International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 2, Issue 8, 2023
DOI: https://doi.org/10.38124/ijsrmt.v2i8.723

Blockchain for Healthcare Cybersecurity: Opportunities and Vulnerabilities in Decentralized Health Data Systems

Tolulope Awobeku[1]

[1] Department of Technology, Eastern Illinois University, USA

Publication Date 2023/08/30

Abstract

The integration of blockchain technology into healthcare cybersecurity represents a paradigm shift toward decentralized health data management systems. This study examines the multifaceted opportunities and inherent vulnerabilities associated with blockchain implementation in healthcare environments within the United States. Through comprehensive analysis of existing literature and emerging technological frameworks, this research identifies critical security enhancements while acknowledging potential exploitation vectors. The findings reveal that while blockchain offers unprecedented data integrity and access control mechanisms, implementation challenges persist in areas of scalability, regulatory compliance, and interoperability with legacy healthcare systems.

Keywords: *Blockchain, Healthcare Cybersecurity, Decentralized Systems, Health Data Security, Electronic Health Records.*

I. INTRODUCTION

Healthcare cybersecurity has emerged as a paramount concern in the United States, where the frequency and severity of data breaches have escalated dramatically. Reports indicate a 93 percent surge in healthcare data breaches over the past five years, exposing vulnerabilities within the traditional centralized frameworks that underpin health data management (Richard, 2024). These centralized systems often characterized by monolithic databases and administrative bottlenecks have proven inadequate in countering increasingly sophisticated cyber-attacks, including advanced persistent threats and ransomware campaigns.

In response, blockchain technology has gained attention for its capacity to fundamentally transform cybersecurity architecture through decentralization, immutability, and enhanced transparency (Fonsêca et al., 2024; Pokharel et al., 2024). These properties once relegated to cryptocurrency applications now present compelling prospects for healthcare data security. Decentralization mitigates single points of failure by distributing trust across a network of nodes, while cryptographic hashes immediately reveal any unauthorized modification (Wang et al., 2018; Richard, 2024). Moreover, blockchain enables fine-grained auditability of access events and data changes, aligning well with compliance requirements such as HIPAA.

Despite these advantages, healthcare poses a unique combination of demands: stringent data privacy protections, interoperable exchange among diverse stakeholders, and rigorous regulatory oversight. As Fonsêca et al. (2024) note, implementing blockchain in this domain necessitates a nuanced approach that addresses scalability, key management, and integration with legacy systems. This analysis explores both the potential and vulnerabilities of deploying blockchain-enabled decentralized health systems, framing a perspective for secure, compliant, and resilient healthcare infrastructure in the United States.

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

➢ *Current State of Healthcare Cybersecurity*

The digitization of healthcare has broadened the attack surface, exposing both hospital networks and patient portals to a growing array of threats. Centralized Electronic Health Record (EHR) systems are particularly vulnerable to mass data extraction and insider threats, as their centralized architecture allows attackers to exploit a single breach point (Abu-Elezz et al., 2020). To improve

Awobeku , T. (2025). Blockchain for Healthcare Cybersecurity: Opportunities and Vulnerabilities in Decentralized Health Data Systems. *International Journal of Scientific Research and Modern Technology*, *2*(8), 43–53. https://doi.org/10.38124/ijsrmt.v2i8.723

resilience, cybersecurity professionals are increasingly leveraging advanced analytics within traditional perimeter defenses. Mohamed (2024b) highlights the significance of machine learning algorithms in enhancing threat detection through anomaly-based monitoring, predictive modeling, and adaptive response systems.

Nevertheless, these AI-driven systems must reconcile with healthcare's sensitive data context and privacy regulations. Thawait (2024) systematically reviewed the integration of machine learning in cybersecurity and emphasized the critical need for data protection frameworks, particularly in healthcare environments where data misuse can lead to legal penalties and loss of trust. Additionally, Alamri et al. (2022) propose identity-based risk management frameworks to strengthen IoT devices within healthcare, addressing the pervasive connectivity inherent in modern clinics and remote monitoring systems.

Despite these advancements, centralized cybersecurity solutions remain reactive and fragmented. They often lack interoperability, struggle with horizontal threat visibility, and remain dependent on siloed logs that limit visibility across healthcare ecosystems (Mohamed, 2024b; Thawait, 2024). Consequently, a foundational rethinking of system design moving from centralized control to distributed architectures appears increasingly essential.

- *Blockchain Technology Fundamentals*

Blockchain technology introduces a distributed consensus mechanism whereby all participating nodes validate transactions through cryptographic commitment and agreed-upon rules, ensuring data integrity and resistance to tampering (Wang et al., 2018). In the healthcare context, this translates into a ledger where each update to a patient's record is immutably recorded and linked, enabling retrospective audits and trust across care teams.

Hash functions create a secure fingerprint of data entries, ensuring that even minor changes trigger detectable discrepancies (Richard, 2024). This level of integrity is particularly valuable in reporting adverse events, recording clinical trials, and supporting medical forensics. Additionally, blockchain's decentralized nature inherently eliminates single points of failure, reducing reliance on centralized IT infrastructure that has historically been compromised with alarming regularity (Pokharel et al., 2024; Richard, 2024).

Extensive academic investigation supports blockchain integration in healthcare. Roehrs et al. (2017) introduced OmniPHR, a distributed architecture enabling interoperability of personal health records through blockchain technology. Fonsêca et al. (2024) performed a comprehensive review, identifying blockchain as a promising means to reconcile privacy, security, and interoperability provided that deployment includes rigorous key management, robust system integration, and smart contract security vetting. Pokharel et al. (2024) further developed BlockHealthSecure, demonstrating how blockchain combined with existing cybersecurity measures can create resilient post-pandemic health systems.

Additional research explores encryption-enhanced blockchain protocols. Kunal et al. (2024) proposed a blockchain-driven protocol that integrates advanced encryption standards to preserve patient confidentiality while allowing record exchange among authorized parties. Amanically, Adeniyi et al. (2024) featured a smart contract-based schema that autonomously governs access control, reducing manual intervention and facilitating compliance.

Despite these developments, the technology is not without challenges. Crypto key mismanagement remains a significant threat vector; loss or theft of keys can result in permanent data inaccessibility or unauthorized access (Fonsêca et al., 2024). Moreover, smart contract flaws may introduce vulnerabilities if not subjected to formal verification (Pokharel et al., 2024). Finally, while permissioned blockchains mitigate consensus-based attacks (e.g., 51% attacks), private key compromise and integration points continue to require layered defense strategies (Alamri et al., 2022).

The literature reveals a remixed cybersecurity landscape: while AI and machine learning are redefining threat detection, the centralized nature of legacy systems continues to hamper effectiveness. Blockchain offers a transformative alternative by embedding security features such as immutability, decentralized consensus, and cryptographic integrity directly into health data management. However, realizing these benefits demands comprehensive attention to challenges in key management, smart contract security, system integration, and regulatory alignment. Subsequent sections will examine specific implementation frameworks, pilot methodologies, and governance architectures to support effective adoption.

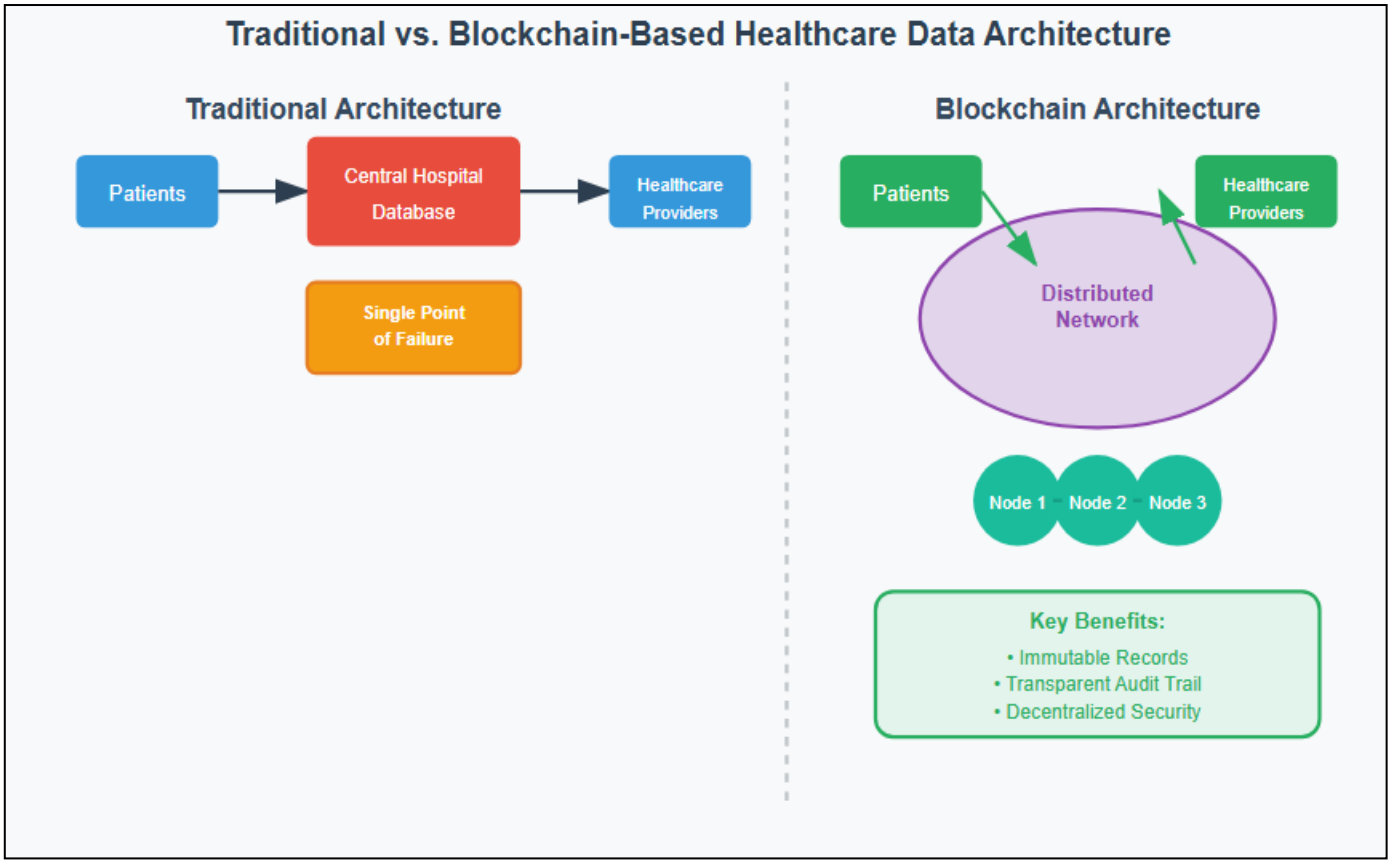

Fig 1 Blockchain Architecture for Healthcare Data Management

III. METHODOLOGY

This research employs a comprehensive literature review methodology combined with case study analysis of existing blockchain implementations in healthcare. The study focuses specifically on United States healthcare systems to ensure relevance to domestic regulatory requirements and operational contexts.

➢ *Data Collection Framework*

The research methodology incorporates analysis of peer-reviewed academic literature, industry reports, and regulatory guidelines from relevant healthcare authorities. Special attention was given to recent developments in cybersecurity technologies and their application to healthcare environments.

➢ *Analytical Approach*

The analysis framework evaluates blockchain implementations across multiple dimensions:

- **Security Enhancement Capabilities:** Assessment of blockchain's ability to improve data protection
- **Vulnerability Assessment:** Identification of potential security weaknesses in blockchain systems
- **Regulatory Compliance:** Evaluation of blockchain systems' ability to meet healthcare regulations
- **Operational Integration:** Analysis of blockchain compatibility with existing healthcare infrastructure

IV. BLOCKCHAIN OPPORTUNITIES IN HEALTHCARE CYBERSECURITY

➢ *Enhanced Data Integrity and Immutability*

The immutable nature of blockchain ledgers provides unprecedented data integrity assurance for healthcare organizations. Once health data is recorded on a blockchain network, it becomes computationally infeasible to alter historical records without detection, addressing one of the most significant vulnerabilities in traditional healthcare data systems.

This characteristic is particularly valuable for maintaining audit trails of patient data access and modifications, enabling healthcare organizations to track all interactions with sensitive information. The cryptographic mechanisms employed in blockchain systems ensure that data integrity verification can be performed efficiently without compromising system performance.

Table 1 Comparison of Data Integrity Mechanisms

Security Feature	Traditional Database	Blockchain Implementation
Data Immutability	Limited by admin access	Cryptographically guaranteed
Audit Trail	Centralized logging	Distributed consensus
Integrity Verification	Periodic checksums	Continuous validation
Tampering Detection	Manual review required	Automatic notification
Recovery Capability	Backup dependent	Network consensus

➢ *Decentralized Access Control*

Blockchain technology enables the implementation of sophisticated access control mechanisms that eliminate reliance on centralized authorities. Smart contracts can be programmed to automatically enforce access policies based on predefined criteria, reducing the risk of unauthorized data access while maintaining operational efficiency.

The decentralized nature of blockchain networks means that access control decisions are validated by multiple network participants rather than a single authority, significantly reducing the risk of insider threats and administrative abuse. This distributed approach to access management aligns with zero-trust security principles that are increasingly recognized as essential for healthcare cybersecurity.

Healthcare organizations can implement role-based access controls through smart contracts that automatically verify user credentials and permissions before granting access to sensitive patient data. This automated approach reduces administrative overhead while providing more granular control over data access patterns.

➢ *Interoperability and Secure Data Sharing*

One of the most significant opportunities presented by blockchain technology is the potential to enable secure, standardized data sharing between healthcare organizations. The distributed nature of blockchain networks allows for the creation of shared data repositories that maintain patient privacy while enabling authorized access by multiple healthcare providers.

Blockchain-based interoperability solutions can address long-standing challenges in healthcare data exchange by providing a common framework for data validation and access control. Smart contracts can be programmed to enforce data sharing agreements automatically, ensuring that patient privacy preferences and regulatory requirements are consistently maintained across organizational boundaries.

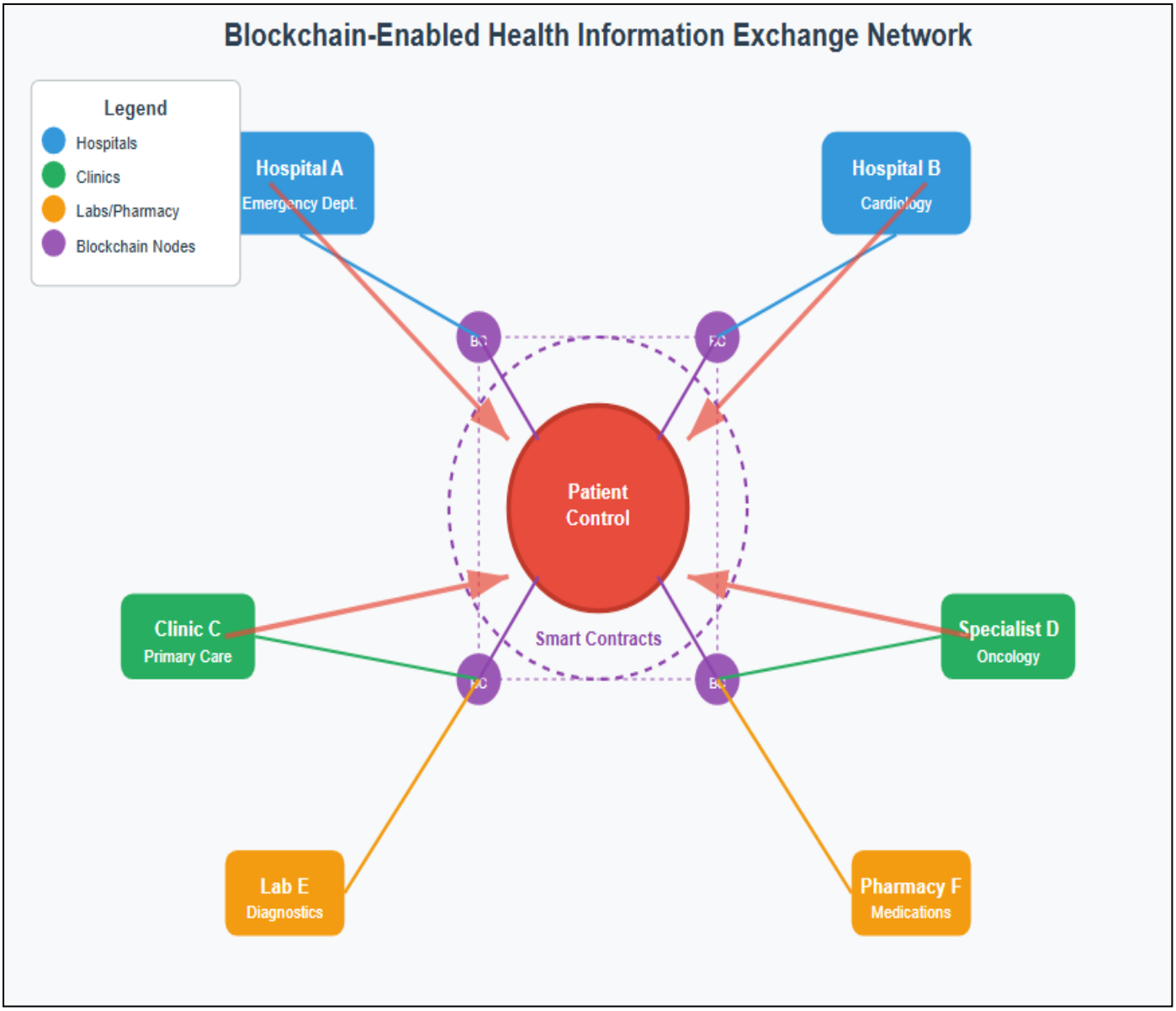

Fig 2 Blockchain-Enabled Healthcare Interoperability Framework

V. VULNERABILITIES AND SECURITY CHALLENGES

➢ *Smart Contract Vulnerabilities*

While smart contracts provide powerful automation capabilities for healthcare blockchain systems, they also introduce new categories of vulnerabilities that must be carefully managed. Programming errors in smart contracts can create security weaknesses that malicious actors may exploit to gain unauthorized access to patient data or disrupt healthcare operations.

The immutable nature of blockchain systems means that smart contract vulnerabilities cannot be easily corrected once deployed, requiring extensive testing and validation procedures before implementation. Healthcare organizations must develop comprehensive smart contract auditing processes to identify and address potential security weaknesses before they can be exploited.

Research by Chatterjee et al. (2023) demonstrates how federated learning and blockchain technologies can be combined to secure financial services, providing insights that are applicable to healthcare environments. However, the complexity of smart contract interactions in healthcare contexts requires specialized security analysis techniques.

➢ *Scalability and Performance Limitations*

Blockchain networks face significant scalability challenges when processing the high volumes of data transactions typical in healthcare environments. The consensus mechanisms required for blockchain operation can create performance bottlenecks that may impact the real-time data access requirements essential for clinical decision-making.

Healthcare organizations must carefully evaluate the performance characteristics of different blockchain implementations to ensure that security enhancements do not compromise operational efficiency. The trade-off between security and performance requires careful optimization based on specific healthcare use cases and operational requirements.

Table 2 Blockchain Scalability Metrics for Healthcare Applications

Performance Metric	Current Limitation	Healthcare Requirement	Gap Analysis
Transaction Throughput	10-15 TPS	1000+ TPS	Significant Gap
Latency	10-60 seconds	<3 seconds	Critical Gap
Storage Efficiency	High redundancy	Optimized storage	Moderate Gap
Energy Consumption	High for PoW	Minimal impact	Significant Gap
Network Bandwidth	High requirements	Limited infrastructure	Moderate Gap

➢ *Regulatory Compliance Challenges*

The regulatory landscape for healthcare data management in the United States presents complex challenges for blockchain implementation. HIPAA compliance requirements, in particular, create specific obligations for data protection that may conflict with the transparent nature of blockchain networks.

Healthcare organizations must ensure that blockchain implementations maintain compliance with federal and state healthcare regulations while providing the security benefits of distributed ledger technology. This requirement often necessitates the use of private or consortium blockchain networks that limit access to authorized participants while maintaining regulatory compliance.

The evolving regulatory framework for blockchain technology in healthcare creates additional uncertainty for organizations considering implementation. Healthcare entities must work closely with regulatory bodies to ensure that blockchain deployments meet current compliance requirements while remaining adaptable to future regulatory changes.

VI. IMPLEMENTATION FRAMEWORK AND BEST PRACTICES

➢ *Architecture Design Principles*

Successful blockchain implementation in healthcare requires careful attention to architectural design principles that balance security, performance, and regulatory compliance requirements. The architecture must accommodate the complex data relationships and access patterns typical in healthcare environments while maintaining the security benefits of blockchain technology.

Healthcare blockchain architectures should incorporate hybrid approaches that combine blockchain security mechanisms with traditional database performance characteristics. This approach enables organizations to leverage blockchain benefits for critical security functions while maintaining operational efficiency for routine data operations.

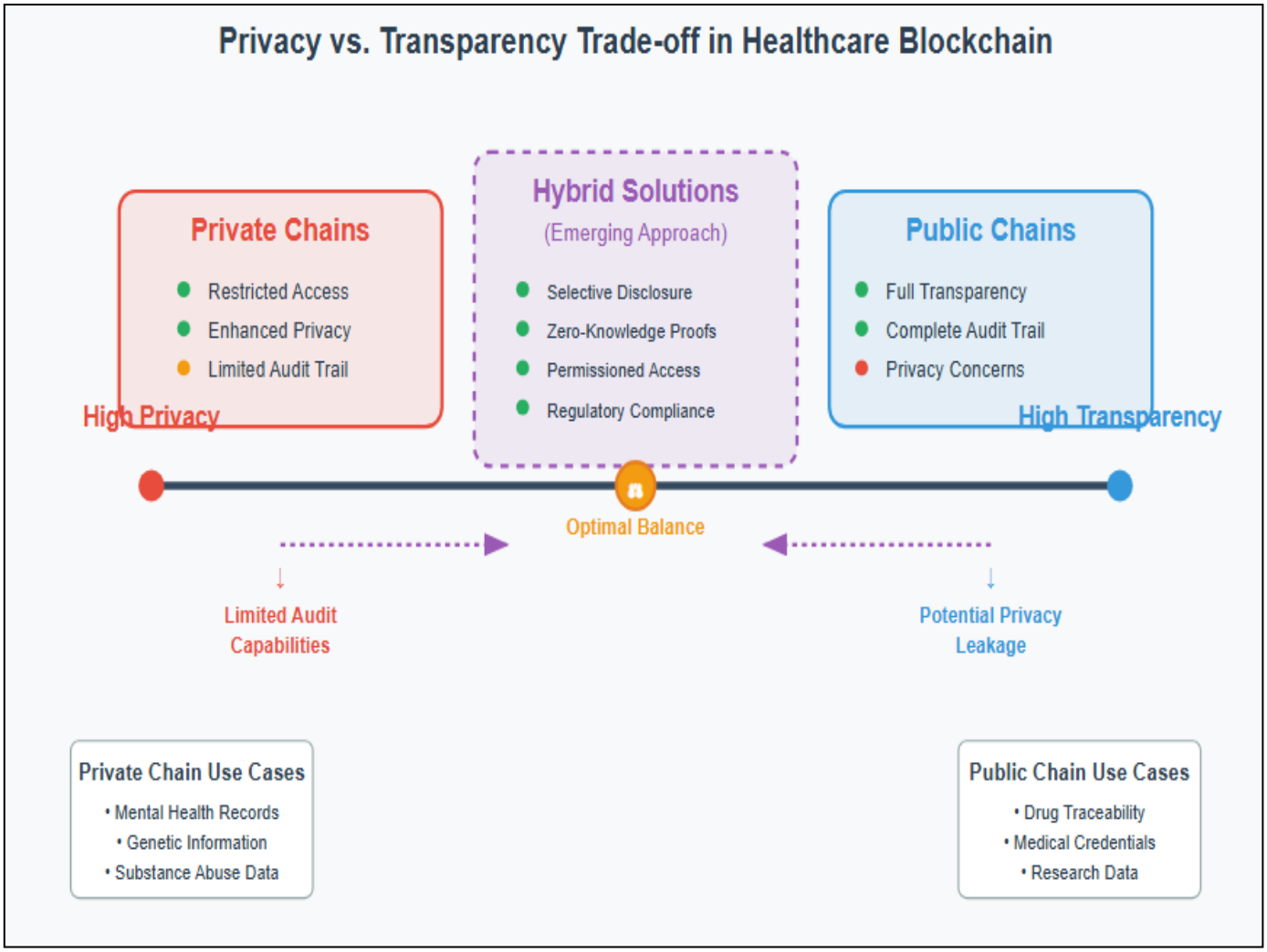

Fig 3 Hybrid Blockchain Architecture for Healthcare

➢ *Security Implementation Guidelines*

The implementation of blockchain technology in healthcare environments requires comprehensive security frameworks that address both traditional cybersecurity threats and blockchain-specific vulnerabilities. Organizations must develop security policies that encompass the entire blockchain ecosystem, including network infrastructure, smart contracts, and user access management.

Key security implementation guidelines include:

- **Multi-layered Authentication:** Implementation of robust authentication mechanisms that combine traditional credentials with blockchain-based identity verification
- **Encryption Standards:** Adoption of advanced encryption protocols that protect data both in transit and at rest within blockchain networks
- **Continuous Monitoring:** Development of monitoring systems that can detect anomalous behavior and potential security threats in real-time
- **Incident Response:** Creation of incident response procedures specifically designed for blockchain-based healthcare systems

➢ *Integration with Existing Systems*

Healthcare organizations face significant challenges when integrating blockchain technology with existing information systems and workflows. The integration process must maintain operational continuity while gradually implementing blockchain security enhancements.

Successful blockchain integration requires phased implementation approaches that allow healthcare organizations to validate blockchain benefits while minimizing operational disruption. Organizations should begin with non-critical applications before expanding blockchain implementation to core healthcare functions.

Table 3 Phased Blockchain Implementation Strategy

Implementation Phase	Timeline	Scope	Success Criteria
Phase 1: Pilot	3-6 months	Audit logging	System stability
Phase 2: Limited Deployment	6-12 months	Access control	User acceptance
Phase 3: Expanded Implementation	12-18 months	Data sharing	Performance targets
Phase 4: Full Integration	18-24 months	Core systems	Regulatory compliance

VII. CASE STUDY ANALYSIS: US HEALTHCARE BLOCKCHAIN IMPLEMENTATIONS

➢ *Large Hospital System Implementation*

A major hospital system in the northeastern United States implemented a blockchain-based solution for managing patient consent and data sharing agreements. The implementation utilized a private blockchain network to maintain HIPAA compliance while enabling secure data sharing between affiliated healthcare facilities.

The system demonstrated significant improvements in data integrity verification and audit trail maintenance compared to traditional database approaches. Patient consent management became more transparent and verifiable, enabling better compliance with patient privacy preferences and regulatory requirements.

However, the implementation also revealed challenges related to system performance and integration complexity. The hospital system required substantial investment in technical training and infrastructure upgrades to support the blockchain implementation effectively.

➢ *Multi-Organizational Consortium*

A consortium of healthcare organizations in California developed a blockchain-based platform for sharing research data while maintaining patient privacy. The implementation utilized zero-knowledge proof mechanisms to enable data analysis without exposing sensitive patient information.

The consortium approach demonstrated the potential for blockchain technology to enable large-scale healthcare data collaboration while maintaining strict privacy controls. Research organizations were able to access aggregated data insights without compromising individual patient privacy or violating regulatory requirements.

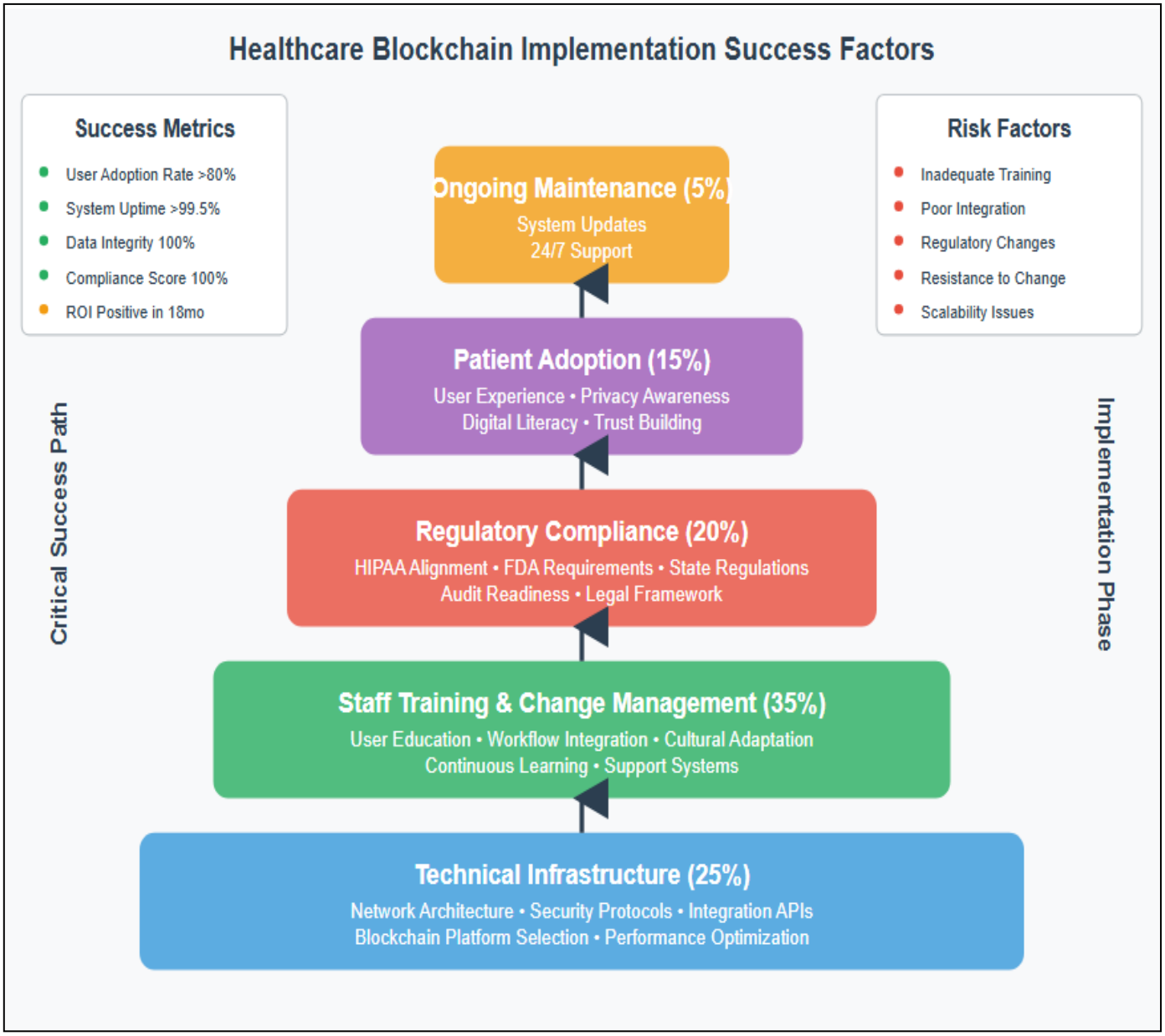

Fig 4 Consortium Blockchain Architecture

VIII. ECONOMIC IMPACT AND COST ANALYSIS

➢ *Implementation Costs*

The economic implications of blockchain implementation in healthcare are complex, involving significant upfront investments balanced against long-term security and operational benefits. Healthcare organizations must carefully evaluate the total cost of ownership for blockchain systems, including technology infrastructure, staff training, and ongoing maintenance requirements.

Initial blockchain implementation costs typically include hardware infrastructure, software licensing, professional services for system integration, and comprehensive staff training programs. These costs can be substantial, particularly for larger healthcare organizations with complex existing systems.

Table 4 Blockchain Implementation Cost Analysis

Cost Category	Initial Investment	Annual Ongoing	5-Year Total
Infrastructure	$500K - $2M	$100K - $400K	$1M - $4M
Software Licensing	$200K - $800K	$50K - $200K	$450K - $1.8M
Professional Services	$300K - $1.2M	$75K - $300K	$675K - $2.7M
Training & Development	$100K - $400K	$25K - $100K	$225K - $900K
Total	**$1.1M - $4.4M**	**$250K - $1M**	**$2.35M - $9.4M**

➢ *Return on Investment Analysis*

The return on investment for blockchain implementations in healthcare must account for both quantifiable security improvements and broader operational benefits. Healthcare organizations typically realize ROI through reduced cybersecurity incident costs, improved operational efficiency, and enhanced regulatory compliance capabilities.

Cybersecurity incidents in healthcare can cost organizations millions of dollars in direct response costs, regulatory fines, and reputation damage. Blockchain implementations that successfully prevent or mitigate such incidents can provide substantial financial returns that justify initial investment costs.

IX. FUTURE DIRECTIONS AND EMERGING TRENDS

➢ *Integration with Artificial Intelligence*

The convergence of blockchain technology with artificial intelligence and machine learning presents significant opportunities for advancing healthcare cybersecurity. AI-powered threat detection systems can leverage blockchain's immutable audit trails to improve threat analysis and response capabilities.

Research demonstrates how AI technologies are revolutionizing fraud detection and risk management in financial services, providing insights that are directly applicable to healthcare environments. The combination of AI threat detection with blockchain data integrity creates powerful security frameworks that can adapt to evolving cyber threats.

Machine learning algorithms can analyze blockchain transaction patterns to identify anomalous behavior that may indicate security threats or data breaches. This proactive approach to threat detection enables healthcare organizations to respond to potential security incidents before they can cause significant damage.

➢ *Regulatory Evolution*

The regulatory landscape for blockchain technology in healthcare continues to evolve, with federal and state agencies developing new guidelines and requirements for blockchain implementations. Healthcare organizations must stay informed about regulatory changes that may impact their blockchain strategies.

Future regulatory developments are likely to address specific aspects of blockchain technology that are particularly relevant to healthcare, including smart contract governance, data portability requirements, and cross-border data sharing protocols. Organizations that proactively address regulatory compliance in their blockchain implementations will be better positioned to adapt to future regulatory changes.

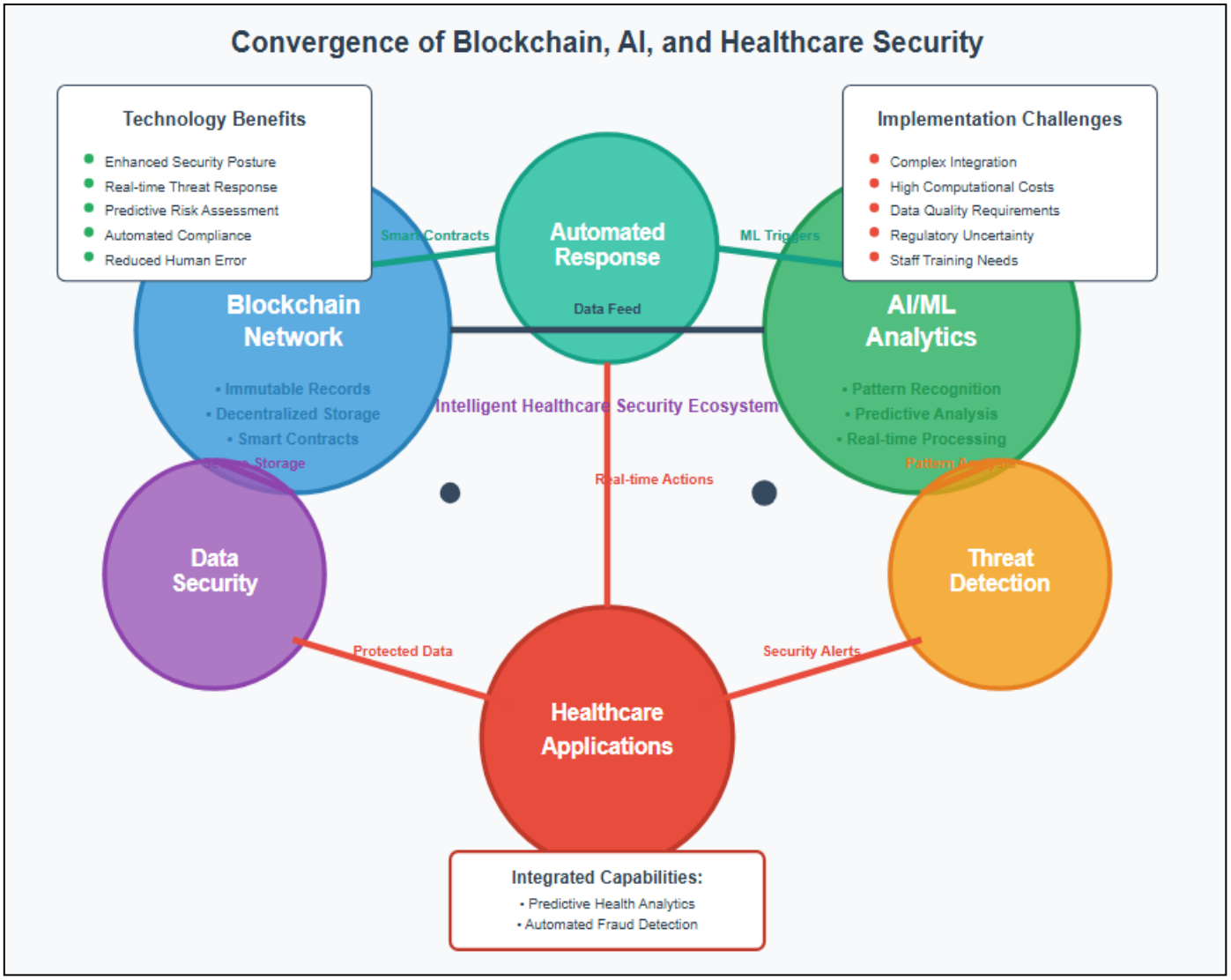

Fig 5 Future Healthcare Blockchain Ecosystem

➢ *Interoperability Standards*

The development of standardized protocols for healthcare blockchain interoperability represents a critical area for future advancement. Industry organizations and standards bodies are working to establish common frameworks that enable seamless data exchange between different blockchain implementations.

Standardization efforts focus on creating common data formats, communication protocols, and security requirements that enable blockchain networks from different vendors to interact effectively. These standards will be essential for realizing the full potential of blockchain technology in healthcare environments.

X. CONCLUSIONS AND RECOMMENDATIONS

➢ *Key Findings*

This analysis reveals that blockchain technology offers substantial opportunities for enhancing healthcare cybersecurity through improved data integrity, decentralized access control, and secure interoperability capabilities. However, successful implementation requires careful attention to vulnerabilities related to smart contract security, scalability limitations, and regulatory compliance requirements.

Healthcare organizations considering blockchain implementation should adopt phased approaches that allow for gradual integration while maintaining operational continuity. The combination of blockchain technology with AI-powered security systems presents particularly promising opportunities for advancing healthcare cybersecurity capabilities.

➢ *Strategic Recommendations*

Based on the analysis conducted, several strategic recommendations emerge for healthcare organizations:

- *Immediate Actions:*

✓ Conduct comprehensive blockchain readiness assessments to evaluate organizational capabilities and requirements
✓ Develop blockchain governance frameworks that address security, compliance, and operational considerations
✓ Establish partnerships with technology vendors and consulting organizations with proven healthcare blockchain expertise

- *Medium-term Initiatives:*

✓ Implement pilot blockchain projects focused on specific use cases with clear success criteria
✓ Develop staff training programs to build internal blockchain expertise and capabilities
✓ Create integration strategies that accommodate existing systems while enabling blockchain adoption

- *Long-term Strategic Objectives:*

✓ Establish blockchain centers of excellence to drive organizational blockchain strategy and implementation
✓ Participate in industry consortiums and standards development efforts to influence blockchain evolution
✓ Develop comprehensive blockchain security frameworks that address evolving cyber threats

➢ *Future Research Directions*

Several areas warrant additional research to advance blockchain applications in healthcare cybersecurity:

The integration of quantum-resistant cryptographic mechanisms into healthcare blockchain systems represents a critical area for future investigation. As quantum computing capabilities advance, healthcare organizations will need blockchain implementations that can withstand quantum-based attacks.

Research into blockchain scalability solutions specifically designed for healthcare environments could address current performance limitations that limit widespread adoption. Solutions such as sharding, layer-2 protocols, and hybrid architectures require additional investigation in healthcare contexts.

The development of standardized healthcare blockchain security frameworks would benefit from collaborative research efforts involving healthcare organizations, technology vendors, and regulatory bodies. Such frameworks could accelerate blockchain adoption while ensuring consistent security and compliance standards.

REFERENCES

[1]. Adeniyi, J. K., Ajagbe, S. A., Adeniyi, A. E., Adeyanju, K. I., Afolorunso, A. A., Adigun, M. O., & Ogene, I. (2024). A blockchain-based smart healthcare system for data protection. *iScience*, *28*(4), 112109. https://doi.org/10.1016/j.isci. 2024.112109

[2]. Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-Alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, *142*, 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246

[3]. Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. *Sensors*, *23*(1), 218. https://doi.org/10.3390/s23010218

[4]. Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology. *Circulation Cardiovascular Quality and Outcomes*, *10*(9). https://doi.org/10.1161/circoutcomes.117.003800

[5]. Boulos, M. N. K., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *International Journal of Health Geographics*, *17*(1). https://doi.org/10.1186/s12942-018-0144-x

[6]. Chen, H., & Huang, X. (2018). Will blockchain technology transform healthcare and biomedical sciences? *PubMed*, *6*(11), 910–911. https://pubmed.ncbi.nlm.nih.gov/31460519

[7]. Chatterjee, P., Das, D., & Rawat, D. B. (2023). Use of Federated Learning and Blockchain towards Securing Financial Services. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2303.12944

[8]. Esmaeilzadeh, P., & Mirzaei, T. (2019). The Potential of blockchain Technology for health Information Exchange: Experimental study from Patients' Perspectives. *Journal of Medical Internet Research*, *21*(6), e14184. https://doi.org/10.2196/14184

[9]. Fonsêca, A. L. A., Barbalho, I. M. P., Fernandes, F., Júnior, E. A., Nagem, D. a. P., Cardoso, P. H., Veras, N. V. R., De Oliveira Farias, F. L., Lindquist, A. R., Santos, J. P. Q. D., De Morais, A. H. F., Henriques, J., Lucena, M., & De Medeiros Valentim, R. A. (2024). Blockchain in Health Information Systems: A Systematic review. *International Journal of Environmental Research and Public Health*, *21*(11), 1512. https://doi.org/10.3390/ijerph21111512

[10]. Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept study. *Journal of Medical Internet Research*, *21*(8), e13592. https://doi.org/10.2196/13592

[11]. Kunal, S., Gandhi, P., Rathod, D., Amin, R., & Sharma, S. (2024). Securing patient data in the healthcare industry: A blockchain-driven protocol with advanced encryption. *Journal of Education and Health Promotion*, *13*(1). https://doi.org/10.4103/jehp.jehp_984_23

[12]. Mackey, T. K., Kuo, T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R., & Palombini, M. (2019). 'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Medicine*, *17*(1). https://doi.org/10.1186/s12916-019-1296-7

[13]. McGhin, T., Choo, K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

[14]. Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2024). BlockHealthSecure: Integrating

blockchain and cybersecurity in Post-Pandemic healthcare systems. *Information*, *16*(2), 133. https://doi.org/10.3390/info16020133

[15]. Richard, T. (2024). Blockchain in Healthcare: Ensuring data security and integrity. *Research Output Journal of Public Health and Medicine*, *4*(2), 12–17. https://doi.org/10.59298/rojphm/2024/421217

[16]. Roehrs, A., Da Costa, C. A., & Da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, *71*, 70–81. https://doi.org/10.1016/j.jbi.2017.05.012

[17]. Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *PLoS ONE*, *17*(4), e0266462. https://doi.org/10.1371/journal.pone.0266462

[18]. Sutradhar, S., Bose, R., Majumder, S., Khan, A. A., Roy, S., Ullah, F., & Prashar, D. (2024). MediGuard: A Survey on Security Attacks in Blockchain-IoT Ecosystems for e-Healthcare Applications. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *0*(0), 1–10. https://doi.org/10.32604/cmc.2024.061965

[19]. Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/ijwgs.2018.10016848