Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Patient Sovereignty in the Digital Age: A Blockchain-Based Framework for Controllable Health Information System

Karan B Patel
University of Texas at Dallas, USA
Corresponding Author: Karan B Patel, **E-mail**: karanpatel@gmail.com

| ABSTRACT
The digitization of health records has created significant challenges, including data fragmentation, security vulnerabilities, and limited patient control over sensitive information. Blockchain technology provides a transformative foundation for patient-controlled health information systems through its decentralization, immutability, and cryptographic security features. This framework shifts control from institutions to patients by implementing a hybrid architecture that stores consent logs on-chain while securing protected health information off-chain. Smart contracts automate patient consent and access control, while standardized healthcare data ensures semantic interoperability. Real-world implementations demonstrate substantial improvements in security, efficiency, and patient engagement. Despite implementation challenges, including initial costs and technical complexity, blockchain-based systems provide significant economic benefits through reduced administrative overhead and security breach mitigation. Addressing ethical considerations such as regulatory compliance and digital equity is essential for these systems to advance healthcare access rather than exacerbating existing inequalities. The transition to patient-sovereign health information represents not only a technological advancement but a fundamental transformation of healthcare information management that empowers patients while improving system efficiency and security.

| KEYWORDS

Blockchain Technology, Patient Sovereignty, Healthcare Interoperability, Smart Contracts, Data Security.

| ARTICLE INFORMATION

ACCEPTED: 23 September 2025 **PUBLISHED:** 28 September 2025 **DOI:** 10.32996/jcsts.2025.7.10.8

1. Introduction: The Evolution and Limitations of Digital Health Records

The evolution of health information technology (HIT) represents a journey from paper-based records to widespread adoption of electronic health records (EHRs). This digital transformation promised to streamline workflows, reduce medical errors, and improve care coordination. However, the current landscape is dominated by centralized, provider-controlled systems that have inadvertently created new challenges. According to Chen and Esmaeilzadeh (2023), despite the availability of various health information exchange (HIE) methods, hospitals face significant barriers to effective information sharing, with organizational and operational challenges limiting the potential benefits of digital health records [1].

A fundamental issue in contemporary healthcare information systems is the fragmentation of patient medical histories across disparate, non-integrated EHR systems operated by various providers. This fragmentation creates data silos that inhibit physicians' access to complete and accurate records, leading to redundant tests and potential gaps in care. Chen and Esmaeilzadeh found that while hospitals have adopted various HIE methods, many still struggle with effective implementation, creating inefficiencies in healthcare delivery and administrative processes [1].

Patients, the true owners of their health data, have become passive subjects in its management, with limited ability to view, share, or track their information. This institution-centered model fundamentally conflicts with increasing demands for patient engagement and data ownership. Additionally, centralized data repositories have become high-value targets for cybercriminals.

According to the HIPAA Journal's healthcare data breach statistics, the healthcare sector experienced 712 major data breaches in 2021, affecting more than 45 million patients. Hacking and IT incidents were responsible for 74% of all breached records, with the average breach costing $9.23 million per incident. Recovery periods from detection to containment often extend to several months [2].

The purpose of this paper is to present blockchain technology as a viable and essential architectural foundation for patient-controlled health information systems. We argue that the inherent features of blockchain directly address the key vulnerabilities of today's centralized EHR systems and create a framework for genuine patient sovereignty over health data.

Challenge Category	Key Issues	Impact
Interoperability	Non-standardized data formats	Fragmented patient records
	Limited information exchange	Duplicate testing and procedures
	Provider-specific information silos	Incomplete clinical decision-making
Security	Centralized data repositories	High-value targets for cyberattacks
	Limited access controls	Unauthorized data exposure
	Extensive breach recovery periods	Prolonged vulnerability windows
Patient Control	Minimal access transparency	Limited visibility into record usage
	Few sharing consent options	Inability to control information flow
	Provider-centric governance	Misalignment with patient ownership
Operational Efficiency	Manual authorization processes	Delayed care delivery
	Redundant data entry	Administrative burden on providers
	Complex reconciliation workflows	Resource diversion from patient care

Table 1: Current Healthcare Information System Challenges (References 1-2)

2. Blockchain as an Enabler of Patient Sovereignty

Blockchain technology functions as a distributed, immutable digital ledger that records transactions securely and transparently across a peer network. Each transaction is grouped into a "block" that is cryptographically linked to the previous one, forming a "chain." This structure makes data tamper-proof; to alter a record, all subsequent blocks would need to be modified and consensus gained from the network, which is practically impossible. Gordon and Catalini (2018) have extensively examined blockchain's potential in healthcare, highlighting its ability to facilitate the transition to patient-driven interoperability and data sovereignty [3].

Gordon and Catalini describe how blockchain applied to healthcare facilitates a paradigm shift from an institution-centered to a patient-centric model. In a blockchain-based system, patients are empowered with control over their own health records. They hold the cryptographic keys that grant access, allowing them to decide who can view their data, for what purpose, and for how long. The authors note that patient-controlled access systems can significantly improve compliance compared to traditional methods, while potentially reducing unauthorized record access attempts and decreasing the time required to validate access requests [3].

Healthcare information system architecture has evolved significantly over recent decades. Early systems were siloed within specific departments such as radiology or pharmacy. The subsequent era saw the rise of comprehensive, monolithic EHRs that consolidated data within individual institutions but largely created impenetrable silos that hindered data exchange between different organizations. Research published in Blockchain in Healthcare Today has explored various blockchain implementations that aim to address these interoperability challenges through distributed ledger technologies and smart contracts [4].

Component	Function	Benefits
On-Chain Elements	Cryptographic record hashes	Tamper-evident verification
	Access logs and permissions	Complete audit trail
	Consent documentation	Immutable authorization history
	Smart contracts	Automated access enforcement
Off-Chain Storage	Protected health information	Cost-effective data management
	Medical imaging files	Scalable information architecture
	Clinical documentation	Regulatory compliance
	Encrypted patient data	Quantum-resistant security
Patient Control Mechanisms	Cryptographic master keys	Sovereign access management
	Granular permission settings	Context-specific authorization
	Time-limited access grants	Temporal control boundaries
	Purpose-specific authorizations	Data minimization enforcement
Interoperability Features	FHIR integration	Standardized data exchange
	API-based communication	Modern system connectivity
	Cross-platform compatibility	Seamless information sharing
	Semantic data mapping	Meaningful clinical exchange

Table 2: Blockchain-Based Healthcare Architecture Components (3-4)

3. Technical Architecture for Patient-Controlled Health Information Systems

A robust and scalable blockchain-based health information system requires a sophisticated architecture that balances security, privacy, and interoperability. This is typically achieved through a hybrid model that incorporates on-chain and off-chain components, smart contracts for logic, and data standards for communication. Zhang et al. (2018) proposed FHIRChain, a blockchain-based architecture for securely sharing clinical data using the FHIR standard. Their research demonstrated significant advantages in security and performance, with their prototype implementation showing the feasibility of using blockchain for access control while maintaining healthcare data privacy [5].

3.1 Hybrid On-Chain/Off-Chain Architecture

Storing entire health records directly on a blockchain is impractical due to the large size of medical data, associated costs, and privacy concerns. Zhang et al. propose a more effective approach using a hybrid architecture where the blockchain serves as a secure and immutable ledger for metadata, access logs, and consent pointers, while the actual Protected Health Information (PHI) is stored off-chain. Their FHIRChain implementation addresses key challenges in healthcare information exchange, including access control, secure data sharing, and patient privacy, while leveraging the FHIR standard for interoperability [5].

Zhang et al.'s implementation demonstrated that on-chain storage should be limited to access control information and data pointers, while maintaining PHI in secure off-chain repositories. This approach significantly reduces blockchain storage requirements while still providing the security benefits of distributed ledger technology. Their architecture enables secure sharing of clinical data without exposing sensitive information on the blockchain itself, addressing both technical and regulatory requirements for healthcare data management [5].

3.2 Smart Contracts for Automated Consent Management

Smart contracts—self-executing agreements with terms written directly into code—are a cornerstone of a patient-controlled health information system. Hylock and Zeng (2019) developed and evaluated HealthChain, a blockchain framework for patient-centered health records that implements smart contracts for consent management. Their research demonstrated advantages over traditional methods, with their proof-of-concept implementation showing how smart contracts can automate access control based on patient consent [6].

Hylock and Zeng's HealthChain framework uses Ethereum-based smart contracts to manage patient consent and data access. Their implementation addresses key challenges in healthcare information exchange, including patient privacy, data security, and interoperability. The system enables patients to define granular permissions for their health data, allowing them to specify who can access specific information and under what conditions. The researchers' evaluation showed that their blockchain-based approach could potentially improve both security and efficiency compared to traditional healthcare information systems [6].

4. Real-World Implementation and Use Cases

While still an emerging area, blockchain applications in healthcare are moving beyond theory to real-world pilots and implementations. Mettler (2016) was among the first to describe how blockchain technology could revolutionize healthcare information systems. His paper outlined potential use cases, including electronic medical records, drug supply chain, biomedical research, and health insurance claims processing, while acknowledging the early stage of blockchain adoption in healthcare [7].

Mettler highlighted Estonia's e-health system as an early example of blockchain-adjacent technology in healthcare. While not a pure blockchain implementation, Estonia's system uses related cryptographic techniques to secure health records and has been considered a precursor to more comprehensive blockchain-based health information systems. Mettler noted that true blockchain implementations in healthcare were still at a nascent stage in 2016, with significant technical and regulatory challenges to overcome [7].

According to market analysis by Grand View Research, the global blockchain technology in healthcare market was valued at approximately $2.37 billion in 2021 and is projected to grow at a compound annual growth rate (CAGR) of 68.1% from 2022 to 2030. Their analysis indicates that electronic health record management accounts for the largest application segment, followed by drug supply chain management and clinical trials. The report identifies North America as the leading regional market, with Asia Pacific expected to see the fastest growth during the forecast period [8].

Implementation Type	Application Focus	Potential Benefits
National Health Records	Population-level health data	Comprehensive health information access
	Citizen-controlled access	Enhanced privacy protection
	Identity verification	Improved authentication
	Health information exchange	Cross-institutional data sharing
Clinical Data Sharing	Medical research	Secure anonymized data access
	Patient consent management	Transparent authorization
	Provider collaboration	Improved care coordination
	Research data integrity	Verifiable research outcomes
Health Wallets	Patient-centered record access	Self-sovereign health information
	Personal health management	Improved health literacy
	Clinical trial participation	Enhanced research participation
	Cross-provider data sharing	Continuous care records
Supply Chain	Pharmaceutical tracking	Counterfeit prevention
	Drug provenance	Enhanced medication safety
	Supply chain transparency	Improved inventory management
	Stakeholder verification	Regulatory compliance
Claims Processing	Insurance verification	Reduced administrative burden
	Automated adjudication	Faster reimbursement
	Fraud prevention	Cost savings
	Payment transparency	Improved financial planning

Table 3: Emerging Blockchain Healthcare Implementations (References 7-8)

5. Economic, Social, and Ethical Implications

5.1 Economic and Operational Effects

The transition to a blockchain-based health information system carries significant economic implications. According to Vazirani et al. (2020), blockchain implementation in healthcare has the potential to generate cost savings through streamlined processes, reduced administrative overhead, and enhanced security measures. Their analysis identifies several potential economic benefits, including reduced administrative costs, decreased data breach expenses, and improved operational efficiency [9].

Vazirani et al. also highlight significant implementation barriers for blockchain in healthcare. These include substantial initial costs, the need for specialized expertise, integration challenges with legacy systems, and extended implementation timelines. They note that achieving interoperability with existing EHR systems requires considerable development effort, potentially extending project timelines beyond initial estimates. Despite these challenges, the authors suggest that long-term benefits could outweigh initial costs, with potential for significant return on investment as the technology matures [9].

5.2 Social and Ethical Considerations

There are important social and ethical dimensions to empowering patients to control their data. Hasselgren et al. (2020) conducted a comprehensive scoping review of blockchain applications in healthcare and health sciences, identifying both opportunities and challenges in the social and ethical domains. Their review found that blockchain could potentially improve patient engagement and trust in healthcare providers by giving patients greater control over their health information [10].

Hasselgren et al. identified several ethical challenges requiring attention in blockchain healthcare implementations. These include concerns about the "right to be forgotten" under privacy regulations, which conflict with blockchain's immutability; digital equity issues that could exacerbate healthcare disparities; and challenges related to patient consent in complex technological systems. The authors emphasize the need for thoughtful implementation strategies that address these ethical considerations to ensure that blockchain technologies advance health equity rather than reinforcing existing inequalities [10].

Dimension	Benefits	Challenges
Economic Advantages	Reduced administrative overhead	High initial implementation costs
	Decreased data breach expenses	Specialized expertise requirements
	Improved revenue cycle efficiency	Extended integration timelines
	Fraud reduction	Legacy system compatibility issues
	Streamlined claims processing	Ongoing maintenance expenses
Operational Effects	Accelerated access authorization	Technical complexity management
	Enhanced system availability	Workflow redesign requirements
	Optimized clinical documentation	Staff training investments
	Automated compliance monitoring	Change management demands
	Improved data integrity	Governance structure adaptation
Social Impact	Increased patient empowerment	Digital literacy barriers
	Enhanced provider trust	Socioeconomic access disparities
	Improved preventive care engagement	Geographic connectivity challenges
	Greater willingness to share health data	Age-related technology gaps
	More active healthcare participation	Cultural adoption variations
Ethical Considerations	Privacy protection enhancement	Regulatory "right to be forgotten" compliance
	Transparent data usage	Equitable access concerns
	Patient-directed research participation	Technology accessibility challenges
	Informed consent improvement	Implementation of equity requirements
	Autonomy reinforcement	Potential digital divide exacerbation

Table 4: Economic and Social Implications of Blockchain Healthcare Systems (References 9-10)

6. Conclusion

The transition toward blockchain-based health information systems represents a fundamental paradigm shift in healthcare data management, moving from institutional control to patient sovereignty. By combining the immutable security of distributed blockchain technology with automated smart contracts and standardized data exchange protocols, these systems address key vulnerabilities of traditional electronic health records while empowering patients with unprecedented control over their sensitive information. Real-world implementations have demonstrated notable improvements in security metrics, operational efficiency, and patient engagement, providing significant economic benefits despite initial implementation barriers of cost and technical complexity. To realize the full potential of this technological transformation, healthcare stakeholders must carefully address ethical considerations, including regulatory compliance and digital equity, through inclusive implementation strategies that ensure these systems advance healthcare access rather than exacerbating existing inequalities. This evolution toward patient-

sovereign health information represents not only a technological advancement but also an ethical imperative to restore data autonomy to patients while creating a more secure, efficient, and equitable healthcare ecosystem.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Anton H, et al., (n.d) Blockchain in healthcare and health sciences—A scoping review. ScienceDirect, https://www.sciencedirect.com/science/article/pii/S138650561930526X
[2] Anuraag A. V, et al., (2020) Blockchain vehicles for efficient Medical Record management, NPJ Digital Medicine, 2020. https://www.nature.com/articles/s41746-019-0211-0
[3] Blockchain in Healthcare Today, (2018) Blockchain in Healthcare Today Platform Approaches *Journal,* 2018. https://blockchainhealthcaretoday.com/index.php/journal
[4] Grand View Research. (2023). Blockchain Technology In Healthcare Market Size, Share & Trends Analysis Report By Network Type (Private, Public), By End-use (Providers, Payers), By Application, By Region, And Segment Forecasts, 2024 - 2030., https://www.grandviewresearch.com/industry-analysis/blockchain-technology-healthcare-market
[5] Matthias M, (2016) Blockchain technology in healthcare: The revolution starts here. IEEE, 2016. https://ieeexplore.ieee.org/document/7749510
[6] Min C, and Pouyan E, (2023) Adoption and use of various health information exchange methods for sending inside health information in US hospitals. ScienceDirect, 2023. https://www.sciencedirect.com/science/article/abs/pii/S1386505623001740
[7] Peng Z, et al., (2018) FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data." ScienceDirect, 2018. https://www.sciencedirect.com/science/article/pii/S2001037018300370
[8] Ray H H, and Xiaoming Z, (2019) A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study, PubMed, 2019. https://pubmed.ncbi.nlm.nih.gov/31471959/
[9] Steve A. (2023) Healthcare Data Breach Statistics. HIPAA Journal, 2023. https://www.hipaajournal.com/healthcare-data-breach-statistics/
[10] William J. G, and Christian C (2018) Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. ScienceDirect, 2018. https://www.sciencedirect.com/science/article/pii/S200103701830028X