (PRHBS)	Prototype (2024)	II	Moderate	No operational deployment
[31]	Zero-knowledge proofs for anonymous authentication	Prototype/proof (2025)	II	Moderate	Benchmark scale limited
[32]	Blockchain meets AI in healthcare	Review (2026)	I	Moderate	Emerging field; thin empirical base

Limitations of the selection process. As a narrative review, study selection was performed by a single author without protocol registration, and the restriction to English-language publications in three databases may have excluded relevant work, introducing potential selection and language bias. Backward citation searching was used to mitigate database bias, and the appraisal in Table I makes the evidential weight of each source explicit rather than implicit. The predominance of review and conceptual designs in the eligible literature (Table I) further limits the strength of the conclusions and is itself a finding of this review. These limitations are discussed further in the Conclusion.

III. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Blockchain technology makes it possible to have a distributed and decentralized database, formed by blockchains

designed to prevent their modification once data has been published; a reliable time stamp is used and linked to a previous block, allowing the transfer of assets and data in a verifiable and reliable way. Fig. 2 illustrates the data flow in a conventional centralized network, where a central server mediates all changes and access requests, representing the single point of control and failure typical of legacy health data systems. In contrast, Fig. 3 depicts the equivalent flow in a blockchain-based network, where changes are proposed by individual nodes and validated through distributed consensus before being permanently registered across the chain eliminating the single point of failure and enhancing both resilience and auditability. This system is especially suitable for storing data ordered in time without the possibility of modification or alteration, recording atomic changes in the system's state, and leaving a timestamp [1]. As it is a system with immutable, decentralized, and verifiable characteristics,

it is currently primarily used in the cryptocurrency market exchange system. However, it is not its exclusive use, and currently, blockchain technology can mean a change for the better in many data management systems; its usefulness is also being studied in areas that handle large volumes of data (big data), such as smart cities or a network of objects interconnected through the Internet (Internet of Things) [9-11].

Structurally, blockchain technology creates a continuous chain of interconnected data blocks shared with all system participants, containing information on multiple transactions [12]. To understand the operation of blockchain data storage and exchange, we must take into account some key elements:

Blocks are data units that store transactions and are cryptographically linked to the previous block, forming an immutable chain.

Transactions are data records, such as transfers of digital assets or medical information, validated by the network and added to a block. These transactions are subject to "Smart contracts," programmable standards implemented in the blockchain that are automatically executed when the conditions are met.

Cryptography encrypts data and ensures privacy and security, limiting access to authorized parties.

Distributed consensus implies that several nodes work together to verify and validate transactions, ensuring reliability and integrity.

There are several types of blockchain, each with its specific characteristics and uses [1]. Some of the most illustrative existing examples would be:

Public: Open network - Anyone can join, validate transactions & view the blockchain data. Public blockchains represent cryptocurrencies where users can buy/sell their coins &/or see what other users own. Users' anonymity & privacy are ensured via encrypted accounts.

Private: A private blockchain is a distributed ledger technology that allows for greater control over who can access the information stored within the ledger. Typically, a small number of entities control this type of blockchain, giving them full authority to approve or deny transaction requests. Companies and organizations often use this type of blockchain to provide increased productivity and security to their internal business operations.

Hybrid: Hybrid networks are defined as those using a combination of the features of a public blockchain, such as open participation and a public transaction ledger, and the features of a private blockchain, such as permissions to access, participate in and manage the network. In this way, hybrid blockchains provide more access and use than public blockchains while providing more privacy and security than private blockchains.

Cryptographic technology using consensus-protocol techniques gives blockchain its unique security properties that prevent malicious changes to recorded data on the distributed ledger. Additionally, since all information must be agreed upon by the majority of those involved with the blockchain before being changed, information remains immutable while on a blockchain. Because the blockchain provides an immutable record of all transactions, people can trust the

records or audits created for them on blockchains when they rely on these types of records for making medical decisions that affect patient safety [2-3], [12].

IV. APPLICATIONS IN THE HEALTH SECTOR

The health sector, including primary care, faces several challenges that directly impact the quality and efficiency of health care. Through its various applications, blockchain has the power to redefine the way challenges are addressed and specific solutions are offered [4].

Although evidence regarding the use of blockchain is booming in scientific literature, this technology and its uses in health systems remain predominantly in a conceptual framework. Despite this, this technology is already the focus of attention of both public and private interests [13]. An example of its institutional application is the European state of Estonia, where cyber-attacks on its public data structure in 2017 led its government to create and implement blockchain-based data management systems [14-15]. Another example to highlight is FHIRChain, a blockchain-based project developed by a research team at Vanderbilt University (Tennessee, EE., UU.), which meets its government standards and explores demonstrating the operation of a decentralized application based on FHIRChain, in this case, to authenticate participants in a study that includes collaborative decision-making [16].

Recent systematic reviews suggest that the integration of blockchain technology in the health sector opens up a range of possibilities that can improve efficiency, security, and transparency in various aspects [1], [2], [4], [5-6], [17]. Below, we explore some of these applications:

A. Interoperability

Blockchain technology could provide a distributed and secure framework for sharing healthcare information across institutions. By using a standardized method of organising and storing health-related information within blockchains, the amount of fragmented health data could decrease, while the security of access to that data could become more patient-controlled. Healthcare professionals would theoretically have access to full and accurate patient records in real-time, enabling more accurate diagnoses and more efficient care coordination [3],[19]. The FHIRChain project demonstrated the technical feasibility of using a blockchain-based, HL7 FHIR-compatible architecture for decentralized clinical data sharing [16], providing one of the few concrete implementation examples available. However, in practice, achieving interoperability through blockchain requires all participating institutions to adopt compatible data standards and governance frameworks, a challenge that has proved difficult even with non-blockchain systems. No large-scale, operational blockchain interoperability network in healthcare has yet been independently validated in the peer-reviewed literature, and most evidence for this application remains at the proof-of-concept stage [1],[2].

Recent developments sharpen both the promise and the difficulty of this agenda. HL7 FHIR R4 has become the mandated exchange standard in the United States certification program (ONC HTI-1 final rule, 2024), giving blockchain gateways a stable canonical data model to anchor to; the European Blockchain Services Infrastructure signals institutional adoption of distributed-ledger rails for public services; and W3C decentralized identifiers (2022) together

with the EU Digital Identity Wallets mandated by eIDAS 2.0 from end-2026 supply the legal-identity scaffolding that cross-organizational access control requires [34], [35]. Cross-chain messaging protocols continue to mature [47], although healthcare interoperability will more plausibly be achieved by pairing ledgers with FHIR and legal-identity frameworks than by chain-native bridges alone.

B. Patient Privacy

Blockchain-based systems use advanced cryptography to give patients granular control over who can access their personal health data. Through public-key cryptography and smart contracts, users could grant and revoke access permissions to selected healthcare professionals at any time, without relying on a centralized administrator [3],[19]. This model represents a meaningful shift toward patient data sovereignty compared to traditional systems where access control is managed institutionally. However, several unresolved issues temper these claims. First, the usability of cryptographic key management for non-technical patients remains a significant practical barrier; if a patient loses their private key, access to their own records may be permanently compromised. Second, while data stored on-chain can be encrypted, metadata about transactions (e.g., the fact that a patient record was accessed) may still be visible to network participants, raising secondary privacy concerns. Third, the effectiveness of blockchain-based access control in meeting GDPR requirements for data minimization and purpose limitation has not been empirically demonstrated [21]. These limitations underscore that blockchain enhances, rather than fully solves, patient data privacy.

Emerging techniques directly address several of these barriers: zero-knowledge proofs now permit anonymous yet verifiable authentication of patients and professionals, with healthcare frameworks demonstrated in 2025 [31]; redactable blockchain constructions allow authorized correction of specific records while preserving verifiable chain structure [30]; and threshold-cryptography wallets with custody delegated to accredited institutions under eIDAS 2.0 mitigate the lost-key problem [34], [35], as detailed in Section V.F.

C. Medical records

Blockchain technology has the potential to serve as a platform for managing Electronic Health Records (EHRs), as all actions regarding the EHR are stored permanently, verifiably, and cannot be modified. All modifications to an EHR would be permanently stamped with the date, time, user ID, and prior state, thereby reducing the potential for records to be lost or altered in an unauthorized manner. EHRs on a blockchain could allow patients to maintain greater control over their health information, while giving healthcare professionals access to accurate and up-to-date data in real-time [3],[6]. A systematic review by Fang et al. [6] confirmed that blockchain personal health record systems are technically implementable, identifying several prototype systems. However, the same review noted critical unresolved issues: the vast majority of existing systems are prototypes without clinical deployment evidence; EHR data volumes are extremely large, making full on-chain storage impractical and necessitating hybrid off-chain architectures; and the transition from legacy EHR systems to blockchain-based ones would require substantial investment and standardization that no healthcare system has yet achieved at scale. The immutability of blockchain also creates complications when records need to

be corrected due to data entry errors a common occurrence in clinical settings since corrections must be appended as new entries rather than overwriting incorrect data, potentially complicating clinical interpretation [14].

The choice of blockchain architecture is as consequential as the decision to adopt blockchain at all. Public, permissionless blockchains are generally unsuitable as the primary infrastructure for EHR management for five reasons. First, confidentiality: transaction payloads and metadata on public chains are visible to anyone, which is incompatible with the confidentiality obligations that health data attract under HIPAA and GDPR Article 9. Second, identity: public-chain pseudonymity does not withstand linkage attacks that can re-identify patients from access patterns. Third, data-subject rights: immutable public records are structurally at odds with rectification and erasure duties. Fourth, performance economics: base-layer throughput on the order of 15–30 transactions per second with ~12-second blocks and fee volatility cannot underpin clinical workflows that require predictable, sub-second authorization (Table III). Fifth, accountability: with unknown, distributed validators there is no identifiable data controller or processor able to bear the legal responsibilities that health regulations impose. Permissioned consortium architectures such as Hyperledger Fabric, Besu or Quorum with QBFT consensus, or Corda Enterprise resolve these objections by restricting validation to identified institutions, enabling channels and private data collections for confidentiality, providing deterministic finality, and demonstrating throughput in the thousands of transactions per second (Section IV.K). Public chains retain a complementary role where transparency itself is the product for example, publicly anchoring hashes of clinical-trial registrations but they should not host identifiable health records.

D. Medical research and clinical trials

Research integrity in clinical trials is a well-documented challenge, with concerns about selective outcome reporting, data manipulation, and post-hoc protocol changes [20]. Blockchain technology has been proposed as a method to address these issues by recording pre-registered trial protocols, consent forms, and results in an unalterable and auditable manner, thereby improving verification and transparency [16],[21]. This application is among the more technically mature: immutable timestamping of protocol registration directly leverages blockchain's core properties without requiring large-scale data storage or real-time clinical integration. However, the limitation of this approach is that blockchain can only ensure the integrity of data once it is entered into the chain; it cannot prevent falsification of data before entry. The quality of trial data recorded on a blockchain is therefore only as reliable as the data collection processes upstream. Furthermore, while the concept has been extensively discussed in the literature, operational blockchain-based clinical trial registries at a scale comparable to existing systems such as ClinicalTrials.gov remain to be demonstrated and validated [20].

E. Drug policy and authentication

Pharmaceutical supply chain integrity is one of the most practically advanced blockchain applications in healthcare. Every step from manufacturer to distributor to community pharmacy can be recorded and verified on a shared blockchain ledger, providing a traceable and tamper-evident record that

helps detect counterfeit or substandard medicines [22]. This is a particularly valuable application in low- and middle-income settings where counterfeit medicines represent a serious public health threat. The Medi-Ledger Network, a permissioned blockchain consortium involving major pharmaceutical companies, represents one of the most mature real-world implementations, having demonstrated operational viability for drug provenance tracking in the United States. However, a critical limitation of this approach is the “oracle problem”: blockchain can guarantee the integrity of data once

recorded, but it cannot verify that the physical product placed on the chain actually corresponds to the registered data. Counterfeit drugs can be entered into the system at the point of registration if that step is compromised. Additionally, achieving full supply chain coverage requires universal adoption by all participants including smaller distributors and pharmacies which presents significant governance and cost challenges [22].

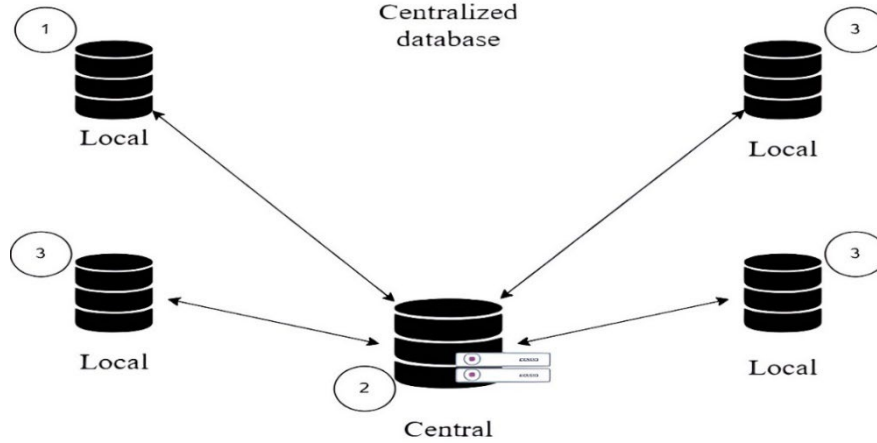


Fig. 2. Data flow in a conventional centralized (hub-and-spoke) health information network. (1) A local server submits a change; (2) the single central server validates and registers it constituting both the system's authority and its single point of failure; (3) validated data become available to the other local servers. All trust is concentrated in the central node. of data flow in a conventional centralized (hub-and-spoke) network.

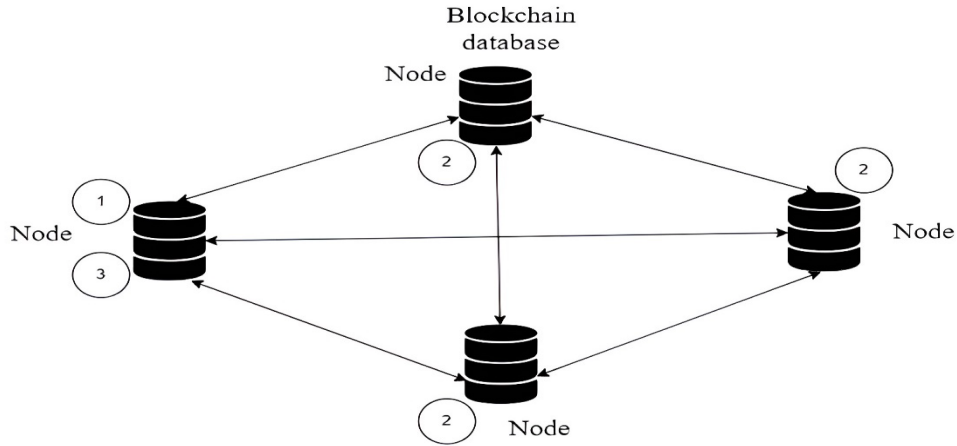


Fig. 3. Data flow in a blockchain-based distributed network. (1) A node proposes a change to the shared ledger; (2) peer nodes independently validate the proposed transaction according to consensus rules; (3) the validated change is permanently registered on every node's copy of the chain, eliminating the single point of failure and producing a tamper-evident audit trail. of the data flow in a blockchain-based distributed network.

The regulatory salience of this application continues to grow. Under the U.S. Drug Supply Chain Security Act, enforcement of full serialization began in November 2023, with stabilization periods extending into 2024–2027 [36], and the final report of the FDA-hosted MediLedger pilot project concluded that a blockchain-based solution is feasible for DSCSA compliance [37]. Section VI.B examines the MediLedger trajectory and the cautionary counter-examples of stalled deployments in depth.

F. Immunizations and epidemics

Accurate and tamper-proof vaccine tracking is a critical public health need, particularly in global immunization programs where supply chain fragmentation leads to waste,

inequitable distribution, and counterfeit products. Blockchain technology has been proposed as a platform to record every step of vaccine delivery from cold-chain manufacturer to final administration in an immutable, auditable ledger that public health authorities and logistics partners can access in real time [5]. During the COVID-19 pandemic, this application attracted significant institutional interest. Ng et al. [5], in a systematic review published in *The Lancet Digital Health*, identified multiple blockchain pilot projects applied to vaccine distribution tracking, contact tracing, and health certificate verification across several countries. Their review confirmed that blockchain's decentralized structure offers meaningful advantages for cross-border data sharing in epidemic

response, where central authorities are absent or distrusted. Blockchain can also support equitable vaccine distribution by providing transparent, verifiable allocation records that reduce the risk of diversion or fraud. Additionally, blockchain-based contact tracing can allow health professionals to identify and isolate potential infection clusters while protecting the identity of individuals through cryptographic pseudonymization [5]. However, the same review noted that most implementations were short-lived pilots without long-term evaluation data, and that integration with existing public health surveillance systems remains technically and politically challenging. The dependence on digital infrastructure and smartphone access also risks excluding the most vulnerable populations in low-resource settings, who arguably have the greatest need for equitable vaccine distribution

G. Telemedicine and informed consent

The expansion of telemedicine and remote care services has increased the need for secure, verifiable processes for patient identification, consent management, and remote data exchange. Blockchain technology could support telemedicine by providing an immutable record of digitally signed informed consent, thereby improving the legal accountability and auditability of remote consultations [18]. Smart contracts could also be used to automate consent workflows, ensuring that patients have explicitly agreed to specific data uses before records are shared with telehealth providers. However, the practical deployment of blockchain-based consent management in telemedicine remains at the conceptual stage. Key challenges include the need for robust digital identity verification systems that can link a real patient to their blockchain identity, the exclusion of patients without adequate digital literacy or device access, and the risk that automated smart contract execution may be too inflexible to accommodate the nuanced, context-specific nature of genuine informed consent in clinical settings. The legal standing of blockchain-recorded consent across different jurisdictions also requires clarification [18].

H. Organ donation and genomics

Organ allocation systems require transparent, tamper-proof registries where donor consent, organ availability, and recipient matching criteria must be reliably recorded and auditable by multiple stakeholders. Blockchain technology could provide an open and verifiable registry that reduces the risk of fraud or administrative error in organ allocation, potentially improving trust among patients, clinicians, and transplant authorities [3]. In genomics research, blockchain could facilitate secure data sharing between institutions without requiring participants to cede control of their genetic data to a centralized repository, enabling large-scale multi-institutional studies while preserving data sovereignty [23]. The Estonian Biobank project, though not blockchain-based, illustrates the governance model that blockchain could formalise [23]. However, both application areas face significant unresolved challenges. Organ donation systems require real-time, 24/7 reliability with zero tolerance for latency or downtime, placing extreme demands on blockchain infrastructure that have not yet been tested at operational scale. In genomics, the volume of data generated by whole-genome sequencing is many orders of magnitude larger than what current blockchain systems can store on-chain, making hybrid architectures with off-chain genomic data storage a practical

necessity. Regulatory frameworks governing the secondary use of genetic data, such as the GDPR's special category protections for biometric data, add further complexity to any blockchain implementation in this domain.

I. Tracking treatment histories

A comprehensive, longitudinal treatment history is essential for safe and effective care coordination, particularly for patients with chronic conditions managed across multiple providers. Blockchain's immutable and chronological record structure could theoretically provide patients and clinicians with a tamper-proof, patient-controlled summary of all treatments, prescriptions, and clinical encounters across institutions [16],[6]. This could reduce duplicate testing, prevent adverse drug interactions caused by information gaps, and facilitate continuity of care during provider transitions. In practice, however, populating such a record requires interoperability with all source systems that generate clinical data, a requirement that remains technically and organizationally challenging. The fragmented nature of current healthcare IT infrastructure means that achieving a complete treatment history on blockchain would require broad adoption across competing systems and vendors a coordination problem that has not been solved by any existing national EHR initiative.

J. Resource Management

Efficient resource management is a persistent operational challenge for healthcare systems, encompassing the allocation of beds, operating theatre time, diagnostic equipment, and medical appointments. Blockchain-based smart contracts could automate resource scheduling and allocation, providing real-time visibility of supply and demand across facilities and reducing administrative overhead [16]. However, the application of blockchain to real-time operational management introduces significant technical requirements. Unlike static data storage, resource management requires high transaction throughput, low latency, and seamless integration with existing hospital information systems requirements that current blockchain platforms are not optimized to meet. Most proposals for blockchain-based resource management remain at the theoretical or simulation stage, and the added complexity compared to existing centralized scheduling systems has not been shown to deliver commensurate benefits in any published operational deployment.

K. Evaluation of key performance parameters

Based on the synthesized literature, Table II provides a structured assessment of blockchain technology across four parameters of central importance to healthcare data management: reliability, interoperability, scalability, and transparency. These parameters constitute critical dimensions for evaluating any healthcare data management solution and are discussed in detail below.

Reliability: Blockchain's distributed consensus mechanism eliminates single points of failure, meaning the network continues to function even if individual nodes go offline [5]. This gives blockchain a theoretical advantage over centralized EHR systems, which are vulnerable to server outages. However, reliability in healthcare requires not only fault tolerance but also real-time responsiveness. Current public and permissioned blockchain platforms process transactions at speeds (typically 15–1,000 transactions per

second for permissioned systems) that are significantly lower than centralized database systems, which can handle tens of thousands of transactions per second [10],[12]. For most healthcare data management tasks this is acceptable, but for real-time emergency care applications it remains a constraint. No published operational healthcare deployment has yet reported system reliability metrics (e.g., uptime, mean time to recovery) comparable to certified medical-grade infrastructure.

Interoperability: Blockchain can serve as a shared, tamper-proof data layer that connects disparate healthcare systems, potentially reducing the data silo problem that characterises current EHR environments [2],[3]. The FHIRChain project demonstrated that pairing blockchain with the HL7 FHIR standard enables cross-institutional data exchange with strong provenance guarantees [16]. Nevertheless, interoperability is a governance and standardization challenge as much as a technical one. Blockchain does not automatically resolve differences in data formats, coding systems (e.g., ICD-10 vs SNOMED), or institutional policies. Full interoperability requires industry-wide agreement on shared ontologies and access protocols, which has not yet been achieved in any healthcare system adopting blockchain.

Scalability: This is the most significant technical limitation identified in the reviewed literature [1],[10],[12],[2]. As the number of nodes and the volume of stored transactions grow, blockchain performance degrades: storage requirements expand continuously, consensus validation slows, and energy consumption increases. Healthcare generates some of the largest data volumes of any sector, including high-resolution imaging (DICOM files often exceeding 100 MB each), genomic datasets, and continuous monitoring streams. Storing this data directly on-chain is computationally and economically impractical with current technology. The established mitigation is a hybrid architecture in which only transaction metadata, access logs, and cryptographic hashes are stored on-chain, while the actual clinical data resides in off-chain encrypted storage [2],[16].

This approach preserves blockchain's auditability and access-control advantages while avoiding the storage scaling problem, but it introduces additional architectural complexity and requires secure management of the off-chain data layer.

Transparency: Blockchain's immutable and append-only ledger provides a complete, verifiable audit trail of all data accesses and modifications, which is a substantial improvement over centralized systems where audit logs can be altered or deleted [12],[3]. In healthcare, this level of transparency strengthens accountability, supports regulatory auditing, and builds trust among patients who can verify who has accessed their records and when. For clinical trials, transparent and time-stamped protocol registration on a blockchain directly addresses the problem of selective outcome reporting [20],[21]. However, full transparency must be balanced against privacy: in public blockchain architectures, transaction metadata is visible to all participants, which may be inappropriate for sensitive health data. Permissioned or private blockchain architectures address this by restricting visibility to authorized participants, but at the cost of reduced decentralization and the need to trust the permissioning authority [1],[2].

While there is currently limited empirical data to support direct comparisons of blockchain with established technologies in healthcare, the reviewed literature suggests that blockchain may offer notable advantages in transparency, data integrity, and patient data sovereignty. However, these claims remain largely conceptual, and real-world implementation evidence is still scarce. Until blockchain applications are more widely piloted and evaluated in healthcare settings, cultural, technological, and organizational barriers will continue to impede large-scale adoption. For widespread acceptance, healthcare users and professionals need to understand the potential benefits of this solution, develop a complete understanding of how it works, and collaborate with all stakeholders for its appropriate implementation and rigorous empirical evaluation.

TABLE II. STRUCTURED ASSESSMENT OF BLOCKCHAIN ACROSS FOUR PARAMETERS OF CENTRAL IMPORTANCE TO HEALTHCARE DATA MANAGEMENT. ALL FOUR PARAMETERS ARE DISCUSSED IN DETAIL IN THE SURROUNDING TEXT.

Parameter	Blockchain performance summary	Principal constraint	Evidence basis
Reliability	Distributed consensus eliminates single points of failure; the network continues to function if individual nodes fail	Real-time responsiveness is unproven; no published healthcare deployment reports uptime/MTTR metrics comparable to certified medical-grade infrastructure	Literature-based [1], [12]; author synthesis
Interoperability	Shared, tamper-proof data layer can connect disparate systems; pairing with HL7 FHIR demonstrated by FHIRChain	A governance and standardization problem as much as a technical one: data formats, coding systems (ICD-10 vs SNOMED CT), and institutional policies are not resolved by the ledger itself	Literature-based [3], [2], [16]
Scalability	Performance degrades as nodes and transaction volume grow; hybrid off-chain architectures mitigate storage growth	Healthcare data volumes (DICOM imaging >100 MB/study, genomic datasets, continuous monitoring streams) exceed practical on-chain capacity; mitigations add architectural complexity	Literature-based [1], [10], [12], [2]
Transparency	Immutable, append-only ledger provides a complete, verifiable audit trail of accesses and modifications	Full transparency conflicts with privacy in public architectures; permissioned designs restrict visibility at the cost of decentralization and trust in the permissioning authority	Literature-based [12], [3], [20], [21]

Beyond this qualitative structuring, the comparison can be anchored quantitatively: Table III compiles published benchmarks for the platforms most relevant to healthcare data

management, and the modeled workload below translates them into hospital-network terms.

TABLE III. REPORTED QUANTITATIVE BENCHMARKS FOR PLATFORMS RELEVANT TO HEALTHCARE DATA MANAGEMENT. VALUES ARE CONFIGURATION-DEPENDENT AND DRAWN FROM THE CITED BENCHMARK STUDIES AND INDUSTRY MEASUREMENTS; NO OPERATIONAL HEALTHCARE DEPLOYMENT PUBLISHES INDEPENDENTLY AUDITED KPIS (SEE TEXT).

Platform / system	Consensus	Reported throughput	Latency / finality	Energy evidence	Source
Bitcoin (public)	Proof of Work	≈ 7 TPS (commonly cited)	Probabilistic; ~ 60 min practical (6 conf.)	Highest energy class among ledgers; consensus-level analysis in [38]	[38]
Ethereum L1, pre-Merge	Proof of Work	$\approx 15\text{--}30$ TPS nominal	≈ 12 s blocks; probabilistic finality	≈ 23 million MWh/yr network electricity (2022 estimate)	[39]
Ethereum L1, post-Merge (Sept 2022)	Proof of Stake	Measured $\approx 14\text{--}26$ TPS (2024–2026)	12 s slots; ~ 2 epochs (~ 13 min) finality	Electricity and carbon reduced by $>99.988\%$	[39]
Ethereum Layer-2 rollups	Rollups settling to PoS L1	Higher effective throughput; tracked live (L2BEAT)	Sub-second soft confirmations typical	Inherits PoS L1; Dencun/EIP-4844 (Mar 2024) cut L2 data-posting costs $\sim 90\%$	[39]
Hyperledger Fabric v1.4–v2.x	Raft ordering (CFT)	$>3,500$ TPS in certain configurations; $\approx 3,000$ TPS peak (official v2.5 Caliper benchmark, minimal topology)	Sub-second typical (EuroSys measurements)	No mining; energy comparable to replicated data-center infrastructure rather than PoW [38]	[40], [41], [42]
Hyperledger Fabric v3.0 (Sept 2024)	SmartBFT (BFT)	BFT ordering added; performance-oriented release	Deterministic finality	As above (no mining)	[43]
Visa network (centralized reference)	Centralized	Capacity $>65,000$ TPS (vendor-stated)	$\approx$ seconds authorization	Centralized data-center consumption	[39]-source: Visa 2023 statement cited in Table III notes]
Conventional hospital EHR / RDBMS	Centralized	Thousands to tens of thousands of simple TPS (indicative; configuration-dependent)	Milliseconds to seconds	Per-record energy negligible relative to application tier	Indicative; vendor benchmarks vary

To translate these figures into healthcare terms, consider an illustrative national network of 50 hospitals. Industry estimates suggest that large hospital networks process on the order of millions of HL7 interface messages per day (an industry estimate; peer-reviewed figures are scarce). Only a fraction of such events requires on-chain notarization typically consent changes, access grants, record-pointer registrations, and audit events. Assuming 5–10% of an average aggregate of $\sim 1,000$ interface messages per second across the network is chain-relevant, and a peak-to-average ratio of 5:1, the ordering service must sustain roughly 250–500 transactions per second at peak within the demonstrated capacity of permissioned platforms and roughly two orders of magnitude above public-chain base layers. These are modeled, illustrative figures, not measurements; one of the clearest gaps this review identifies is that no operational healthcare deployment publishes independently audited throughput, latency, or uptime metrics, and future pilots should do so (Section VIII).

V. CURRENT BARRIERS AND CHALLENGES

Despite the theoretical potential described in the preceding section, the adoption of blockchain technology in healthcare faces substantial barriers. These barriers span regulatory, technical, economic, and socio-cultural dimensions, and collectively explain why blockchain adoption in health systems has remained largely confined to pilot and conceptual projects [1],[2],[4],[5–6],[17], [21]. The following subsections examine each barrier category and assess its implications for the viability of blockchain as a mainstream healthcare data management solution.

The principal barriers identified in the reviewed literature are discussed below.

A. Regulations and Laws

Creating comprehensive standards and regulations is critical for the effective and safe implementation of technology; without standards and rules that are specific to the manner in which blockchain will be implemented in the healthcare industry, there will be confusion about how to proceed. Uncertainties surrounding security, privacy and compliance with regulations contribute to inhibiting the adoption of blockchain solutions for the healthcare industry [1], [2], [4], [5], [6], [19]. A particularly acute tension exists between the immutability of blockchain records and the "right to erasure" (right to be forgotten) established under the General Data Protection Regulation (GDPR) in the European Union and similar provisions under the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Both frameworks require that personal health data can be corrected or deleted upon patient request, which fundamentally conflicts with blockchain's design principle of creating a tamper-proof and permanent audit trail. Potential technical mitigations include storing only data hashes on-chain while keeping personal data in off-chain encrypted storage, or using permissioned private blockchains with governance models that allow designated administrators to invalidate specific records. However, whether such approaches satisfy regulatory requirements remains legally untested in most jurisdictions, underscoring the need for clear, blockchain-specific regulatory guidance from health authorities and data protection regulators [21].

B. Technical complexity

The recent and technically complex nature of blockchain technology demands a learning curve. Experts in implementation and research are still scarce, as are specialists in their specific security systems and prevention of cyberattacks. It is also necessary to consider what it means to train managerial profiles, health professionals, and administrative personnel in any new technology and integrate it with existing systems and the day-to-day clinical practice [3], [2], [16].

C. Technological and economic costs

Obstacles include initial development and adaptation costs, staff training, integration with existing systems, ongoing maintenance, storage, processing, and energy consumption expenses [3], [6]. The more blocks a chain contains and the more participants there are in the decentralized network, the more requirements the network will need to function optimally and securely. The challenge of maintaining a massive blockchain-based data network has been described, and scalability is one of the current problems in the cryptocurrency market. All this will imply constant maintenance of a decentralized network with a data exchange based on a standard chain also in continuous growth and, therefore, will require a system that allows an exchange of a chain with increasing weight while maintaining simultaneity [10], [12]. From an architectural standpoint, permissioned or private blockchain models are generally considered more appropriate for healthcare than fully public blockchains, as they allow organisations to control participant access while reducing the energy and computational overhead associated with proof-of-work consensus mechanisms. Hybrid architectures, combining on-chain transaction records with off-chain encrypted storage for sensitive data, may offer a practical compromise between transparency and data minimization principles. Interoperability standards such as HL7 FHIR (Fast Healthcare Interoperability Resources) have been proposed as a compatible layer for blockchain-based health data exchange, and projects such as FHIRChain [16] have begun to demonstrate feasibility. Nevertheless, performance constraints including transaction throughput, latency, and storage growth remain active areas of research and have yet to be validated at healthcare-system scale. Despite this, it is necessary to weigh the initial costs of blockchain adoption against the potential long-term benefits in terms of transparency, security, and efficiency in handling health data.

D. Lack of experience and confidence

The recent emergence of the technology and its other uses in the cryptocurrency market have aroused a certain sense of suspicion and concern in the general population. Controlled access and cryptography ensure that only authorized parties can access the information, and even so, blockchain can be considered a secure technology as long as it cannot intervene in the atomic changes of the system. Data management is subject to extensive responsibility, especially in health data, so there should be sufficient compelling reasons in the risk/benefit balance to bet on this type of technology. Therefore, blockchain solutions must implement robust privacy and security measures to comply with current data protection regulations and must work to prevent future undesirable events [6].

E. Ethical Considerations

Blockchain was born as a technology to support cryptocurrencies, plagued by skepticism, and is still erroneously linked only to them. This relationship has created shadows on blockchain technology, associating it with speculation or fraud contexts related to the volatility of some cryptocurrencies. These shadows, which can be understood as pending challenges, are not part of its essence but emanate from the immaturity of the text and its misuse in some cases, as can happen with any other technology.

It is necessary to develop collective, critical, and ethical thinking about blockchain. Some reviews have been interested in this topic, but all agree that future research should be based on particular ethical frameworks and specific practical texts [24].

F. Technical mitigation strategies

Several of the barriers in Sections V.A–V.E now have concrete, increasingly mature technical responses; we summarize them with their maturity level (standardized, piloted, or research) because they inform both procurement decisions and the future directions in Section VIII.

Scalability. Three complementary strategies dominate. First, hybrid architectures keep only transaction metadata, access logs, and cryptographic hashes on-chain while clinical content resides in off-chain encrypted stores; content-addressed off-chain storage such as IPFS with on-chain hash anchoring has been shown to relieve chain growth for EHR deployments [44]. Second, Layer-2 protocols execute transactions off the base chain and settle periodically: rollups on Ethereum, whose data-availability costs fell by roughly an order of magnitude after the Dencun upgrade activated EIP-4844 in March 2024, illustrate the approach, although healthcare use remains at proof-of-concept stage. Third, permissioned platforms mitigate scalability structurally by replacing proof-of-work with ordering-based consensus: Hyperledger Fabric's execute-order-validate design sustains thousands of transactions per second in published benchmarks (Table III) [40]–[42], and v3.0 adds Byzantine-fault-tolerant ordering [43]. Sharding partitioning ledger state across node groups remains a research-stage option for public chains.

Regulatory compliance. For the immutability–erasure conflict (Section V.A), the most direct responses are (i) data minimization by design never placing personal data on-chain combined with crypto-shredding (destroying off-chain decryption keys to effect erasure), and (ii) redactable blockchain constructions based on chameleon-hash trapdoors that permit authorized editing while preserving verifiable chain structure; a 2024 healthcare implementation demonstrates the approach [30], building on the foundational construction of Ateniese et al. [45]. Distributing the trapdoor among a data-protection council prevents unilateral rewriting. Whether these constructions satisfy supervisory authorities in all jurisdictions remains to be tested and is flagged as an open legal-technical question.

Privacy. Beyond permissioned membership, fine-grained confidentiality can be obtained from zero-knowledge proofs, which allow a party to prove a property of hidden data without revealing the data [31]; from channels and private data collections in permissioned platforms, which restrict ledger visibility to subsets of organizations; and from trusted execution environments that compute over protected data

inside attested enclaves [46]. Each carries operational costs proof latency, enclave key ceremonies that must be weighed per use case.

Interoperability. Interoperability is primarily a governance and standards problem, but technical enablers have consolidated around canonical clinical data models HL7 FHIR R4 as the exchange standard, increasingly mandated by certification programs paired with blockchain gateways of the FHIRChain type [16]; and, where multiple chains must cooperate, cross-chain messaging protocols [47]. National infrastructure programs (e.g., EBSI in Europe) provide institutional rails for identity and credential use cases [34].

Key management. The practical barrier of patient-side key custody (Section IV.B) is being addressed with threshold and multi-party computation wallets, social-recovery patterns, and more realistically for healthcare delegation of custody to accredited institutions or national identity providers under eIDAS 2.0 wallets [34], [35]. Maturity: piloted.

We emphasize that none of these mitigations removes the structural challenges of governance, cost, and organizational change; they narrow the technical gap so that the remaining barriers are, increasingly, institutional rather than cryptographic.

VI. COMPARATIVE ANALYSIS: BLOCKCHAIN VS. TRADITIONAL SYSTEMS AND OTHER EMERGING TECHNOLOGIES

A. Comparative assessment and decision matrix

Table IV demonstrates the similarities and differences between data management technologies used within the healthcare sector. The three comparators were selected to

represent the main alternatives that healthcare organisations currently consider or employ: Traditional Centralized Systems represent the incumbent standard; Cloud-Based Solutions reflect the dominant contemporary upgrade path; and Federated Learning was included because it addresses similar goals to blockchain (enabling cross-institutional data collaboration without centralising sensitive records) and is increasingly cited in the healthcare data governance literature as a privacy-preserving alternative. The comparison highlighted the strengths of blockchain in terms of security and transparency compared to the other three technologies. The drawbacks of blockchain include its difficulty in terms of scalability and regulatory compliance. Traditional centralized systems are the most widely used and simplest way to manage healthcare data, but they are also susceptible to single point failures and do not provide the same level of auditability as blockchain systems. While cloud-based solutions allow for easy scalability, the data protections and privacy offered by cloud service providers place additional risk on the end-user. Federated learning provides an opportunity to retain all sensitive information securely within each organization while still enabling model training across multiple organisations without sacrificing data sovereignty. For healthcare decision-makers, the choice between these technologies should be driven by the specific use case: blockchain is most appropriate where an immutable, auditable, and decentralized record is essential (e.g., drug supply chain integrity, clinical trial registration); cloud solutions remain preferable for scalable and cost-effective data storage; and federated learning is better suited for scenarios requiring cross-institutional analytics without data sharing. Blockchain should therefore be viewed as a complementary, rather than universal, tool within a diversified health data management strategy.

TABLE IV. COMPARATIVE ANALYSIS OF DATA MANAGEMENT TECHNOLOGIES IN HEALTHCARE.

Feature / Characteristic	Blockchain	Traditional Centralized Systems	Cloud-Based Solutions	Federated Learning	Evidence basis
Data Security	Strong security through cryptographic techniques and consensus mechanisms; data is immutable [1],[12],[2].	Vulnerable to single points of failure; relies on perimeter defenses [1],[4].	Moderate security with cloud provider protocols; risk of breaches if misconfigured.	High data security since data is not centralized, only model parameters are shared.	Literature-based [1], [12], [2]
Data Privacy	Patients have control over access; privacy preserved via encryption and private blockchains [3],[6],[21].	Privacy depends on internal data control policies; may be prone to data leaks.	Managed by the cloud provider, with varying levels of privacy protection.	Privacy is preserved as data remains locally at the healthcare facilities.	Literature-based [3], [6], [21]
Interoperability	Blockchain can enhance interoperability by creating a shared, tamper-proof data layer [3],[16],[19].	Often limited due to data silos across healthcare institutions.	Varies depending on the provider; integration may require additional APIs.	Interoperable through federated model learning, but does not directly integrate data.	Literature-based [3], [16], [21]
Scalability	Limited by the size of the blockchain; performance may degrade with large datasets and many nodes [1],[10],[12],[2].	Typically scalable but central servers can become bottlenecks under high demand.	Highly scalable with large data processing capabilities through distributed servers.	Scalable in terms of model learning; depends on available local computation power.	Literature-based [1], [10], [12], [2]
Transparency	Full transparency with immutable records; all changes are traceable [12],[3],[20].	Limited transparency; data logs are internal and may not be easily auditable.	Transparency depends on cloud provider; potential audit logs are available.	Transparency in training models, but limited insight into the data itself.	Literature-based [12], [3], [20]
Technical Complexity	Requires specialized knowledge in cryptography, consensus mechanisms, and blockchain architecture [10],[3],[6].	Generally less complex; handled by internal IT infrastructure.	Moderately complex; depends on cloud management and IT integration efforts.	Requires knowledge of machine learning and data privacy strategies.	Literature-based [10], [3], [6]
Operational Costs	High initial development and energy costs; but	Moderate, depending on IT staff and	Subscription-based pricing models; costs	Costs are moderate, focusing on local	Literature-based [10],

	lower costs in ongoing security [10],[3],[6].	infrastructure maintenance.	vary based on storage and data transfer needs.	computation rather than centralized infrastructure.	[3], [6]; costs indicative
Trust and Adoption	High trust among participants due to transparency and immutability, but low adoption due to emerging nature [1],[2],[4].	High trust within institutions, but lacks transparency with external stakeholders.	High adoption with strong trust in major providers (e.g., AWS, Google Cloud).	High potential for trust due to privacy-preserving methods, but still emerging in healthcare.	Partly author synthesis [1], [2], [4]
Regulatory Compliance	Challenges with compliance due to unclear regulatory frameworks for blockchain use in healthcare; conflicts with GDPR right to erasure and HIPAA data correction requirements [1],[2],[21].	Well understood and compliant with existing regulations.	Must comply with cloud-specific regulations like GDPR or HIPAA.	Compliant with data privacy regulations as data does not leave local storage.	Literature-based [1], [2], [21]

Table IV is complemented by Table V, which maps representative healthcare use cases to recommended approaches and measurable selection criteria, providing an

operational bridge from the comparative analysis to procurement practice.

TABLE V. DECISION MATRIX MAPPING REPRESENTATIVE HEALTHCARE USE CASES TO RECOMMENDED APPROACHES AND MEASURABLE SELECTION CRITERIA (AUTHOR SYNTHESIS, GROUNDED IN SECTIONS IV–V).

Healthcare use case	Recommended approach	Candidate technology	Measurable selection criteria
EHR exchange and record integrity	Blockchain as integrity/consent layer over existing EHR	Hyperledger Fabric + HL7 FHIR R4 gateway	Deterministic finality <1–2 s; ~10 ³ TPS headroom; confidentiality via channels/PDCs
Drug traceability	Consortium chain for end-to-end provenance	Fabric-class private chain with GS1 identifiers	Regulatory anchor (DSCSA); modest TPS needs; universal participant adoption
Clinical trial registration and consent	Hash anchoring of timestamps; consent state machine	Public-chain anchoring or permissioned chain	Verifiable timestamps; low TPS; auditability for regulators
Patient identity and credentials	Self-sovereign identity on permissioned rails	W3C DID/VC; eIDAS 2.0 wallet; EBSI	Standardization (2022/2024); revocation latency; recovery governance
Imaging and genomic bulk data	Keep off-chain; anchor hashes only	Encrypted object stores; IPFS-style content addressing	Storage economics; retrieval latency; on-chain growth bounded
Cross-institutional analytics	Federated learning, optionally with blockchain audit layer	FL frameworks + on-chain aggregation certificates	Raw-data locality; audit overhead quantified
Scalable general storage and applications	Do not use blockchain	Cloud object/compute platforms	Cost per TB; elasticity; operational maturity
Emergency record access	Break-glass via smart contract + local cache	Permissioned chain + offline verification	Availability under partition; authorization latency <1 s

B. Critical appraisal of implementation trajectories

Because most blockchain-in-healthcare literature reports concepts or prototypes, examining the trajectories of real deployments is essential for separating durable value from technological enthusiasm. Two contrasting groups are instructive (Table VI). Sustained implementations tend to share five properties: (1) a narrow, compliance-driven scope Estonia's KSI blockchain, operational as an integrity-assurance layer over the national electronic health record infrastructure since 2016, guarantees that records and access logs have not been tampered with, without moving clinical data on-chain [14], [15]; similarly, the MediLedger consortium two dozen major supply-chain companies emerged from an FDA-hosted pilot whose final report concluded that a blockchain-based solution is feasible for compliance with the U.S. Drug Supply Chain Security Act [37], a regulatory anchor kept relevant by the DSCSA's phased enforcement (serialization from November 2023, with stabilization periods extending into 2024–2027) [36]. (2)

integration with, rather than replacement of, incumbent systems; (3) stable governance and funding (state e-health programs, or industry consortia sharing a compliance problem); (4) modest throughput requirements; and (5) measurable, legally mandated value.

Stalled or terminated efforts exhibit the mirror image. MIT's MedRec, an influential Ethereum-based EHR permissioning prototype piloted with Beth Israel Deaconess Medical Center, remained a research prototype and is no longer maintained emblematic of the prototype-to-production gap also visible in FHIRChain's lineage [16]. we.trade, a trade-finance consortium platform built on Hyperledger Fabric and backed by major European banks and IBM, ceased operations through insolvency in June 2022 after failing to secure continued investment [48]. IBM, once the most prominent enterprise blockchain vendor, sharply reduced its blockchain unit after revenue shortfalls reported in 2021, and the IBM Blockchain Platform reached end of support in April 2023 [49], [50] a caution for healthcare adopters regarding vendor risk. The comparative lesson is not that the technology

fails technically, but that blockchain deployments survive only where a regulatory mandate, shared governance, and integration economics align supporting this review's

recommendation of selective, compliance-anchored adoption rather than platform-first projects.

TABLE VI. FACTORS DIFFERENTIATING SUSTAINED FROM STALLED BLOCKCHAIN IMPLEMENTATIONS. SOURCES: [14]–[16], [37], [36], [48]–[50].

Dimension	Sustained implementations (Estonia KSI since 2016; MediLedger)	Stalled / terminated (MedRec; we.trade; IBM Blockchain Platform)
Regulatory anchor	National e-health mandate; DSCSA compliance requirement	None beyond research interest
Scope	Narrow: integrity layer over existing records; one supply-chain workflow	Broad platform ambitions spanning many workflows
Governance	State e-health program + vendor contract; 24-member industry consortium	Academic prototype lifecycle; bank consortium without common P&L
Integration	Overlays incumbent Oracle EHR / existing wholesale systems	Requires new workflows and multi-party adoption
Funding continuity	State-backed program; member dues tied to compliance value	Venture/consortium funding exhausted (we.trade insolvency, June 2022)
Vendor continuity	Long-running national vendor engagement	Vendor retreat: IBM unit downsized (reported 2021); platform end-of-support April 2023

VII. REFERENCE ARCHITECTURE FOR A PERMISSIONED NATIONAL HEALTH NETWORK

To make the preceding analysis actionable, this section distills the evidence of Sections IV–VI into a reference architecture for a blockchain-based health information system spanning a national hospital network, addressing the platform and consensus selection question directly; the architecture is summarized in Fig. 4.

Platform choice. A consortium-governed Hyperledger Fabric network (v2.5 LTS today, with a migration path to v3.0) is recommended. Fabric is selected because: (i) security and legal accountability membership is restricted to identified organizations through an MSP/PKI hierarchy (a national root CA with per-institution intermediate CAs), so every transaction is attributable to an accountable, statutorily responsible entity, which no public chain can offer; (ii) privacy channels segregate data domains (clinical care; consent and identity; pharmaceuticals and trials) and private data collections restrict bilateral visibility, with attribute-based access control enforced in chaincode; (iii) scalability and performance the execute-order-validate pipeline sustains thousands of transactions per second with sub-second latency in published benchmarks [40]–[42], and deterministic finality suits clinical authorization workflows; (iv) Fabric has no native cryptocurrency, avoiding token-regulatory exposure; and (v) hybrid off-chain storage keeps clinical payloads in encrypted repositories with only hashes on-chain, bounding chain growth (Section V.F).

Consensus choice. For ordering, SmartBFT (Byzantine fault tolerant, available in Fabric v3.0) is preferred when ordering nodes are operated by mutually independent

authorities, regional health authorities together with the ministry because BFT ordering removes single-operator trust and tolerates malicious or compromised orderers, the stronger trust model that a multi-stakeholder national network requires [43]. Where a single well-governed operator runs the ordering service, Raft is the pragmatic choice: lower message complexity and latency, with crash tolerance sufficient under strict administrative controls. The trade-off is explicit Raft assumes honest-but-fallible orderers, whereas SmartBFT assumes possible Byzantine behavior at moderate additional overhead; for national scale, four to seven ordering nodes would be geo-distributed across regions. Public Ethereum is rejected for the reasons set out in Section IV.C; Quorum or Besu with QBFT consensus, and Corda Enterprise, remain credible alternatives where Ethereum Virtual Machine tooling or bank-style bilateral flows dominate.

Identity, compliance, and sizing. Patient and clinician identity would integrate the national eID and, from end-2026, the EU Digital Identity Wallets mandated by eIDAS 2.0, via W3C decentralized identifiers and verifiable credentials [34], [35]. GDPR compliance uses the crypto-shredding and governed-redaction tooling of Section V.A, and crypto-agility for the post-quantum transition (FIPS 203/204/205; RSA/ECC deprecation expected around 2030–2035 [51], [52] is a design requirement, because immutable audit records outlive today's signatures. Sizing: the modeled 50-hospital network of Section IV.K requires roughly 250–500 chain-relevant transactions per second at peak comfortably within demonstrated permissioned-platform capacity and approximately two orders of magnitude above public-chain base layers, which is the quantitative core of the design justification.

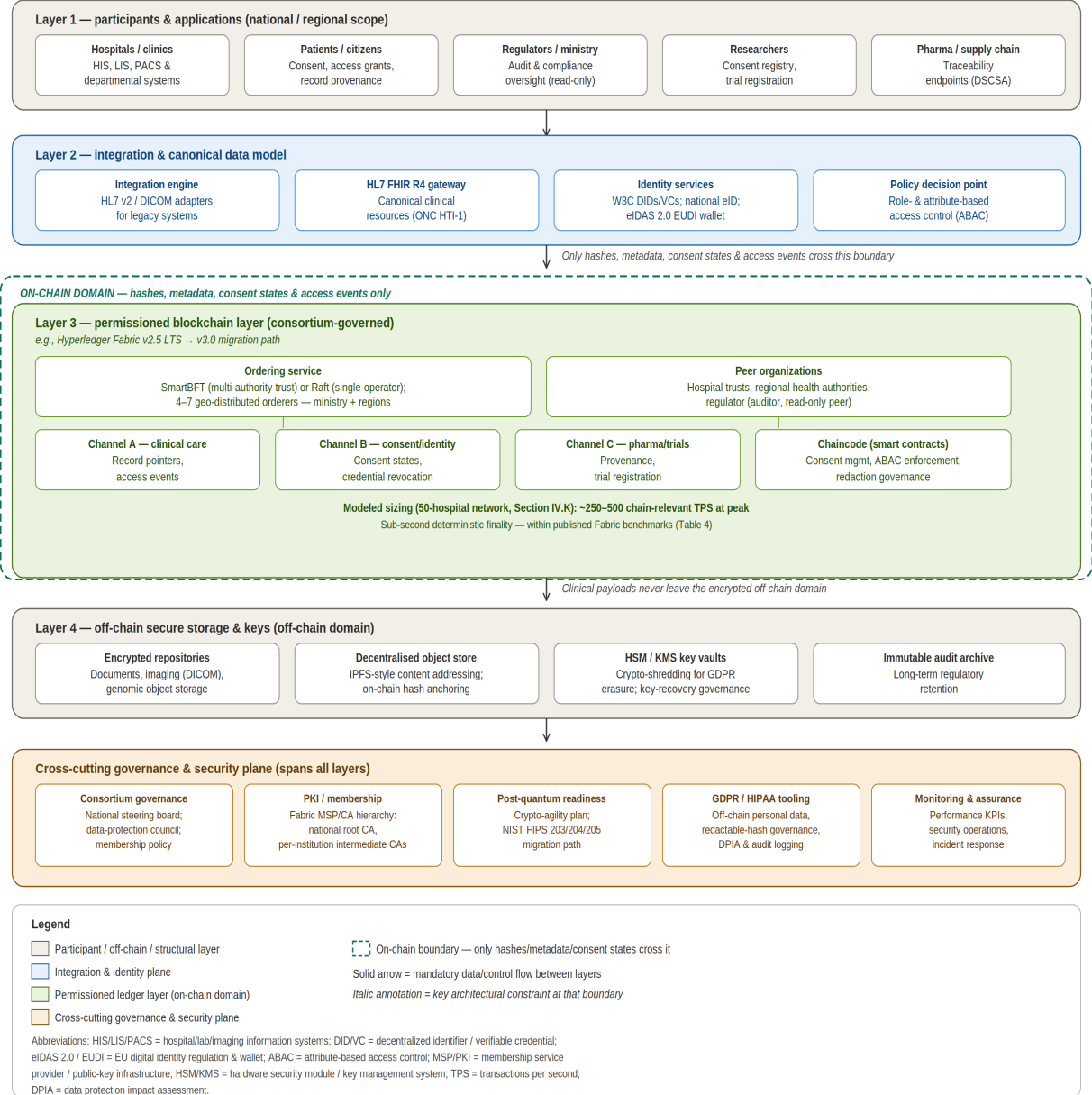


Fig. 4. Reference architecture for a permissioned national healthcare blockchain network: participant systems (Layer 1) connect via an HL7 FHIR R4 integration plane (Layer 2) to an on-chain permissioned ledger (Layer 3, dashed boundary) recording only hashes, metadata, and consent states, with clinical payloads held off-chain (Layer 4) under a cross-cutting governance plane. Platform, consensus, and sizing rationale are given in Section VII.

VIII. FUTURE RESEARCH DIRECTIONS AND EMERGING TECHNOLOGIES

The barriers analyzed in Section V are unlikely to be resolved by blockchain alone; they will be reshaped by convergence with adjacent technologies and by regulatory standardization. Based on the synthesized literature and recent developments in the field, six directions appear most consequential for healthcare data management.

A. Artificial intelligence and blockchain integration

Clinical AI generates its own accountability problems: model updates, training-data provenance, and decision logs are exactly the record types that benefit from immutable notarization. Convergence reviews published in 2024–2026 map a fast-growing literature in which blockchain serves as the audit and incentive layer for AI pipelines including federated learning, whose data locality (Section VI) pairs

naturally with on-chain aggregation certificates and consent audit [32], [53]. Research needs: quantification of on-chain-audit overhead on learning pipelines; standards for recording model provenance (hashes of weights, training cohorts, and evaluation reports) suitable for clinical governance.

B. Zero-knowledge proofs

ZKPs allow one party to prove a property of hidden data that a patient is enrolled in a trial, vaccinated, or over 18 without revealing the data itself; healthcare frameworks combining ZKPs with smart contracts and off-chain storage were demonstrated in 2025 [31], and STARK-based anonymous authentication has been proposed for cross-border health services. Rollup systems built on validity proofs also contribute to scalability (Section V.F). Research needs: proof-generation latency for clinical-grade claims; key management for patient-held credentials; standardization of claim vocabularies.

C. Confidential computing

Trusted execution environments (TEEs) permit computation over data that remains encrypted in use, inside hardware-attested enclaves. Hybrid architectures pairing TEE-based oracles with smart contracts simultaneously address confidentiality and the oracle problem (Section IV.E): the enclave attests both the code and the data source before results are notarized on-chain [46]. Research needs: side-channel robustness in hospital infrastructure; governance of attestation authorities; integration certification for medical devices.

D. Decentralized identity and verifiable credentials

The W3C Decentralized Identifiers specification reached Recommendation status in 2022 [35], and healthcare SSI applications patient-held consent credentials, professional licenses, immunization certificates have been systematically mapped [29], [54]. Regulatory tailwinds are decisive: Regulation (EU) 2024/1183 (eIDAS 2.0) obliges member states to offer EU Digital Identity Wallets by the end of 2026 [34], and the European Blockchain Services Infrastructure provides pan-European rails. Research needs: integrating professional registries with DID issuance; revocation at clinical latency; recovery of patient-controlled identifiers without recreating centralization.

E. Post-quantum cryptography

Medical records carry confidentiality expectations of many decades, exposing them to “harvest now, decrypt later” collection. NIST finalized the first post-quantum standards in August 2024 FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [51] with quantum-vulnerable RSA/ECC expected to be deprecated around 2030 and disallowed around 2035 [52]. Blockchains are peculiarly exposed: entries placed on an immutable chain cannot be retroactively re-signed, so crypto-agility hybrid classical/post-quantum signatures, hash-based schemes for long-lived audit records, and migration governance must be a design requirement for health ledgers, not an afterthought. Research needs: throughput and storage costs of PQC signatures on chain; migration paths for existing records.

F. Blockchain interoperability protocols

No single chain will serve all health ecosystems. Cross-chain messaging protocols (IBC, CCIP, and related designs) are maturing and are surveyed in the recent literature [47]; for healthcare, however, interoperability will more plausibly be achieved by pairing ledgers with canonical clinical standards HL7 FHIR R4, increasingly mandated by certification programs and legal-identity frameworks (eIDAS 2.0) than by chain-native bridges alone, with public infrastructure such as EBSI signaling institutional adoption of distributed ledgers for public services [34]. Research needs: secure FHIR-to-chain gateways; cross-chain consent portability; liability allocation across chains.

IX. CONCLUSION

This narrative review has examined the current state of blockchain technology as a data management solution in the healthcare sector. The reviewed literature consistently identifies blockchain’s core properties immutability, decentralization, cryptographic security, and transparent auditability as theoretically well-suited to address

longstanding challenges in health data management, including fragmented interoperability, limited patient control over personal data, and vulnerability to unauthorized access. Several real-world pilot applications, including Estonia’s national health data infrastructure and the FHIRChain project, provide preliminary evidence that blockchain-based systems are technically feasible in healthcare contexts. However, it is important to note that the majority of evidence currently available is conceptual or limited to small-scale pilots. Large-scale, controlled empirical studies comparing blockchain-based systems with existing technologies in terms of clinical outcomes, system performance, and cost-effectiveness remain largely absent from the literature. Claims about quality improvements and efficiency gains should therefore be understood as well-grounded hypotheses requiring rigorous validation rather than established facts.

The barriers documented in this review scalability constraints, regulatory conflicts, high implementation costs, and limited empirical validation are not merely technical problems but structural challenges that require coordinated responses from clinicians, technologists, regulators, and policymakers. Of the application areas examined, pharmaceutical supply chain authentication and clinical trial registration currently show the strongest alignment between blockchain’s technical properties and practical healthcare needs. Primary care interoperability represents a longer-term opportunity with significant potential, provided that interoperability standards and governance frameworks can be established. Blockchain adoption should not be pursued for its novelty, but selectively, in domains where its specific properties immutability, decentralization, and transparent auditability address limitations that existing technologies cannot resolve.

This review has several limitations that should be acknowledged. First, as a narrative review, it does not include a formal systematic search protocol or quantitative synthesis of results; findings therefore reflect the authors’ interpretive synthesis of the available literature rather than a statistically aggregated evidence base. Second, the paper does not present original empirical data, simulation results, or prototype measurements. No new blockchain system was designed, implemented, or tested as part of this work. The contribution is therefore theoretical and analytical: synthesizing the existing evidence base, critically identifying gaps between claimed and demonstrated benefits, and providing a structured comparative framework for decision-makers. Third, the literature search was restricted to English-language publications between January 2017 and January 2026, as documented in Section II, which may have excluded relevant non-English studies or work published outside this window. Fourth, the rapidly evolving nature of blockchain technology means that some technical constraints discussed (e.g., transaction throughput limits) may be partially addressed by developments occurring after the search period. These limitations reinforce the call for primary empirical research in this area.

Overcoming current obstacles and enabling the use of blockchain technology within healthcare will require targeted research efforts. Specifically, future studies should prioritise: (1) controlled pilot studies measuring the impact of blockchain-based EHR systems on clinical workflow efficiency and data accuracy, using quantitative performance metrics such as transaction throughput, query latency, and

system uptime; (2) comparative legal analyses assessing how different blockchain architectures can be designed to comply with GDPR and HIPAA without compromising data integrity; (3) health economic analyses quantifying the long-term cost-benefit ratio of blockchain adoption relative to cloud-based and centralized alternatives; and (4) user acceptance studies examining the readiness of healthcare professionals and patients to adopt blockchain-based systems. Progress on these research fronts will transform blockchain from a promising conceptual tool into a rigorously validated component of the future healthcare data ecosystem.

For healthcare organizations, the practical implications of this review can be summarized in four decision rules. First, adopt blockchain only where immutability, multi-party mistrust, or regulatory provenance requirements are themselves the problem drug traceability, trial registration, consent auditability and not as a general database replacement; for scalable storage and routine analytics, cloud and conventional architectures remain superior (Table V).

Second, prefer permissioned consortium architectures with deterministic finality, and design for data minimization from day one: personal data off-chain, hashes and consent states on-chain. Third, before committing capital, require vendors to publish measured key performance indicators sustained throughput under clinical workloads, authorization latency, storage growth, availability, and total cost of ownership against the organization's own transaction profile, since the literature offers almost no audited deployment data (Table I). Fourth, plan for regulatory and cryptographic change: GDPR-compliant erasure workflows, eIDAS 2.0-compatible identity, and crypto-agility against post-quantum migration timelines should be procurement requirements, not afterthoughts. Framed this way, blockchain is neither a paradigm shift that obsoletes existing systems nor a failed experiment, but a specialized notarial and coordination layer whose value is conditional and verifiable.

APPENDIX

TABLE VII. ABBREVIATIONS.

Abbreviation	Definition	Abbreviation	Definition
ABAC	Attribute-based access control	PBFT	Practical Byzantine Fault Tolerance
AI	Artificial intelligence	PHI	Protected health information
BFT	Byzantine fault tolerance	PHR	Personal health record
CFT	Crash fault tolerance	PoA	Proof of Authority
DID/VC	Decentralized identifier / verifiable credential	PoS	Proof of Stake
DICOM	Digital Imaging and Communications in Medicine	PoW	Proof of Work
DSCSA	Drug Supply Chain Security Act (United States)	PQC	Post-quantum cryptography
EBSI	European Blockchain Services Infrastructure	QbD	Quality by design
EHR	Electronic health record	QBFT	Quorum Byzantine Fault Tolerance
eIDAS 2.0	Regulation (EU) 2024/1183 on European digital identity	SGX	Software Guard Extensions (Intel TEE)
EUDI	European Union Digital Identity (Wallet)	SSI	Self-sovereign identity
FL	Federated learning	TEE	Trusted execution environment
FHIR	Fast Healthcare Interoperability Resources (HL7)	TPS	Transactions per second
GDPR	General Data Protection Regulation (EU)	ZKP	Zero-knowledge proof
HIPAA	Health Insurance Portability and Accountability Act (United States)	HSM/KMS	Hardware security module / key management system
HL7	Health Level Seven International	IPFS	InterPlanetary File System
IoT	Internet of Things	IT	Information technology
KSI	Keyless Signature Infrastructure	MSP	Membership Service Provider (Fabric)

REFERENCES

- [1] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare*, vol. 7, No. 2, Art. No. 56, 2019. <https://doi.org/10.3390/healthcare7020056>
- [2] U. Khalil, O. A. Malik, M. Uddin, and C. L. Chen, "A Comparative Analysis on Blockchain versus Centralized Authentication Architectures for IoT-Enabled Smart Devices in Smart Cities: A Comprehensive Review, Recent Advances, and Future Research Directions," *Sensors*, Vol. 22, no. 14, Art. No. 5168, 2022. <https://doi.org/10.3390/s22145168>
- [3] R. F. Ibrahim, Q. Abu Al-Haija, and A. Ahmad, "DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology," *Sensors*, Vol. 22, no. 18, Art. No. 6806, 2022. <https://doi.org/10.3390/s22186806>
- [4] P. Bagga, A. K. Das, V. Chamola, and M. Guizani, "Blockchain-envisioned access control for internet of things applications: A comprehensive survey and future directions," *Telecommun. Syst.*, vol. 81, No. 1, pp. 125--173, 2022. <https://doi.org/10.1007/s11235-022-00938-7>
- [5] P. Esmailzadeh, "Evolution of Health Information Sharing Between Health Care Organizations: Potential of Nonfungible Tokens," *Interact.*

- J. Med. Res., vol. 12, Art. N° e42685, 2023. <https://doi.org/10.2196/42685>
- [6] Q. Mamun, "Blockchain technology in the future of healthcare," *Smart Health*, vol. 23, Art. N° 100223, 2022. <https://doi.org/10.1016/j.smhl.2021.100223>
- [7] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences: A scoping review," *Int. J. Med. Inform.*, vol. 134, Art. N° 104040, 2020. <https://doi.org/10.1016/j.ijmedinf.2019.104040>
- [8] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Inform.*, vol. 142, Art. N° 104246, 2020. <https://doi.org/10.1016/j.ijmedinf.2020.104246>
- [9] A. McCauley, "Why big pharma is betting on blockchain," [Internet], *Harvard Business Review*. 2020. [cited 2023 Dec 10] Available from: <https://hbr.org/2020/05/why-big-pharma-is-betting-on-blockchain>
- [10] J. Priisalu and R. Ottis, "Personal control of privacy and data: Estonian experience," *Health Technol. (Berl)*, vol. 7, N°4, pp. 441--451, 2017. <https://doi.org/10.1007/s12553-017-0195-1>
- [11] J. Redman, "Estonian Health Records to Be Secured by Blockchain," *Bitcoin News*, 4 mars 4, 2016. <https://news.bitcoin.com/estonian-health-records-secured-by-blockchain/>
- [12] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and St. Rosenbloom, "FHIR-Chain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Comput. Struct. Biotechnol. Journal*, vol. 16, pp. 267--278, 2018. <https://doi.org/10.1016/j.csbj.2018.07.004>
- [13] WY Ng, TE Tan, PVH Movva, AHS Fang, KK Yeo, D Ho, FSS Foo, Z Xiao, K Sun, TY Wong, AT Sia, DSW Ting., "Blockchain applications in health care for COVID-19 and beyond: A systematic review," *Lancet Digit. Heal.*, vol. 3, N° 12 pp. e819--e829, 2021. [https://doi.org/10.1016/s2589-7500\(21\)00210-7](https://doi.org/10.1016/s2589-7500(21)00210-7)
- [14] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain Personal Health Records: Systematic Review," *J. Med. Internet Res.*, vol. 23, N°4, Art. N° e25094, 2021. <https://doi.org/10.2196/25094>
- [15] A. A. M. M. Qambar, "A Blockchain Based Policy Framework for the Management of Electronic Health Record (EHRs)," 2022. UAEU Theses (1002). https://scholarworks.uaeu.ac.ae/all_theses/1002
- [16] J. A. Oliva, "Adaptation of primary care centers to virtuality", (Adaptación de los centros de atención primaria a la virtualidad), *Primary Care*, vol. 3, Art. N° 100119, 2021. <https://doi.org/10.1016/j.appr.2021.100119>
- [17] T Rathod, NK Jadav, MD Alshehri, S Tanwar, R Sharma, R-A Felseghi, MS Raboaca. Blockchain for Future Wireless Networks: A Decade Survey. *Sensors*. Vol. 22, N° 11, Art. N° 4182, 2022. <https://doi.org/10.3390/s22114182>
- [18] C. Alvarez-Romero, A. Martínez-García, M. Bernabeu-Wittel, and C. L. Parra-Calderón, "Health data hubs: An analysis of existing data governance features for research," *Health Res. Policy Syst.*, vol. 21, art Numb. 70, Jul. 2023. <https://doi.org/10.1186/s12961-023-01026-1>
- [19] J.W.T.M. de Kok, M.Á.A. de la Hoz, Y. de Jong, *et al.* A guide to sharing open healthcare data under the General Data Protection Regulation. *Sci Data* Vol. 10, Art. N° 404, 2023. <https://doi.org/10.1038/s41597-023-02256-2>
- [20] D. Roosan, Y. Wu, V. Tatla, Y. Li, A. Kugler, J. Chok, MR. Roosan, "Framework to enable pharmacist access to health care data using Blockchain technology and artificial intelligence," *J. Amer. Pharm. Assoc.*, vol. 62, N° 4, pp. 1124--1132, 2022. <https://doi.org/10.1016/j.japh.2022.02.018>
- [21] L. Leitsalu, T. Haller, T. Esko, M. L. Tammesoo, H. Alavere, H. Snieder, M. Perola, P. C. Ng, R. Mägi, L. Milani, K. Fischer, and A. Metspalu, "Cohort Profile: Estonian Biobank of the Estonian Genome Center, University of Tartu," *Int. J. Epidemiol.*, vol. 44, N°4, pp. 1137--1147, 2015. <https://doi.org/10.1093/ije/dyt268>
- [22] M. M. Sharif and F. Ghodoosi, "The Ethics of Blockchain in Organizations," *J. Bus. Ethics*, vol. 178, N°4, pp. 1009--1025, 2022. <https://doi.org/10.1007/s10551-022-05058-5>
- [23] A. L. A. Fonsêca, I. M. P. Barbalho, F. Fernandes, E. Arrais Júnior, D. A. P. Nagem, P. H. Cardoso, N. V. R. Veras, F. L. O. Farias, A. R. Lindquist, J. P. Q. dos Santos, A. H. F. Morais, J. Henriques, M. Lucena, and R. A. M. Valentim, "Blockchain in Health Information Systems: A Systematic Review," *Int. J. Environ. Res. Public Health*, vol. 21, N°11, p. 1512, 2024. <https://doi.org/10.3390/ijerph21111512>
- [24] S. Cihan, N. Yilmaz, A. Ozsoy, et al., "A systematic review of the blockchain application in healthcare research domain: toward a unified conceptual model," *Med. Biol. Eng. Comput.*, vol. 63, pp. 1319--1342, 2025. <https://doi.org/10.1007/s11517-024-03274-x>
- [25] M. S. B. Kasyapa and C. Vanmathi, "Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies," *Front. Digit. Health*, vol. 6, art Numb. 1359858, 2024. <https://doi.org/10.3389/fdgth.2024.1359858>
- [26] F. Z. Chentouf, M. E. A. Hassoun, and S. Bouchkaren, "Electronic Health Record Systems Based on Blockchain: A Comprehensive Survey," *Applied Sciences*, vol. 16, N°8, Art. Num. 3768, 2026. <https://doi.org/10.3390/app16083768>
- [27] A. Pokharel and S. Kathayat, "Blockchain-Enabled Self-Sovereign Identity Applications in Health Care: Scoping Review," *J. Med. Internet Res.*, vol. 28, e89574, 2026. <https://doi.org/10.2196/89574>
- [28] S. Xu, J. Ning, X. Li, J. Yuan, X. Huang, and R. H. Deng, "A Privacy-Preserving and Redactable Healthcare Blockchain System," *IEEE Trans. Serv. Comput.*, vol. 17, N°2, pp. 364--377, 2024. <https://doi.org/10.1109/TSC.2024.3356595>
- [29] M. Madine, K. Salah, R. Jayaraman, and I. Yaqoob, "Zero-knowledge proofs for anonymous authentication of patients on public and private blockchains," *Array*, vol. 28, e.100590, 2025. <https://doi.org/10.1016/j.array.2025.100590>
- [30] J. Liu and X. Hu, "Blockchain meets AI in healthcare: a review of convergent technologies for digital health transformation," *Front. Blockchain*, vol. 9, e.1766092, 2026. <https://doi.org/10.3389/fbloc.2026.1766092>
- [31] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain--or--rewriting history in bitcoin and friends," in 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 2017, pp. 111--126. <https://doi.org/10.1109/EuroSP.2017.37>
- [32] N. Choi and H. Kim, "Technological Convergence of Blockchain and Artificial Intelligence: A Review and Challenges," *Electronics*, vol. 14, N°1, Art Numb.84, 2025. <https://doi.org/10.3390/electronics14010084>
- [33] R. A. Pava-Díaz, J. Gil-Ruiz, and D. A. López-Sarmiento, "Self-sovereign identity on the blockchain: Contextual analysis and quantification of SSI principles implementation," *Front. Blockchain*, vol. 7, e. 1443362, 2024. <https://doi.org/10.3389/fbloc.2024.1443362>
- [34] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Milwaukee, WI, USA, 2018, pp. 264--276. <https://doi.org/10.1109/MASCOTS.2018.00034>
- [35] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference (EuroSys '18), Porto, Portugal, April 23 - 26, 2018, Art. no. 30, pp. 1-15. <https://doi.org/10.1145/3190508.3190538>
- [36] D. Enyeart, "Benchmarking Hyperledger Fabric 2.5 Performance," *LF Decentralized Trust Blog*, Feb. 16, 2023. [Online]. Available: <https://www.lfdecentralizedtrust.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance>
- [37] LF Decentralized Trust. "Version 3.0 of Hyperledger Fabric, an LF Decentralized Trust Project, Now Available". september 16, 2024. <https://www.lfdecentralizedtrust.org/announcements/version-3.0-of-hyperledger-fabric-an-lf-decentralized-trust-project-now-available>
- [38] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The Energy Consumption of Blockchain Technology: Beyond Myth," *Bus. Inf. Syst. Eng.*, vol. 62, N°6, pp. 599--608, 2020. <https://doi.org/10.1007/s12599-020-00656-x>
- [39] N. Hinov, "Non-Compensatory Security and Utility Gates for Blockchain Lifecycle Assessment: Framework Development and an Operational-Energy Application to the Ethereum Merge," *Appl. Sci.*, vol. 16, N°15, e.7820, 2026. <https://doi.org/10.3390/app16157820>
- [40] O. Gillot, W. J. Buchanan, and M. G. Tehrani, "Energy Consumption of Post-Quantum Cryptography on Constrained and General-Purpose Architectures," *Cryptography*, vol. 10, N°4, e.55, 2026. <https://doi.org/10.3390/cryptography10040055>

- [41] D. Moody, R. Perlner, A. Regenscheid, A. Robinson, and D. Cooper, "Transition to post-quantum cryptography standards," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Internal Report 8547 (Initial Public Draft), Nov. 2024. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8547.ipd>
- [42] A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, F. A. Marino, and S. Ranise, "The eIDAS regulation: a survey of technological trends for European electronic identity schemes," *Appl. Sci.*, vol. 12, N°24, p. art numb. 12679, 2022. <https://doi.org/10.3390/app122412679>
- [43] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, Eds., "Decentralized Identifiers (DIDs) v1.0," *W3C Recommendation*, World Wide Web Consortium, Jul. 19, 2022. [Online]. Available: <https://www.w3.org/TR/did/>
- [44] C. Baethge, S. Goldbeck-Wood, and S. Mertens, "SANRA—a scale for the quality assessment of narrative review articles," *Res. Integr. Peer Rev.*, vol. 4, N°1, art. numb. 5, 2019. <https://doi.org/10.1186/s41073-019-0064-8>
- [45] R. Ferrari, "Writing narrative style literature reviews," *Med. Writ.*, vol. 24, N°4, pp. 230--235, 2015. <https://doi.org/10.1179/2047480615Z.000000000329>
- [46] Q. N. Hong, S. Fàbregues, G. Bartlett, F. Boardman, M. Cargo, P. Dagenais, M.-P. Gagnon, F. Griffiths, B. Nicolau, A. O'Cathain, M. Rousseau, and I. Vedel, P. Pluye, "The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers," *Educ. Inf.*, vol. 34, N°4, pp. 285--291, 2018. <https://doi.org/10.3233/EFI-180221>
- [47] M. Sample, "MediLedger DSCSA Pilot Project," Chronicled / MediLedger Network, San Francisco, CA, USA, Tech. Rep., 2024.
- [48] G. Bhavsar, "Exception management in pharmaceutical industries to attain DSCSA compliance," *Int. J. Drug Reg. Affairs*, vol. 13, no. 1, pp. 24--27, 2025, <https://doi.org/10.22270/ijdra.v13i1.738>
- [49] L. Wang, X. Liu, W. Shao, C. Guan, Q. Huang, S. Xu, and S. Zhang, "A Blockchain-Based Privacy-Preserving Healthcare Data Sharing Scheme for Incremental Updates," *Symmetry*, vol. 16, N°1, art. numb. 89, 2024. <https://doi.org/10.3390/sym16010089>
- [50] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152--167, 2022. <https://doi.org/10.1016/j.jpdc.2022.03.009>
- [51] E. Wragg, "we.trade calls it quits after running out of cash," *Global Trade Review (GTR)*, Jun. 6, 2022. [Online]. Available: <https://www.gtreview.com/news/top-stories/we-trade-calls-it-quits-after-running-out-of-cash/>
- [52] I. Allison, "IBM blockchain is a 'shell of its former self' after revenue misses, job cuts: Sources," *CoinDesk*, Feb. 1, 2021. [Online]. Available: <https://www.coindesk.com/business/2021/02/01/ibm-blockchain-is-a-shell-of-its-former-self-after-revenue-misses-job-cuts-sources/>
- [53] R. Clarke, L. McGuire, M. Baza, A. Rasheed, and M. Alsabaan, "Online voting scheme using IBM cloud-based hyperledger fabric with privacy-preservation," *Appl. Sci.*, vol. 13, N°13, art. Numb. 7905, 2023. <https://doi.org/10.3390/app13137905>
- [54] A. Bigiotti, L. Mostarda, A. Navarra, A. Pinna, D. Sestili, R. Tonelli, and M. Vaccargiu, "Blockchain Agnostic Protocols: An Analysis of the State of the Art," *ACM Comput. Surv.*, vol. 58, N°2, Art. N°30, pp. 1--36, 2026. <https://doi.org/10.1145/3758089>