

Systematic Review

Advancing Blockchain and Quantum Technologies for Secure E-Health Systems: A Systematic Review and Conceptual Security Framework

Abdullah Alabdulatif 

Department of Computer Science, College of Computer, Qassim University, Buraydah 52571, Saudi Arabia; a.alabdulatif@qu.edu.sa

Abstract

The rapid digitalisation of healthcare has accelerated the adoption of telemedicine, Electronic Health Records (EHRs), and the Internet of Medical Things (IoMT), transforming healthcare delivery into a highly interconnected and patient-centric ecosystem. In response to growing concerns about data security, privacy, and interoperability, blockchain technology has emerged as a promising solution for its decentralization, immutability, auditability, and secure access control. However, many existing blockchain infrastructures rely on classical cryptographic primitives, including RSA- or elliptic-curve-based public-key mechanisms and cryptographic hash functions such as SHA-256, whose relevant security properties may be affected by sufficiently powerful quantum attacks. This review investigates the convergence of blockchain and quantum technologies to address emerging security threats in e-health systems. A structured literature review was conducted in accordance with the PRISMA 2020 guidelines using the IEEE Xplore, PubMed, ACM Digital Library, Google Scholar, and Crossref databases, covering studies published between January 2018 and June 2025. Following a systematic screening and eligibility-verification process, 57 relevant studies were selected and analyzed. The review evaluates quantum-resilient security mechanisms, including Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), and NIST-standardized Post-Quantum Cryptography (PQC) algorithms specified in FIPS 203, FIPS 204, and FIPS 205. Based on the identified research gaps in the state of the art, this study also proposes a novel four-layer Quantum-Blockchain Security Architecture (QBSA) designed for secure healthcare environments. The analysis further reveals significant challenges associated with lightweight PQC deployment for IoMT devices, interoperability standardization, quantum hardware limitations, and regulatory compliance in cross-institutional healthcare systems. The findings highlight the necessity of integrating quantum-resilient cryptographic frameworks with blockchain infrastructures to support the development of secure, scalable, and patient-centric next-generation e-health ecosystems.



Academic Editor: Christos J. Bouras

Received: 5 July 2026

Revised: 18 August 2026

Accepted: 20 August 2026

Published: 26 August 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: quantum computing; blockchain technology; E-health security; post-quantum cryptography (PQC); quantum key distribution (QKD); Electronic Health Records (EHR); Internet of Medical Things (IoMT)

1. Introduction

Healthcare delivery is undergoing a profound digital transformation that is reshaping how medical services are provided, managed, and accessed [1]. In recent decades, the

widespread adoption of EHRs, telemedicine platforms, and the IoMT has shifted healthcare infrastructure from isolated, institution-centric systems toward highly interconnected digital ecosystems [1–4]. These advancements have significantly improved clinical efficiency, remote patient monitoring, healthcare accessibility, and personalized treatment delivery. However, the increasing interconnectivity of healthcare infrastructures has also introduced substantial security, privacy, and interoperability challenges.

The rapid expansion of IoMT devices has further intensified these concerns. IoMT-enabled healthcare systems continuously collect, transmit, and analyze a large volume of sensitive patient information across clinical and remote environments [5,6]. Although such technologies enhance personalized healthcare services and real-time monitoring capabilities, they simultaneously enlarge the cyberattack surface of healthcare ecosystems. In recent years, the healthcare sector has experienced some of the highest rates of data breaches due to the high value and sensitivity of medical information [7]. A notable example is the 2021 cyberattack on the Irish Health Service Executive, which severely disrupted healthcare operations nationwide and exposed vulnerabilities in modern digital healthcare infrastructure [8].

Despite ongoing technological advancements, many healthcare institutions continue to rely on traditional centralized architectures for managing sensitive medical data. These systems often suffer from limited transparency, poor interoperability, single points of failure, and insufficient patient control over personal health records [9]. Furthermore, compliance with regulatory frameworks, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), introduces additional technical, operational, and ethical complexities related to data governance and secure information exchange.

To address these limitations, blockchain technology has emerged as a promising solution for secure and decentralized healthcare data management [10–12]. Through distributed ledger mechanisms, cryptographic hashing, consensus protocols, and smart contract automation, blockchain enables immutable record-keeping, verifiable data provenance, transparent auditing, and decentralized access control. Consequently, blockchain-based healthcare applications have gained significant attention in areas such as EHR management, telemedicine, pharmaceutical supply chains, insurance claim processing, and patient consent management [13–15].

Nevertheless, despite its advantages, blockchain technology remains structurally dependent on classical cryptographic primitives, including RSA, SHA-256, and ECDSA. These cryptographic mechanisms are theoretically vulnerable to future large-scale quantum computing attacks. Shor's algorithm can efficiently solve the integer factorization and elliptic-curve discrete logarithm problems, thereby threatening the security of RSA- and ECDSA-based systems [16]. Similarly, Grover's algorithm reduces the effective security strength of cryptographic hash functions such as SHA-256 by significantly accelerating brute-force search operations [17]. As major technology organizations, including IBM and Google, continue to advance quantum computing research, concerns regarding the long-term security of existing blockchain infrastructures are becoming increasingly significant [18,19].

1.1. Motivation of the Study

As mentioned above, the emergence of quantum computing presents a critical challenge for blockchain-enabled healthcare systems due to their reliance on quantum-vulnerable cryptographic algorithms. Although recent advancements in PQC, Quantum Key Distribution (QKD), and Quantum Random Number Generation (QRNG) provide promising directions for quantum-resilient security, existing studies remain fragmented

and largely application-specific. Current research primarily focuses on either blockchain security, post-quantum cryptographic mechanisms, or quantum communication protocols independently, while comprehensive frameworks integrating these technologies within healthcare environments remain limited. Furthermore, the increasing adoption of IoMT devices, cross-institutional healthcare data exchange, and AI-driven healthcare services demand scalable, interoperable, and future-proof security architectures capable of resisting both classical and quantum-era cyber threats. These challenges highlight the urgent need for a systematic investigation into the convergence of blockchain and quantum technologies for secure e-health infrastructures.

1.2. Research Contributions

Motivated by these challenges, this study provides a comprehensive review and conceptual framework for quantum-resilient blockchain-based healthcare systems. The main contributions of this study are summarized as follows:

- **Provide a systematic literature review:**

A structured review of 57 peer-reviewed studies published between January 2018 and June 2025 was conducted across IEEE Xplore, PubMed, ACM Digital Library, Google Scholar, and Crossref to analyze the intersection of blockchain, quantum security, and e-health systems.

- **Provide a comparative analysis of existing frameworks:**

Twenty representative studies at the blockchain–quantum–healthcare intersection were systematically compared across six analytical dimensions, including cryptographic design, blockchain platform, healthcare context, maturity level, security objectives, and implementation limitations.

- **Provide a quantum threat assessment for healthcare blockchain:**

The study analyses the impact of quantum computing threats on existing blockchain infrastructures, particularly focusing on vulnerabilities associated with RSA, ECDSA, SHA-256, and conventional key exchange mechanisms.

- **Proposed Quantum-Blockchain Security Architecture (QBSA):**

A novel four-layer Quantum-Blockchain Security Architecture (QBSA) is proposed to support secure, scalable, and quantum-resilient healthcare ecosystems through the integration of PQC, QKD, QRNG, and permissioned blockchain infrastructures.

- **Provide a technical evaluation of NIST-standardized PQC algorithms:**

The paper presents a comparative analysis of NIST-standardized PQC algorithms (FIPS 203, FIPS 204, and FIPS 205) with emphasis on computational efficiency, security strength, and suitability for IoMT-constrained healthcare deployments.

- **Identification of open challenges and future directions:**

The study highlights unresolved challenges related to lightweight PQC integration, interoperability, regulatory compliance, quantum hardware limitations, and secure cross-border healthcare data exchange.

1.3. Research Methodology

This review follows a structured methodology based on the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [20]. Relevant literature published between 1 January 2018 and 30 June 2025 was collected from five scientific sources: IEEE Xplore, PubMed, ACM Digital Library (queried through the Crossref meta-data API), Google Scholar, and the Crossref scholarly metadata index. Crossref was adopted

in place of Scopus—to which institutional access was not available—because it offers an open and fully reproducible query interface. The search was executed on 11 August 2026, during the revision of this article, and was restricted to records published within the review window. The generic search string combined three concept groups using Boolean operators: (“blockchain” OR “distributed ledger”) AND (“quantum” OR “post-quantum” OR “quantum key distribution” OR “quantum-resistant”) AND (“healthcare” OR “e-health” OR “EHR” OR “electronic health record” OR “Internet of Medical Things” OR “IoMT” OR “telemedicine”). The string was syntactically adapted to each source (e.g., “All Metadata” in IEEE Xplore, title/abstract fields in PubMed, six documented bibliographic queries in Crossref, and a publisher-scoped Crossref query for ACM content); for Google Scholar, the 200 highest-ranked results were screened. The complete source-specific search strategies are provided in Supplementary File S1. This review was conducted and reported in accordance with the PRISMA 2020 statement [20] (completed checklist in Supplementary File S1); the review protocol was not registered.

The search returned 556 records in total: IEEE Xplore (n = 263), Google Scholar (n = 200), Crossref (n = 47), PubMed (n = 39), and ACM Digital Library via Crossref (n = 7). After removal of 66 duplicates, 490 records underwent title and abstract screening, during which 383 records were excluded (209 not related to the blockchain–quantum–healthcare scope, 73 published outside 2018–2025, 61 from non-eligible venues or with unverifiable peer-review status, and 40 preprints, book chapters, theses, or standards documents). The remaining 107 records were assessed for eligibility through publication-date verification against the 30 June 2025 cut-off and a content review; 50 records were excluded at this stage (43 published after the cut-off—with the dates of ten borderline records verified individually against the publisher pages—and 7 that were editorials, correction notices, a book chapter identified at full-text review, non-healthcare applications, or lacked substantive quantum-security content), yielding 57 included studies. Screening was rule-assisted (keyword-based pre-classification of titles and abstracts) and performed by the author in two passes separated in time, with borderline records re-examined individually; a standardized extraction form recording publication year, source, technology focus, healthcare context, and key findings was used (Supplementary File S1). As a single-author review, no inter-reviewer disagreement procedure was applicable, which is acknowledged as a methodological limitation. Study adequacy was appraised using a four-criterion checklist (clarity of security objectives, technical soundness, evaluation evidence, and healthcare relevance), and the resulting classification is reported in Supplementary Table S2.

To avoid ambiguity regarding the composition of the evidence base, four categories of cited material are distinguished throughout this review: (i) the 57 studies forming the systematic-review corpus (peer-reviewed, January 2018–June 2025), listed in full in Supplementary Table S2; (ii) background references cited for specific technical or contextual points but not retrieved by the systematic search, including foundational works published before 2018 (e.g., Shor’s and Grover’s algorithms, the BB84 protocol, and early systems such as MedRec); (iii) standards and institutional reports (e.g., NIST FIPS 203/204/205 and industry incident reports), which are treated as primary technical sources rather than corpus studies; and (iv) a representative subset of 20 studies selected for the in-depth comparative analysis in Table 3 (selection criteria are given in Section 7.1), drawn from both the corpus and the foundational literature. Entries in Table 3 that fall outside the search corpus are explicitly marked. The inclusion criteria considered studies that:

- were published between 1 January 2018 and 30 June 2025,
- were peer-reviewed and written in English,
- addressed blockchain, quantum security, or e-health technologies,
- and demonstrated technical or architectural relevance to healthcare cybersecurity.

Studies were excluded if they:

- lacked healthcare relevance,
- were non-technical or editorial articles,
- duplicated previously indexed works,
- or did not contribute directly to blockchain or quantum-security applications in healthcare.

Figure 1 illustrates the PRISMA 2020-based study selection workflow adopted in this review [20].

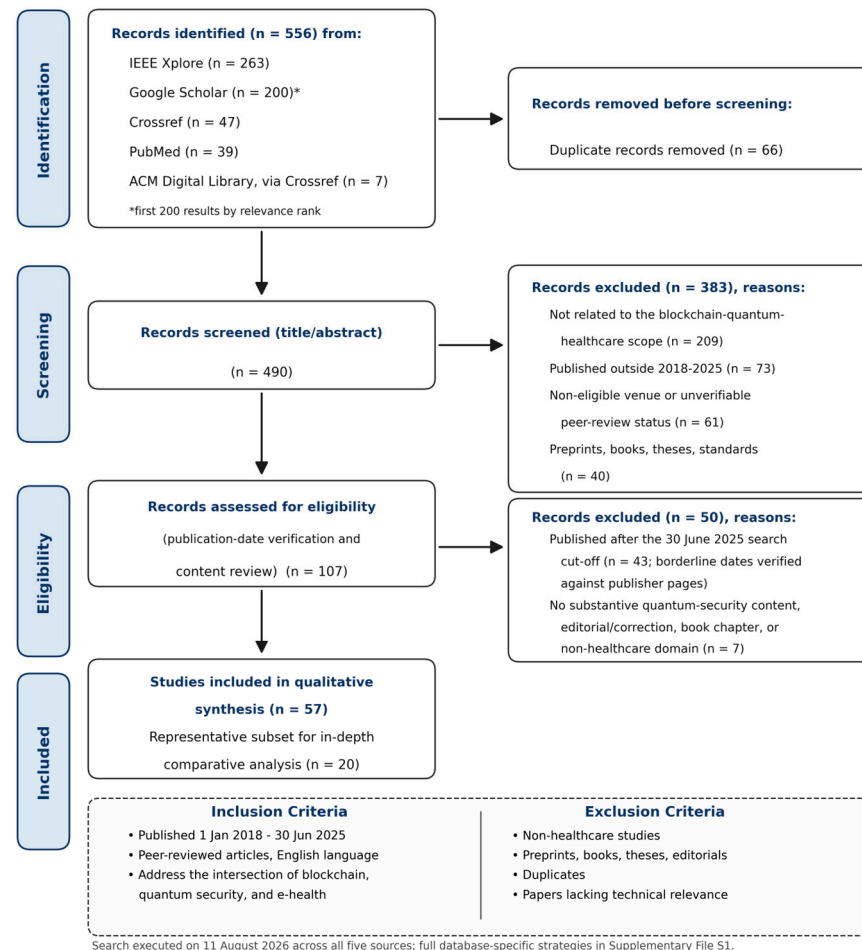


Figure 1. PRISMA 2020 flow diagram of the study identification, screening, and inclusion process [20].

1.4. Organization of the Study

The remainder of this paper is organized in the following manner. Following the introduction, Section 2 outlines the essential security and operational requirements of e-health systems. Section 3 discusses blockchain technology and its healthcare applications. Section 4 introduces the principles of quantum computing and its relevance to healthcare security. Section 5 analyses quantum threats to blockchain-based e-health systems. Section 6 examines opportunities enabled by quantum-enhanced blockchain technologies. Section 7 presents hybrid frameworks and the proposed QBSA. Section 8 discusses open challenges and research gaps. Section 9 highlights future research directions, and finally, Section 10 concludes the paper.

2. Requirements of Secure E-Health Systems

Having established the motivation for quantum-resilient healthcare security, this section distils the essential security and operational requirements that any secure e-health

architecture must satisfy; these requirements also serve as the design criteria against which the QBSA proposed in Section 7 was formulated [21,22]. Contemporary e-health ecosystems integrate Electronic Health Records (EHRs), telemedicine platforms, cloud infrastructures, wearable devices, and IoMT technologies to support efficient healthcare operations and real-time patient monitoring. Within this ecosystem, EHR systems play a critical role in storing, managing, and exchanging sensitive clinical information, including medical histories, prescriptions, diagnostic reports, and laboratory results. Despite these advancements, the increasing digitization and interconnectivity of healthcare systems pose substantial challenges to security, privacy, scalability, and governance. Consequently, the development of secure and resilient e-health infrastructures requires several fundamental operational and security requirements, as discussed below.

2.1. Data Security and Privacy

Healthcare data is highly sensitive and represents one of the most valuable targets for cybercriminals. E-health systems must therefore ensure strong protection against unauthorized access, data tampering, ransomware attacks, medical identity theft, and man-in-the-middle attacks. Recent studies indicate that the healthcare sector incurs some of the highest financial losses from cybersecurity breaches due to the critical nature of patient information [23]. To maintain trust and regulatory compliance, healthcare systems must guarantee:

- confidentiality of patient data,
- integrity of medical records,
- secure data transmission,
- and the availability of healthcare services during cyber incidents.

2.2. Interoperability and Secure Data Exchange

Modern healthcare environments involve heterogeneous systems operated by hospitals, laboratories, pharmacies, insurance providers, and telemedicine platforms. These systems often rely on different communication standards and data formats, creating interoperability challenges [21]. A robust e-health system must support secure and standardized data exchange while preserving data integrity and consistency across institutions. Standards such as HL7 FHIR and DICOM play an essential role in enabling interoperable healthcare communication. However, maintaining secure cross-platform interoperability remains a major technical challenge, particularly in decentralized and multi-institutional healthcare environments.

2.3. Patient Consent Management and Confidentiality

Healthcare regulations such as HIPAA and GDPR require healthcare organizations to provide patients with greater control over their personal data [22]. E-health systems must therefore support transparent consent management mechanisms that allow patients to:

- authorize or revoke access to medical records,
- control data sharing permissions,
- and ensure privacy-preserving access management.

In addition to regulatory compliance, maintaining patient confidentiality is essential for building trust in digital healthcare services. Consequently, secure authentication, cryptographic access control, and auditable data governance mechanisms are critical requirements for next-generation healthcare infrastructures.

2.4. Scalability and System Adaptability

The rapid growth of IoMT devices, wearable sensors, and healthcare data generation places increasing computational and storage demands on healthcare infrastructures. E-health systems must therefore remain scalable and adaptable while supporting real-time data processing, remote monitoring, and continuous clinical service availability [24]. Traditional centralized systems frequently experience performance bottlenecks under high transaction volumes and large-scale data exchange scenarios. Consequently, modern healthcare architectures must support:

- dynamic scalability,
- distributed processing,
- low-latency communication,
- and efficient resource management without compromising security or reliability.

2.5. Access Control and Quantum-Resilient Security

Secure access control mechanisms are fundamental for protecting sensitive healthcare information from unauthorized disclosure. Role-Based Access Control (RBAC) and Attribute-Based Encryption (ABE) are widely adopted approaches for restricting access according to user roles, identities, and contextual permissions [25]. However, many existing healthcare systems continue to rely on classical cryptographic algorithms that may become vulnerable in the era of large-scale quantum computing. As a result, future e-health infrastructures must transition to quantum-resilient cryptographic mechanisms that protect healthcare data against both classical and quantum-enabled cyber threats. The integration of PQC, QKD, and blockchain-based trust management is therefore emerging as a critical research direction for developing secure next-generation healthcare ecosystems.

2.6. Summary

In summary, a secure and reliable e-health system must balance confidentiality, integrity, interoperability, scalability, patient autonomy, and quantum-resilient security. As healthcare ecosystems continue to evolve toward highly interconnected digital environments, blockchain and quantum-safe cryptographic technologies are becoming increasingly important for establishing trustworthy, decentralized, and future-proof healthcare infrastructures, which will be discussed in detail in the forthcoming sections.

3. Blockchain Technology in E-Health

Blockchain technology has emerged as a transformative paradigm for secure and decentralized data management in healthcare systems. A blockchain is a distributed ledger technology that maintains immutable and chronologically ordered records across multiple network nodes without relying on a central authority. Its core characteristics, including decentralization, transparency, traceability, immutability, and auditability, make blockchain particularly suitable for addressing the growing challenges associated with healthcare data security, interoperability, and trust management in multi-stakeholder healthcare ecosystems [10,26]. In healthcare environments, blockchain enables secure information sharing among hospitals, laboratories, insurance providers, pharmacies, patients, and regulatory authorities while preserving data integrity and minimizing unauthorized access. Through cryptographic hashing, distributed consensus mechanisms, and smart contract automation, blockchain infrastructures can establish tamper-resistant healthcare systems with improved accountability and operational transparency.

3.1. Key Use Cases of Blockchain in Healthcare

Blockchain technology has gained significant attention across several healthcare domains due to its ability to provide secure, transparent, and decentralized data management capabilities. In the following, we discuss a few such use cases, and Table 1 further describes the benefits of blockchain in healthcare.

Table 1. Benefits of Blockchain Technology in E-Health.

Attribute	Healthcare Benefit/(s)
Data Integrity	Ensures that EHRs cannot be altered after being committed to the distributed ledger, preventing unauthorized modification and retroactive tampering.
Transparency	Provides auditable and timestamped transaction histories accessible to authorized healthcare stakeholders.
Decentralization	Eliminates reliance on centralized custodians and reduces single points of failure within healthcare infrastructures.
Security	Protects healthcare information through cryptographic hashing, distributed consensus mechanisms, and smart contract-based access control.
Patient Empowerment	Enables patients to dynamically manage permissions and revoke access to personal health records when necessary.

- EHR management

Blockchain-based EHR systems enable secure storage and controlled sharing of patient medical records while preserving data integrity and confidentiality. Healthcare records stored through blockchain architectures become tamper-resistant and accessible only to authorized entities using cryptographic authentication mechanisms. In addition, smart contracts facilitate automated consent management, secure access control, and auditable healthcare transactions [27,28].

- Pharmaceutical supply chain monitoring

Blockchain technology improves transparency and traceability throughout pharmaceutical supply chains by enabling end-to-end tracking of drugs from manufacturers to patients. This capability helps reduce counterfeit medicine distribution, ensures compliance with temperature-controlled transportation requirements, and strengthens product authenticity verification [29].

- Telemedicine and remote healthcare services

The rapid growth of telemedicine platforms and remote healthcare monitoring systems has increased the need for secure communication infrastructures. Blockchain-based frameworks support encrypted medical data exchange, secure remote consultations, and trusted inter-institutional communication among healthcare providers, thereby improving the reliability of distributed healthcare services [3].

- Healthcare insurance and dispute resolution

Smart contract-enabled blockchain systems can automate insurance claim verification, billing procedures, and healthcare dispute resolution processes. Automated verification mechanisms reduce fraudulent activities, improve operational transparency, and enhance trust among healthcare stakeholders [30].

3.2. Limitations of Current Blockchain Implementations

Despite its advantages, blockchain technology still faces several technical and operational limitations that restrict its large-scale adoption in healthcare systems as follows.

- **Bandwidth and transaction throughput limitations**

Public blockchain infrastructures often experience limited transaction throughput and high latency under large-scale workloads. Healthcare systems generate substantial volumes of clinical and IoMT data, making conventional public blockchain architectures insufficient for handling real-time healthcare transactions efficiently [31].

- **Scalability challenges**

Direct on-chain storage of large healthcare datasets, including medical imaging and continuous IoMT monitoring data, is both economically and computationally inefficient. Consequently, hybrid architectures combining blockchain-based metadata management with off-chain storage systems are generally preferred for scalable healthcare deployments [32].

- **Interoperability barriers**

Integrating blockchain infrastructures with legacy EHR systems, heterogeneous medical devices, and healthcare communication standards remains technically complex and resource intensive. The absence of universally adopted interoperability frameworks further complicates the seamless exchange of healthcare data across institutions [33].

- **Privacy and regulatory constraints**

Although blockchain provides transparency and immutability, these characteristics may conflict with regulatory requirements such as GDPR and HIPAA, particularly regarding data modification, deletion rights, and cross-border data governance. Maintaining patient privacy while preserving blockchain auditability, therefore, remains an ongoing research challenge.

- **Quantum security vulnerabilities**

Most existing blockchain systems rely on classical cryptographic primitives such as RSA, SHA-256, and ECDSA for transaction authentication and integrity verification. These mechanisms are theoretically vulnerable to future quantum computing attacks, particularly through Shor's and Grover's algorithms [2,34]. Consequently, transitioning toward quantum-resilient cryptographic infrastructures has become increasingly important for securing next-generation healthcare blockchain ecosystems.

4. Quantum Computing: Principles and Healthcare Applications

Quantum computing represents a transformative computational paradigm based on the principles of quantum mechanics. Unlike classical computing systems, which process information using binary bits represented as either 0 or 1, quantum computing utilizes quantum bits (qubits) that can exist in multiple states simultaneously through the phenomenon of superposition. This capability enables quantum systems to perform highly parallel computations and solve specific classes of problems significantly faster than classical computers [35]. The computational advantage of quantum computing is primarily derived from three fundamental quantum-mechanical principles:

- **Superposition:**

A qubit can simultaneously exist in a combination of multiple states, enabling parallel computation across a vast solution space and significantly increasing computational efficiency relative to classical systems.

- **Entanglement:**

Quantum entanglement establishes strong correlations between qubits such that the state of one qubit becomes dependent on another, regardless of physical distance. This

phenomenon enables highly complex computational interactions and forms the foundation of Quantum Key Distribution (QKD) protocols.

- **Quantum interference:**

Quantum interference amplifies correct computational outcomes while suppressing incorrect solutions through constructive and destructive wave interactions. This principle is extensively utilized in quantum algorithms such as Grover's search algorithm and quantum Fourier transform-based computations [36].

Overall, these quantum-mechanical properties enable several promising applications across healthcare and biomedical domains, which are further discussed in the next subsection.

4.1. Healthcare Applications of Quantum Computing

- **Pharmaceutical and drug discovery**

Quantum computing can significantly accelerate pharmaceutical research by simulating molecular and atomic-scale interactions with higher computational precision than classical systems. Quantum simulations support faster identification of drug candidates, protein interaction analysis, and optimization of complex biochemical processes, thereby reducing drug development time and cost [37].

- **Genomic and precision medicine analysis**

Quantum algorithms offer substantial potential for accelerating genomic sequencing, mutation analysis, and large-scale biological data processing. These capabilities can enhance precision medicine workflows by enabling more efficient identification of genetic variations and personalized treatment strategies [38].

- **Medical imaging and diagnostics**

Quantum-enhanced image reconstruction and noise-reduction techniques can improve the quality and diagnostic accuracy of medical imaging modalities such as Magnetic Resonance Imaging (MRI) and Computed Tomography (CT). Advanced quantum algorithms may further support faster image processing and real-time diagnostic analysis [39].

- **Healthcare resource optimization**

Quantum optimization techniques, including quantum annealing, can improve healthcare logistics by optimizing hospital resource allocation, patient scheduling, treatment planning, and pharmaceutical supply chain management. Such approaches may significantly enhance operational efficiency within large-scale healthcare systems [40].

- **Quantum-Safe Healthcare Security**

Quantum computing introduces both opportunities and challenges for healthcare cybersecurity. While future large-scale quantum computers may threaten existing cryptographic infrastructures, quantum technologies also provide advanced security mechanisms. QKD, PQC, and QRNG offer promising approaches for establishing quantum-resilient healthcare communication and data protection systems [41–44].

4.2. Current Limitations and Future Outlook

Despite its transformative potential, quantum computing technology remains in an early stage of development. Current quantum systems are constrained by limited qubit stability, noise susceptibility, error correction challenges, and high hardware complexity [45]. Consequently, present-day quantum computers are not yet capable of practically breaking widely deployed cryptographic systems at scale.

Nevertheless, major technology organizations, including IBM and Google, continue to make substantial progress toward fault-tolerant quantum computing architectures [18]. As quantum hardware advances over the coming decades, the security implications for classical cryptographic systems and blockchain infrastructures are expected to become increasingly significant. This emerging transition highlights the urgent need for quantum-resilient security mechanisms capable of protecting future healthcare ecosystems against both classical and quantum-enabled cyber threats.

5. Quantum Threats to Blockchain-Based E-Health Systems

Blockchain-based e-health systems rely heavily on classical cryptographic primitives to ensure authentication, integrity, confidentiality, and non-repudiation. In many widely deployed blockchain infrastructures, elliptic-curve signatures such as ECDSA are used for transaction signing and identity authentication, while hash functions such as SHA-256 support block integrity, transaction validation, and, in public networks, proof-of-work consensus. It should be emphasized, however, that cryptographic choices vary considerably across platforms: blockchain systems combine different signature schemes (e.g., Ed25519, Schnorr, BLS), hash functions (e.g., SHA-3/Keccak, BLAKE2), consensus mechanisms, and permission models, and permissioned healthcare ledgers such as Hyperledger Fabric typically avoid proof-of-work altogether. The threat analysis below therefore applies to the common configurations that rely on quantum-vulnerable primitives rather than to all blockchain systems uniformly. Although these primitives are secure against classical adversaries, they may become vulnerable in the presence of sufficiently powerful quantum computers [16,17,46].

Shor's algorithm represents one of the most significant quantum threats to blockchain security. It can solve integer factorization and elliptic curve discrete logarithm problems in polynomial time, thereby undermining the security assumptions of RSA, ECDH, and ECDSA-based systems [16,47]. In blockchain-enabled healthcare environments, this could allow an adversary to recover private keys, forge digital signatures, impersonate healthcare entities, and authorize fraudulent transactions. Such attacks may compromise the integrity of patient records, enable unauthorized access to sensitive medical data, or disrupt trust among hospitals, insurers, laboratories, and patients.

Grover's algorithm introduces a more limited, complementary threat to symmetric cryptography and cryptographic hash functions. It provides only a quadratic speedup for unstructured search and does not break SHA-256: it is the preimage and second-preimage resistance of the function that would be degraded, from 2^{256} to approximately 2^{128} quantum operations, while collision resistance is affected even less; both remain far beyond foreseeable quantum resources once realistic quantum-circuit costs and error-correction overheads are taken into account [17,48]. The practical impact therefore depends on which security property is targeted: mining-style search problems and proof-of-work difficulty assumptions are the most exposed, whereas hash-based integrity verification in permissioned healthcare ledgers is affected only marginally and can be hardened by doubling hash output lengths. The consequences of quantum-enabled attacks are particularly severe in e-health environments because medical data is highly sensitive, long-lived, and safety-critical. Compromised cryptographic credentials could allow attackers to manipulate patient records, falsify prescriptions, forge clinical authorizations, disrupt medical supply chains, or gain unauthorized access to insurance and billing systems [3,49]. Unlike many financial records, healthcare records must often remain confidential and trustworthy for decades, making them vulnerable to "harvest now, decrypt later" attacks, where encrypted medical data is collected today and decrypted once quantum capabilities mature.

Security agencies and standardization bodies have increasingly recognized the long-term risks posed by quantum computing compared to classical public-key cryptography. Although practical large-scale quantum attacks are not yet feasible, the potential future compromise of widely deployed schemes such as RSA and ECDSA highlights the urgent need for proactive migration toward quantum-safe cryptographic infrastructures [41,50]. Therefore, blockchain-based e-health systems must transition to post-quantum cryptography, quantum-secure key management, and hybrid migration strategies to ensure long-term resilience. For a better understanding, Table 2 provides a threat assessment of blockchain components in e-health.

Table 2. Quantum Threat Assessment of Blockchain Components in E-Health.

Blockchain Component	Quantum Vulnerability Description	Severity
Digital signatures (ECDSA)	Shor’s algorithm can solve the elliptic curve discrete logarithm problem in polynomial time, enabling private key recovery, signature forgery, and identity impersonation.	Critical
Key exchange (ECDH/RSA)	Shor’s algorithm can compromise ECDH and RSA-based key exchange mechanisms, enabling retroactive decryption of harvested encrypted healthcare communications.	Critical
Hash functions (SHA-256)	Grover’s algorithm reduces the effective security strength of brute-force search operations, weakening hash-based integrity verification and proof-of-work assumptions.	Moderate
Smart contract logic	Smart contracts that depend on cryptographic signature verification or hash-based authentication may be bypassed through forged or compromised cryptographic inputs.	Medium
Key management	Poorly protected private keys stored on-chain, in centralized repositories, or in vulnerable devices may become exposed through quantum-assisted cryptanalysis or weak key-management practices.	High
EHR integrity verification	If hash-based anchoring or signature verification is weakened, the reliability of tamper detection and long-term medical record integrity may be compromised.	Moderate

6. Opportunities: Quantum-Enhanced E-Health Blockchain

The emergence of quantum computing introduces significant security challenges for existing blockchain infrastructures; however, it also creates new opportunities for developing quantum-resilient healthcare systems. To protect blockchain-enabled e-health ecosystems against future quantum-enabled cyber threats, integrating quantum-safe technologies has become increasingly important. In particular, four major technological directions are emerging as key enablers of secure next-generation healthcare blockchain infrastructures.

6.1. Post-Quantum Cryptography

PQC refers to cryptographic algorithms designed to remain secure against attacks from both classical and quantum computers. In 2024, the National Institute of Standards and Technology (NIST) standardized several PQC algorithms under FIPS 203, FIPS 204, and FIPS 205 to support future quantum-resilient communication systems [41–43].

The adoption of PQC within blockchain infrastructures can significantly strengthen the long-term security of healthcare systems by replacing vulnerable cryptographic primitives such as RSA and ECDSA. Blockchain platforms, including Ethereum and Hyperledger, have already begun research into integrating PQC mechanisms into transaction authentication, key exchange, and digital signature verification [51]. In healthcare environments, PQC-based systems may provide secure EHR management, quantum-resilient patient authentication, and protected inter-institutional data exchange.

6.2. Quantum Key Distribution

QKD provides theoretically secure key exchange mechanisms based on the principles of quantum mechanics. Protocols such as BB84 [44] and E91 [52] leverage quantum phenomena, including superposition and the no-cloning theorem, to detect eavesdropping attempts during communication. Importantly, the security guarantees of QKD hold only under specific theoretical and implementation assumptions: QKD distributes symmetric key material but requires an authenticated classical channel, and it does not by itself provide endpoint security, application-level authentication, or availability. Eavesdropping detection is statistical rather than instantaneous—an elevated quantum bit error rate above a predefined threshold indicates probable interception—and practical implementations may deviate from ideal models through device imperfections [53].

In healthcare systems, QKD can enhance the confidentiality and integrity of sensitive medical communications between hospitals, laboratories, insurance providers, and telemedicine platforms. By ensuring secure cryptographic key generation and exchange, QKD can strengthen the protection of EHR systems, patient monitoring infrastructures, and remote healthcare services against future quantum-enabled interception attacks.

Recent advancements in satellite-assisted QKD have further extended secure quantum communication over long distances, enabling large-scale and cross-border healthcare communication infrastructures [54]. Although QKD was previously limited to laboratory-scale implementations, ongoing developments indicate growing potential for deployment in national and enterprise-level healthcare networks.

6.3. Quantum Random Number Generation

Secure cryptographic systems rely heavily on high-quality random number generation for encryption keys, authentication tokens, and digital signatures. Conventional pseudo-random number generators may become vulnerable to prediction or cryptanalysis under advanced attack scenarios. QRNG utilizes inherently unpredictable quantum processes to generate truly random values, thereby improving cryptographic security [55,56]. In blockchain-enabled healthcare systems, QRNG can strengthen authentication protocols, patient consent management systems, and cryptographic key generation processes by reducing the risk of predictable or compromised random number sequences.

6.4. Quantum-Enhanced Optimization in Healthcare Systems

Quantum computing techniques, including quantum annealing and hybrid variational algorithms, offer promising opportunities for optimizing complex healthcare operations [40]. When integrated with blockchain-enabled healthcare infrastructures, these techniques may improve:

- hospital resource allocation,
- patient scheduling,
- emergency response coordination,
- medical supply chain optimization,
- and large-scale healthcare data analytics.

Such optimization capabilities can enhance operational efficiency while maintaining secure and transparent healthcare management through blockchain-based infrastructures.

6.5. Toward Quantum-Resilient Healthcare Ecosystems

The convergence of blockchain technology with PQC, QKD, QRNG, and quantum-enhanced optimization techniques represents a promising direction for the development of secure next-generation healthcare ecosystems. Together, these technologies can improve data confidentiality, trust management, interoperability, and long-term resilience against

quantum-enabled cyber threats. However, despite these opportunities, several technical, operational, and regulatory challenges remain unresolved, including hardware limitations, computational overhead, interoperability constraints, and large-scale deployment feasibility. These challenges are discussed further in the upcoming sections.

7. Hybrid Frameworks, Architectures, and the Proposed QBSA

The convergence of blockchain technology and quantum-security mechanisms has stimulated the development of next-generation architectures for secure healthcare systems. Existing research demonstrates growing interest in integrating PQC, QKD, QRNG, and blockchain infrastructures to establish quantum-resilient e-health ecosystems. However, most current implementations remain fragmented, application-specific, or limited to conceptual and prototype-level deployments. Based on the structured literature analysis conducted in this review, five major categories of hybrid quantum-blockchain healthcare frameworks were identified. These frameworks are comparatively analyzed in Table 3 alongside the proposed Quantum-Blockchain Security Architecture (QBSA).

7.1. Systematic Comparison of Existing Studies

Table 3 presents a comparative analysis of 20 representative studies addressing the intersection of blockchain, quantum security, and healthcare systems. The comparison evaluates each framework according to cryptographic approach, blockchain (BC) platform, healthcare application domain, primary security objective, implementation maturity, and key technical limitations.

The 20 studies were selected from the review corpus and from the foundational and enabling-technology literature cited throughout this article (non-corpus entries are marked †) according to four criteria: (i) coverage—every major technology category identified in the corpus (QKD-based, PQC-based, hybrid, consent-oriented, IoMT-oriented, and enabling quantum-communication technologies) is represented by at least two studies; (ii) architectural completeness—preference was given to studies describing an implementable architecture or system over purely positional papers; (iii) citation impact within the corpus; and (iv) diversity of blockchain platforms and healthcare contexts. Surveys and non-healthcare enabling-technology demonstrations (e.g., satellite QKD) are retained deliberately and are labelled as such, because they define the technological envelope within which healthcare architectures must operate; the table is accordingly presented as a comparison of representative studies rather than of healthcare implementations. Maturity levels are assigned from the evidence reported in each study using the following six-level maturity scale (applied consistently in Table 3): Conceptual/Theoretical—architecture or analysis only, with no implementation; Experimental—partial implementation evaluated in a laboratory setting; Prototype—an end-to-end working implementation evaluated at limited scale; Near-production—an implementation evaluated on production-grade infrastructure or in a pilot deployment; Field-tested/Demonstrated—operation demonstrated in a real operational environment; and Survey—a secondary study synthesizing prior work. For the corpus studies in this comparison, the assigned maturity level and its supporting evidence are recorded in Supplementary Table S2; foundational and enabling-technology entries (marked †) are classified from their original publications. Thematically, the corpus itself is dominated by 2023–2025 proposals for quantum-resistant EHR sharing, IoMT authentication, and quantum-assisted or federated healthcare architectures [57–59] (Supplementary Table S2), which corroborates the trend analysis presented in this section.

Table 3. Systematic comparison of 20 representative studies at the blockchain-quantum-healthcare intersection.

Study	Cryptography	BC Platform	Healthcare Context	Primary Challenge	Maturity	Key Limitation
Gajjar et al. [3]	QKD (BB84)	Hyperledger	Telehealth	Channel confidentiality	Prototype	Distance-limited QKD
Prajapat et al. [4]	PQC + GenAI	IoT Ledger	IoMT Healthcare	Device authentication	Experimental	Computational overhead
Mondal et al. [5]	Quantum + FL + BC (AI-driven)	Hybrid BC	Personalized medicine	Unified AI-quantum-BC analytics	Conceptual/Theoretical	Limited security evaluation
Agarwal et al. [1]	PQC (Hybrid)	Hyperledger Fabric	Healthcare 5.0	Quantum-resistant access control	Prototype	Limited scale testing
Alam et al. [2]	PQC Analysis	Ethereum	EHR Management	Quantum threat modelling	Conceptual/Theoretical	No implementation
Fernandez-Carames [26] †	Lattice PQC	Generic BC	IoT Security	Post-quantum BC survey	Survey	No healthcare focus
Sun et al. [60] †	PQC + QRNG	Custom Ledger	EHR Sharing	Decentralised key mgmt	Prototype	Single-institution only
Yang et al. [51] †	PQC (multiple schemes)	Multiple platforms	Generic (cross-domain)	PQC-quantum BC survey	Survey	No healthcare focus
Rathee et al. [61] †	Hybrid Crypto	Blockchain-IoT	Remote Monitoring	Secure IoT-BC bridge	Prototype	No PQC integration
Dagher et al. [33] †	ABE + Hashing	Ethereum	EHR Access Control	Patient privacy	Prototype	Quantum-vulnerable
Albanese et al. [62] †	Consent smart contracts	Private permissioned BC	Clinical Consent	Revocable consent	Prototype	No quantum resilience
Griggs et al. [14] †	HTTPS + BC Hash	Ethereum	Remote Monitoring	Automated health alerts	Prototype	SHA-256 vulnerability
Kuo et al. [10] †	Standard BC Crypto	Various	Biomedical Data	Data provenance	Survey	Quantum-vulnerable
Azaria et al. [28] †	RSA + BC	Ethereum	EHR Permissions	Patient data access	Prototype	RSA breakable by Shor
Das et al. [63] †	Hybrid classical + PQC	Hyperledger Fabric	Permissioned BC	Quantum-safe consensus	Prototype	Limited health context
Shen et al. [64] †	AES + digest chains	Custom ledger (MedChain)	Data Sharing	Interoperability	Prototype	No PQC component
Yin et al. [54] †	Entangled QKD	N/A (channel)	Satellite Comms	Long-distance QKD	Field-tested/Demonstrated	No BC integration
Ebrahimi et al. [65] †	Lattice PQC (crypto-processor)	— (no ledger)	Edge/IoT medical devices	Constrained-device PQC	Experimental	No blockchain integration
Liao et al. [66] †	Satellite QKD	N/A	Telecom Backbone	QKD at continental scale	Field-tested/Demonstrated	No health application
Tanwar et al. [13] †	ECDSA + SHA-256	Hyperledger Fabric	EHR Sharing	Data taxonomy	Survey	Quantum-vulnerable

The structured analysis presented in Table 3 reveals several important research observations. First, most existing studies focus on isolated components of quantum-secure healthcare systems rather than fully integrated architectures. Some frameworks primarily investigate blockchain-based healthcare management, whereas others focus independently on QKD communication or PQC-enabled authentication mechanisms. Comprehensive end-to-end integration of blockchain, PQC, QKD, and healthcare interoperability remains limited.

Second, many existing implementations remain at conceptual, experimental, or prototype stages. Large-scale deployment evaluations, real-world healthcare integration, and interoperability validation are still insufficiently explored. Third, lightweight quantum-safe cryptographic mechanisms suitable for constrained IoMT environments remain an open challenge. Although several studies propose lightweight PQC approaches, computational overhead, latency, and memory limitations continue to restrict practical deployment on wearable healthcare devices and edge-based medical systems. Overall, these findings highlight the need for unified, scalable, and quantum-resilient healthcare security architectures capable of integrating blockchain governance, post-quantum cryptography, secure communication, and healthcare interoperability standards.

7.2. Proposed Four-Layer Quantum-Blockchain Security Architecture (QBSA)

Based on the identified research gaps and the comparative findings summarized in Table 3, this study proposes a novel four-layer QBSA for secure e-health ecosystems. The

proposed architecture integrates quantum-safe cryptographic mechanisms, blockchain governance, and healthcare interoperability technologies to provide end-to-end protection for healthcare data and communication infrastructures. The QBSA consists of four interconnected layers, as illustrated in Figure 2.

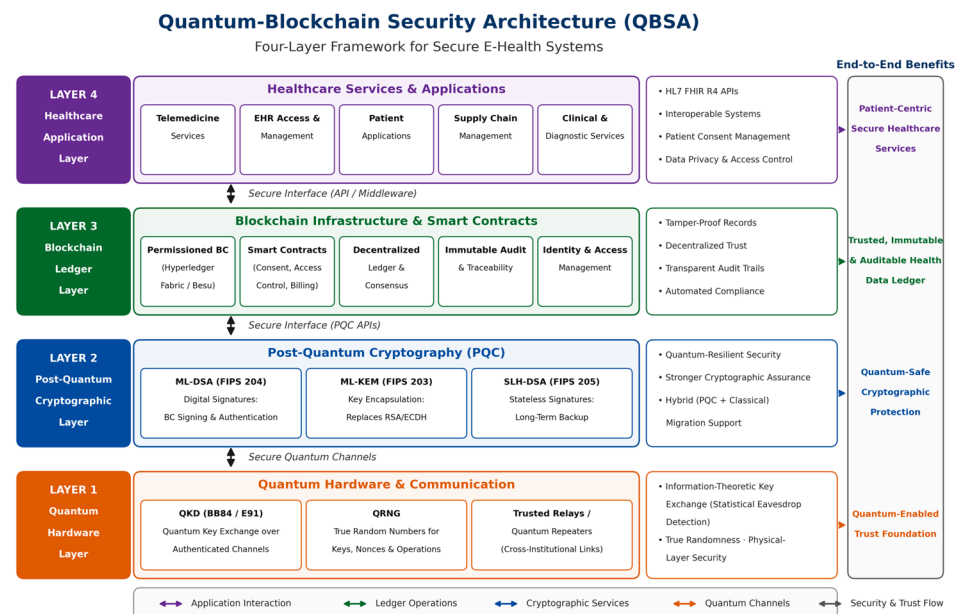


Figure 2. Proposed Four-Layer Quantum-Blockchain Security Architecture (QBSA) for Secure E-Health System.

- **Layer 1—Quantum Hardware Layer**

The hardware layer forms the foundational trust infrastructure of the proposed architecture. This layer integrates QKD and QRNG technologies to establish secure cryptographic foundations for healthcare communication systems. QKD protocols such as BB84 and E91 enable theoretically secure cryptographic key exchange between healthcare institutions by leveraging quantum-mechanical properties and the no-cloning theorem, with the classical reconciliation channel authenticated by post-quantum message authentication. For cross-institutional distances beyond direct fiber links, Layer 1 can accommodate trusted-relay QKD nodes where the requisite quantum-communication infrastructure is deployed and, as the technology matures, quantum repeaters [67]; both are treated here as deployment assumptions and forward-looking options rather than presently ubiquitous healthcare infrastructure. Simultaneously, QRNG mechanisms generate highly unpredictable random values for secure cryptographic operations, authentication systems, and key generation processes. Together, these technologies establish a quantum-resilient foundation for secure healthcare communication.

- **Layer 2—Post-Quantum Cryptographic Layer**

The cryptographic layer integrates NIST-standardized PQC algorithms to replace vulnerable classical cryptographic mechanisms.

- ML-DSA (FIPS 204) replaces ECDSA for blockchain transaction signing and node authentication.
- ML-KEM (FIPS 203) replaces RSA and ECDH for secure key encapsulation and exchange.
- SLH-DSA (FIPS 205) provides stateless backup signature functionality for long-term cryptographic resilience.

To support gradual migration from legacy systems, the architecture adopts a hybrid cryptographic model in which classical and post-quantum algorithms operate simultaneously during transitional deployment phases.

- Layer 3—Blockchain Ledger Layer

The blockchain layer provides decentralized governance, immutable auditing, and secure healthcare transaction management. Healthcare records are anchored on permissioned blockchain infrastructures such as Hyperledger Fabric or Hyperledger Besu. Smart contracts automate patient consent management, access control enforcement, insurance adjudication, and healthcare transaction validation. A federated ledger model enables multiple healthcare institutions to maintain sovereign data ownership while participating in a shared and auditable trust infrastructure.

- Layer 4—Healthcare Application Layer

The application layer includes user-facing healthcare services and interoperable clinical systems. Applications communicate through standardized HL7 FHIR R4-compliant APIs to support interoperability across hospitals, telemedicine platforms, laboratories, and IoMT ecosystems. Lightweight PQC mechanisms are integrated into constrained medical devices to support secure authentication and encrypted communication. In addition, blockchain-linked pharmaceutical supply chain modules provide secure provenance tracking, while patient-facing applications support dynamic consent revocation and privacy-preserving healthcare data sharing.

7.3. Technical Comparison of NIST-Standardized PQC Algorithms for E-Health Deployment

Table 4 provides a comparative technical evaluation of NIST-standardized PQC algorithms relevant to blockchain-based healthcare systems. RSA-2048 is included as a classical reference for comparison.

Table 4. Technical comparison of NIST-standardized PQC algorithms and selected classical/pre-standard schemes for e-health blockchain. Key and signature/ciphertext sizes are taken from FIPS 203/204/205 [41–43]; FN-DSA (FALCON) sizes from the NIST third-round report [49]; embedded performance is characterized by pqm4 benchmarks on ARM Cortex-M4 [68].

Algorithm	Standard/Status	Function	Public-Key Size (Bytes)	Signature/Ciphertext Size (Bytes)	NIST Security Category	Size Overhead vs. Classical (sig. ct + pk)
ML-KEM-768	FIPS 203 (2024) [41]	Key-encapsulation mechanism	1184	1088 (ct)	Category 3	$\approx 4.4\times$ vs. RSA-2048
ML-KEM-1024	FIPS 203 (2024) [41]	Key-encapsulation mechanism	1568	1568 (ct)	Category 5	$\approx 6.1\times$ vs. RSA-2048
ML-DSA-65	FIPS 204 (2024) [42]	Digital signature	1952	3309 (sig.)	Category 3	$\approx 54\times$ vs. ECDSA-P256
ML-DSA-87	FIPS 204 (2024) [42]	Digital signature	2592	4627 (sig.)	Category 5	$\approx 74\times$ vs. ECDSA-P256
SLH-DSA-SHA2-128s	FIPS 205 (2024) [43]	Digital signature (stateless, hash-based)	32	7856 (sig.)	Category 1	$\approx 81\times$ vs. ECDSA-P256
FN-DSA-512 (FALCON-512) ‡	Draft FIPS 206 (forthcoming) ‡	Digital signature	897	≈ 666 (sig.)	Category 1	$\approx 16\times$ vs. ECDSA-P256
RSA-2048 (classical ref.)	PKCS #1/FIPS 186 (classical)	Public-key encryption/signature	256	256	Quantum-insecure (Shor)	$1\times$ (reference)
ECDSA-P256 (classical ref.)	FIPS 186 (classical)	Digital signature	33 (compressed)	64	Quantum-insecure (Shor)	$1\times$ (reference)

‡ FALCON is planned for standardization as FN-DSA in the forthcoming FIPS 206; it is not standardized in FIPS 203, 204, or 205 and is included here as a pre-standard candidate only. The FN-DSA-512

signature size is the average encoded length. ECDSA-P256 sizes refer to compressed public keys and raw 64-byte signatures. NIST security categories denote design-strength equivalence classes (Category 1 $\approx$ AES-128 key search, Category 3 $\approx$ AES-192, Category 5 $\approx$ AES-256), not measured attack costs. † Study cited from outside the systematic-search corpus (Section 1.3)—a foundational work, an enabling-technology study, or a background reference—included for comparative and historical context.

Table 4 deliberately reports objective, specification-derived quantities—key and signature/ciphertext sizes and NIST security categories—rather than qualitative performance labels. Runtime behavior is platform-dependent and is best characterized by reproducible embedded benchmarks: on an ARM Cortex-M4-class microcontroller, the pqm4 project reports ML-KEM operations completing on the order of one million clock cycles, ML-DSA-65 signing requiring a few million cycles (with verification several times faster), FN-DSA-512 signing being considerably more expensive on devices without floating-point acceleration despite its compact signatures, and SLH-DSA signing costing on the order of billions of cycles, which effectively confines it to non-interactive, long-term backup roles [68]. These characteristics indicate that ML-KEM-768 offers a practical balance of security and bandwidth for healthcare key encapsulation, that ML-DSA-65 is a reasonable default choice for blockchain transaction signing, and that compact-signature schemes such as FN-DSA-512 will become attractive for constrained IoMT links once FIPS 206 is finalized. A meaningful suitability assessment for IoMT devices must additionally account for key-generation cost, RAM and flash footprint, implementation complexity, numerical stability, side-channel resistance, and energy consumption; Section 7.7 therefore complements this table with a quantitative feasibility analysis, and Section 8.3 discusses lightweight deployment challenges.

7.4. QKD–Blockchain Integration Protocol

The integration of QKD with blockchain-enabled healthcare systems within the QBSA framework proceeds through four operational phases.

- Phase 1—Quantum key distribution

Healthcare institutions establish secure communication channels using QKD protocols such as BB84 or E91. Owing to quantum-mechanical properties and the no-cloning theorem, eavesdropping attempts perturb the exchanged quantum states and can be detected statistically: the measured quantum bit error rate is compared against a predefined threshold before any derived key is used. The classical post-processing channel is authenticated using post-quantum message authentication.

- Phase 2—Secure payload encryption

Patient data exchanged between healthcare institutions is encrypted using symmetric encryption mechanisms such as AES-256, where encryption keys are securely generated and distributed through QKD channels.

- Phase 3—Blockchain anchoring

Encrypted healthcare transactions, digital signatures, and integrity hashes are securely anchored onto the permissioned blockchain infrastructure. PQC-protected signatures ensure long-term tamper resistance and auditability.

- Phase 4—Authenticated retrieval and verification

Authorized healthcare entities retrieve encrypted medical records through cryptographically verified authentication mechanisms. Blockchain-based audit trails ensure traceability, accountability, and integrity verification throughout the data lifecycle.

Table 5 summarizes the maturity levels of existing hybrid quantum-blockchain healthcare frameworks and positions the proposed QBSA as a comprehensive conceptual architecture integrating quantum hardware, PQC, blockchain governance, and interoperable healthcare applications into a unified security model.

Table 5. Maturity Overview of Hybrid Quantum-Blockchain E-Health Frameworks. Maturity here denotes the integration maturity of the composite framework category, assessed with the six-level scale defined in Section 7.1, rather than the maturity of the individual cited studies.

Framework	Core Components	Target Use Case	Maturity Level	Key References
QKD-Enabled Blockchain EHR	QKD (BB84/E91) + Hyperledger	Secure inter-hospital record sharing	Prototype	[3,60]
Post-Quantum Smart Contracts	ML-DSA/SLH-DSA + Ethereum	EHR consent, insurance, research	Prototype	[51,63]
Quantum-IoMT Blockchain	QRNG + ML-KEM + IoMT Ledger	Wearable security, remote diagnostics	Experimental	[4,65]
Federated Q-Health Ledger	Permissioned BC + QKD + Fed. AI	Nationwide health data exchange	Conceptual/Theoretical	[5,64]
Quantum-Secured Consent System	ML-DSA + BC + Tokenisation	Genomics, clinical trials, donation	Prototype	[28,62]
Proposed QBSA (This Review)	4-Layer: HW/Crypto/Ledger/App	Comprehensive e-health integration	Conceptual/Theoretical	This work

7.5. Threat Model, Trust Assumptions, and Security Considerations

The QBSA is a conceptual architecture; accordingly, this subsection makes its underlying threat model and trust assumptions explicit and frames its protective properties as design objectives rather than experimentally validated guarantees.

Adversary model. The architecture considers a network adversary with full control over classical communication channels (a Dolev–Yao-style attacker able to intercept, replay, reorder, and inject messages) who may additionally (i) record encrypted traffic today for decryption once cryptographically relevant quantum computers become available (harvest-now-decrypt-later); (ii) mount key-recovery and signature-forgery attacks based on Shor’s algorithm against any residual RSA/elliptic-curve material; and (iii) compromise a bounded minority of consensus nodes or individual IoMT endpoints. Physical attacks on quantum hardware, malicious insiders holding legitimate administrative credentials, and denial-of-service attacks on the underlying network are addressed only partially—through auditability and redundancy—and remain open problems.

Trust assumptions. The model assumes that (i) the certificate and membership authorities of the permissioned ledger are honest at enrollment time; (ii) the classical post-processing channel of QKD is authenticated using PQC-based message authentication, since QKD itself does not provide entity authentication; (iii) trusted-relay QKD nodes, where used, are operated within the security perimeter of participating institutions; and (iv) endpoint devices execute cryptographic operations correctly, with IoMT devices provisioned with device-unique credentials at manufacture or enrollment.

Key lifecycle and data-management decisions. Patient data are stored off-chain in institutional repositories; only PQC-signed integrity digests, consent states, and access-control events are anchored on-chain. This on-chain/off-chain split keeps large clinical objects (e.g., medical imaging) off the ledger and enables GDPR-compatible erasure: deleting or re-keying the off-chain object and destroying its encryption key (crypto-shredding) renders the immutable on-chain digest permanently uninterpretable while preserving

the audit trail. Keys follow a defined lifecycle—generation (QRNG-seeded), distribution (ML-KEM encapsulation, or QKD where links exist), scheduled and event-driven rotation, revocation through certificate-status transactions on the ledger, and escrow-free backup via institutional key-management services. Patient consent revocation is enforced by smart contracts that invalidate access tokens at the ledger layer. IoMT devices are enrolled through a registration transaction binding the device identity to its PQC public key; compromised devices are removed by revoking that binding, which consensus nodes enforce on all subsequent transactions. When QKD infrastructure is unavailable or out of range, the architecture degrades gracefully to a PQC-only mode (ML-KEM key establishment over classical channels), so quantum hardware remains an enhancement rather than a single point of failure. Table 6 maps the threats identified in Section 5 to the corresponding architectural controls.

Table 6. Mapping of identified quantum-era threats to QBSA controls.

Threat (cf. Section 5)	QBSA Layer	Architectural Control	Residual Risk
Signature forgery/key recovery via Shor’s algorithm (ECDSA, RSA)	Layer 2	ML-DSA transaction signing; ML-KEM key establishment; hybrid dual-signing during migration	Implementation flaws; side-channel leakage
Harvest-now-decrypt-later interception of medical communications	Layers 1–2	AES-256 payload encryption with QKD-derived or ML-KEM-encapsulated keys	Metadata exposure; traffic analysis
Grover-accelerated attacks on hash-based integrity	Layer 3	Extended-output hashing (e.g., SHA-384/SHA-3) for anchoring and audit trails	Long-term hash-migration effort
Compromised or spoofed IoMT devices	Layers 2/4	PQC device identities; on-chain enrollment and revocation transactions	Physical device capture
Malicious or faulty consensus nodes	Layer 3	Permissioned membership; fault-tolerant consensus; immutable audit trails	Collusion above the fault threshold
Unauthorized access and consent violations	Layers 3–4	Smart-contract consent enforcement; RBAC/ABE access control	Insider misuse of valid credentials

End-to-end protection, scalability, interoperability, patient control, and quantum resilience should therefore be read as design objectives of the QBSA. Their formal verification—through security proofs, simulation, or prototype evaluation—is part of the research agenda described in Sections 7.7 and 9.3, and data-flow and sequence diagrams for the principal clinical workflows are planned as part of the prototype specification.

7.6. Positioning of the QBSA Against Existing Frameworks

Table 7 positions the proposed architecture against the five framework categories identified in the corpus (cf. Tables 3 and 5) across the capability dimensions that Sections 2–6 established as requirements for quantum-resilient e-health.

The novelty of the QBSA therefore lies not in any individual technology—each of which has been studied in isolation—but in three specific aspects. First, to the best of our knowledge, within the reviewed corpus, it is one of the few identified healthcare-specific architectures that explicitly align with the finalized 2024 NIST PQC standards (FIPS 203/204/205) rather than with pre-standard candidate algorithms. Second, it integrates all four quantum-security building blocks (PQC, QKD, QRNG, and hybrid migration) with permissioned blockchain governance and HL7 FHIR R4 interoperability in a single layered

model, whereas prior frameworks combine at most two of these elements (Table 7). Third, it makes the quantum-to-application trust chain explicit, defining how quantum-generated keys propagate upward through the cryptographic, ledger, and application layers under an explicit threat model (Section 7.5), with a graceful PQC-only fallback when quantum hardware is unavailable.

Table 7. Capability comparison of the proposed QBSA with existing hybrid quantum-blockchain healthcare framework categories.

Framework Category	PQC (FIPS 203–205)	QKD	QRNG	FHIR Interop.	IoMT Path	Consent Mgmt.	Explicit Threat Model
QKD-enabled blockchain EHR [3,60]	No	Yes	Partial	No	No	Partial	No
Post-quantum smart contracts [51,63]	Partial (pre-standard)	No	No	No	No	Partial	Partial
Quantum-IoMT ledger [4,65]	Partial	No	Yes	No	Yes	No	No
Federated Q-health ledger [5,64]	No	Partial	No	Partial	No	Partial	No
Quantum-secured consent [28,62]	No	No	No	No	No	Yes	No
Proposed QBSA (this work)	Yes (FIPS 203/204/205)	Yes (with relay path)	Yes	Yes (HL7 FHIR R4)	Yes (lightweight PQC)	Yes (smart contracts)	Yes (Section 7.5)

7.7. Quantitative Feasibility Considerations

As a review, this study does not present a new experimental implementation; nevertheless, the practical feasibility of the QBSA can be bounded quantitatively from specification data and published benchmarks. Accordingly, all performance and feasibility figures reported here and in Section 8.2 are specification-based projections or values inferred from published benchmarks, not measurements obtained from an implementation of the QBSA. Table 8 quantifies the per-transaction bandwidth cost of post-quantum and hybrid signing for a representative blockchain transaction carrying a 250-byte payload.

Table 8. Per-transaction signature overhead of NIST-standardized signature schemes relative to ECDSA-P256 (sizes from FIPS 204/205 [42,43]; 250-byte payload; 1 MB reference block).

Scheme	Signature + Public Key (Bytes)	Overhead vs. ECDSA (×)	Approx. Signature-Carrying Transactions per 1 MB Block
ECDSA-P256 (classical)	97	1.0	≈3000
ML-DSA-65	5261	≈54	≈190
Hybrid (ECDSA + ML-DSA-65)	5358	≈55	≈187
FN-DSA-512 (pre-standard)	1563	≈16	≈578
SLH-DSA-SHA2-128s	7888	≈81	≈129

Three observations follow. First, block capacity for signature-carrying transactions drops by roughly one order of magnitude when moving from ECDSA to ML-DSA-65, which translates into proportionally lower throughput at a constant block size and block interval, or into larger blocks and higher propagation latency at constant throughput; in permissioned deployments such as Hyperledger Fabric or Besu, where no gas market exists, the cost appears as increased block size, endorsement-message volume, and storage growth rather than fees. Published integration studies corroborate feasibility: PQFabric demonstrated hybrid classical/post-quantum signatures in Hyperledger Fabric with moderate end-to-end overhead dominated by signature size [63], and recent surveys reach consistent

conclusions across platforms [51]. Second, during a hybrid migration phase, an IoMT device must transmit both a classical and a PQC signature, adding roughly 3.4 kB of signature payload per message for ECDSA plus ML-DSA-65 (excluding certificates)—negligible on hospital networks but material on low-power wide-area medical links, which motivates compact schemes such as FN-DSA-512 (≈ 1.6 kB including the public key) once FIPS 206 is finalized. Third, embedded benchmarks (pqm4, ARM Cortex-M4) show ML-KEM and ML-DSA operations completing within milliseconds at typical microcontroller clock rates, whereas SLH-DSA signing requires seconds, confirming the Layer-2 role assignments in the QBSA [68]. For QKD, reported field deployments constrain the design space: metropolitan fiber links sustain kilobit-per-second secret-key rates over tens of kilometres, trusted-relay backbones extend range at the cost of relay trust, and satellite links have demonstrated intercontinental reach at lower key rates [53,54,66]; the QBSA therefore reserves QKD-derived keys for high-value inter-institutional channels and relies on ML-KEM elsewhere. A full prototype implementing the QBSA on Hyperledger Fabric with liboqs-based signing, including a sensitivity analysis across classical, hybrid, and fully post-quantum configurations, is identified as priority future work in Section 9.3.

8. Challenges and Open Research Problems

Despite the significant potential of integrating blockchain and quantum technologies within healthcare systems, several technical, operational, and regulatory challenges remain unresolved. These limitations currently restrict the large-scale deployment of quantum-resilient healthcare infrastructures and highlight important directions for future research.

8.1. Immature Quantum Hardware Infrastructure

One of the primary limitations of quantum-enabled healthcare security systems is the immaturity of current quantum hardware technologies. Existing quantum computing and quantum communication infrastructures remain highly sensitive to environmental noise, thermal instability, and qubit decoherence, which significantly affect operational reliability and scalability [53].

In addition, current QKD systems are constrained by communication distance limitations. Although secure quantum communication has been demonstrated over long distances through satellite-assisted QKD systems, maintaining stable quantum channels across large-scale healthcare networks remains technically complex [54,66]. Signal degradation, infrastructure cost, and deployment complexity further limit the feasibility of implementing quantum-secure communication systems in geographically distributed or rural healthcare environments. Consequently, substantial advancements in fault-tolerant quantum hardware, quantum repeaters, and scalable communication infrastructures are required before practical large-scale healthcare deployment becomes feasible. Within the proposed QBSA, these distance limitations are addressed at Layer 1: for metropolitan and regional scales, trusted-relay QKD nodes operated inside the security perimeters of participating institutions can bridge cross-institutional links, while emerging quantum repeaters—once they reach operational maturity—would remove the need to trust intermediate relay sites and enable end-to-end quantum key distribution across national healthcare networks [67]. Institutions located beyond QKD reach fall back to the PQC-only operating mode described in Section 7.5, so the availability of quantum hardware never becomes a prerequisite for baseline security.

8.2. PQC Integration Overhead in Blockchain Systems

Post-Quantum Cryptography algorithms generally require significantly larger public keys, ciphertexts, and digital signatures compared with classical cryptographic schemes.

Although these algorithms provide strong resistance against quantum-enabled attacks, their computational and storage overhead introduce important performance challenges for blockchain infrastructures [51,69].

Healthcare blockchain systems already process large volumes of medical transactions, IoMT communications, and access-control operations. The integration of large PQC signatures and key-management structures may increase transaction latency, block size, storage requirements, and network communication overhead. Consequently, redesigning blockchain architectures to efficiently support PQC mechanisms without degrading healthcare system performance remains a major research challenge. The magnitude of this overhead can be made concrete using the specification data in Table 4: replacing a 64-byte ECDSA signature with a 3309-byte ML-DSA-65 signature multiplies the per-transaction signature payload by roughly fifty, and SLH-DSA signatures approach 8 kB. In permissioned deployments such as Hyperledger Fabric or Besu—where no gas market exists—this manifests as larger endorsement messages, faster ledger growth, and a reduced number of signature-carrying transactions per block (on the order of a tenfold reduction at a fixed block size; see Table 8), whereas in gas-based platforms equivalent costs would appear as substantially higher per-transaction fees. During a hybrid migration phase, every message additionally carries both signature families, so constrained IoMT uplinks bear the combined payload of roughly 3.4 kB per message for ECDSA plus ML-DSA-65 (excluding certificates); Section 7.7 quantifies these costs and the compact-signature alternatives.

8.3. Lightweight PQC for IoMT Environments

The deployment of quantum-safe cryptographic mechanisms in IoMT environments presents an additional challenge due to the constrained computational capabilities of many medical devices. Wearable sensors, implantable medical devices, and edge healthcare systems often operate with highly limited memory, processing power, and energy availability [61,65]. Many existing IoMT devices have only a few kilobytes of RAM and limited flash storage, making it difficult to implement computationally intensive PQC algorithms. Although lightweight PQC approaches are currently being investigated, balancing security strength, computational efficiency, latency, and energy consumption remains a largely unresolved problem. Developing lightweight and resource-efficient post-quantum security mechanisms specifically optimized for constrained healthcare environments, therefore, represents a critical future research direction.

8.4. Regulatory, Ethical, and Legal Challenges

The integration of blockchain and quantum-security technologies within healthcare systems introduces significant regulatory and ethical complexities. Existing regulatory frameworks, including GDPR and HIPAA, were not originally designed to address decentralized quantum-resilient healthcare infrastructures or cross-border quantum-secure communication systems [48,62]. On the other hand, several unresolved legal questions remain, including determining responsibility in the event of cross-border data breaches, defining ownership and governance of distributed healthcare records, establishing standards for quantum-safe data retention, and ensuring compliance with patient privacy regulations within immutable blockchain environments. Failure to address these challenges may reduce public trust and hinder the adoption of quantum-enhanced healthcare technologies.

8.5. Interoperability and Standardization Gaps

Another major challenge involves the lack of standardized interoperability frameworks across blockchain platforms, PQC systems, healthcare communication protocols, and quantum-security infrastructures. Current healthcare ecosystems rely on heterogeneous

standards such as HL7 FHIR and DICOM, while blockchain and PQC implementations often operate using incompatible architectures [33,69]. The absence of internationally accepted standards for integrating blockchain, quantum-safe cryptography, and healthcare interoperability mechanisms creates significant barriers to large-scale deployment. Without standardized frameworks, integrating legacy hospital systems with quantum-resilient blockchain infrastructures remains technically difficult and operationally expensive. Accordingly, future research must focus on developing interoperable architectures, standardized migration strategies, and globally accepted governance frameworks to support secure and scalable quantum-resilient healthcare ecosystems.

8.6. Summary of Research Challenges

The transition toward quantum-resilient blockchain-based healthcare systems remains a multidisciplinary challenge involving cryptography, distributed systems, healthcare informatics, networking, regulation, and quantum engineering. Although existing research demonstrates promising progress, practical deployment still requires substantial advancements in scalable quantum hardware, lightweight PQC mechanisms, interoperable healthcare standards, regulatory governance, and secure real-world implementation strategies. Addressing these challenges will be essential for enabling trustworthy, secure, and future-proof healthcare infrastructures capable of operating in the emerging quantum era.

9. Future Research Directions

Addressing the challenges discussed in the previous section requires a coordinated and interdisciplinary research strategy involving cybersecurity, healthcare informatics, quantum engineering, distributed systems, and regulatory governance. Based on the gap analysis presented in Table 3, several critical future research directions can be identified for the development of secure and scalable quantum-resilient healthcare ecosystems.

9.1. Lightweight PQC for Resource-Constrained Healthcare Devices

One of the most important research priorities is the development of lightweight post-quantum cryptographic mechanisms optimized for constrained IoMT environments. Many wearable healthcare devices, implantable sensors, and edge-based monitoring systems operate using low-power processors such as ARM Cortex-M architectures with highly limited memory and computational resources. Thus, future research should focus on optimizing PQC implementations for constrained medical hardware, minimizing cryptographic latency and energy consumption, and developing lightweight secure communication protocols for healthcare environments. Algorithms such as ML-KEM and FALCON-512 represent promising candidates for developing PQC-optimized TLS handshake protocols suitable for real-time healthcare communication systems.

9.2. PQC-Native Blockchain Architectures

Most existing blockchain platforms were originally designed using classical cryptographic assumptions and therefore require substantial modification to support post-quantum security. Future blockchain infrastructures should be designed with quantum resilience as a foundational architectural requirement rather than as an external add-on mechanism. Hence, research efforts should focus on PQC-native smart contract execution environments, quantum-resilient consensus protocols, secure post-quantum identity management, and hybrid migration frameworks for legacy healthcare systems. In addition, healthcare interoperability standards such as HL7 FHIR R4 should be enhanced to support secure integration with PQC-enabled blockchain infrastructures and decentralized healthcare identity systems [51,63].

9.3. Federated Quantum-Blockchain Healthcare Testbeds

The practical deployment of quantum-secure healthcare systems requires realistic experimental environments that can evaluate interoperability, scalability, and security performance under real-world healthcare conditions. Future research should therefore prioritize the development of federated quantum-blockchain healthcare testbeds integrating QKD simulators, PQC-enabled blockchain platforms, IoMT communication systems, and existing hospital information infrastructures. Such test environments would enable comprehensive validation of the proposed Quantum-Blockchain Security Architecture (QBSA) and support performance evaluation within operational healthcare ecosystems. As an immediate next step, we plan a minimal QBSA prototype on Hyperledger Fabric using liboqs-based ML-DSA signing, reporting transaction latency, throughput, block-size growth, signature-verification time, memory footprint, and energy consumption on constrained IoMT hardware, together with a sensitivity analysis contrasting classical, hybrid classical/PQC, and fully post-quantum configurations (cf. Section 7.7).

9.4. Ethical, Legal, and Regulatory Framework Development

The emergence of decentralized quantum-resilient healthcare systems introduces new ethical and legal considerations that extend beyond existing regulatory frameworks. Current regulations, such as GDPR and HIPAA, provide limited guidance regarding quantum-secure healthcare communication, decentralized patient identity management, cross-border healthcare data governance, and immutable blockchain-based medical records. Future interdisciplinary research should focus on developing globally accepted governance frameworks that ensure patient privacy protection, data sovereignty, transparent consent management, and regulatory compliance in distributed healthcare environments. Mechanisms such as reversible consent, privacy-preserving identity management, and quantum-safe auditability may play a critical role in future healthcare governance models [48,62].

9.5. AI-Quantum-Blockchain Convergence

The convergence of AI, blockchain technology, and quantum computing represents one of the most promising future directions for next-generation healthcare systems. AI-driven healthcare analytics combined with quantum-enhanced optimization and blockchain-based trust management may significantly improve personalized medicine, predictive diagnostics, genomic analysis, healthcare automation, and secure collaborative medical research. Federated learning models integrated with blockchain infrastructures may further support privacy-preserving distributed AI training while maintaining patient data confidentiality. Simultaneously, PQC and QKD mechanisms can provide quantum-resilient protection for inter-institutional AI communication and distributed healthcare analytics [60,63].

9.6. Toward Next-Generation Quantum-Resilient Healthcare Ecosystems

The future of secure digital healthcare will likely depend on the successful integration of blockchain governance, quantum-safe cryptography, AI, and interoperable healthcare communication infrastructures. Although current technologies remain at relatively early stages of maturity, continued advancements in quantum computing, PQC standardization, and decentralized healthcare systems are expected to accelerate the development of secure and patient-centric healthcare ecosystems. Consequently, future research should emphasize scalable implementation strategies, interdisciplinary collaboration, and practical deployment validation to ensure the safe transition toward trustworthy quantum-resilient healthcare infrastructures.

10. Conclusions

This study has systematically examined the convergence of blockchain technology and quantum computing within e-health systems through the analysis of 57 peer-reviewed studies published between January 2018 and June 2025. The findings demonstrate that although blockchain technology has significantly improved healthcare data management through decentralization, transparency, auditability, and secure information sharing, existing blockchain infrastructures remain vulnerable to future quantum-enabled attacks due to their dependence on classical cryptographic primitives such as RSA, ECDSA, and SHA-256. The analysis highlights that quantum algorithms, particularly Shor's and Grover's algorithms, pose substantial long-term threats to blockchain-based healthcare systems by potentially compromising digital signatures, key exchange mechanisms, and hash-based integrity verification processes. As healthcare data is highly sensitive, long-lived, and safety-critical, the transition toward quantum-resilient security infrastructures has become an increasingly important requirement for future digital healthcare ecosystems. This review further demonstrates that blockchain technology continues to provide significant advantages for patient-centric healthcare management through distributed trust, tamper-resistant medical record storage, decentralized governance, and secure multi-institutional collaboration. However, the long-term sustainability of these systems depends on the successful integration of quantum-safe cryptographic mechanisms capable of resisting future quantum computing threats.

The comparative analysis of existing studies revealed several important research gaps across the hardware, cryptographic, ledger, and application layers. Current implementations remain fragmented, with limited integration between blockchain infrastructures, PQC, QKD, and healthcare interoperability frameworks. In response to these limitations, this study proposed the Quantum-Blockchain Security Architecture, a four-layer conceptual framework designed to support secure, scalable, and quantum-resilient healthcare systems. Despite the promising opportunities offered by quantum-enhanced healthcare security, several open challenges remain unresolved. These include immature quantum hardware infrastructures, computational overhead associated with PQC deployment, lightweight security requirements for constrained IoMT devices, interoperability limitations, and the absence of globally standardized regulatory frameworks for quantum-secure healthcare systems. Future healthcare ecosystems will likely depend on the successful convergence of blockchain governance, post-quantum cryptography, quantum-secure communication, and AI-driven healthcare analytics. Consequently, interdisciplinary collaboration among researchers, healthcare providers, cybersecurity experts, policymakers, and standardization bodies will be essential for developing trustworthy, scalable, and patient-centric healthcare infrastructures capable of operating securely in the emerging quantum era.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/electronics15173831/s1>, Supplementary File S1: Advancing Blockchain and Quantum Technologies for Secure E-Health Systems: A Systematic Review and Conceptual Security Framework—Supplementary methodological documentation (database-specific search strategies, screening procedure, and PRISMA 2020 checklist); Supplementary Table S1 (characteristics and classification of the 57 included studies). Supplementary Table S2—57 included studies. The full bibliographic details of all 57 included studies are provided in Supplementary Table S2; those not cited elsewhere in the main text are listed here for completeness as references [70–118].

Funding: This research was funded by the Deanship of Graduate Studies and Scientific Research, Qassim University, project number QU-APC-2026.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University (<https://www.qu.edu.sa>) for financial support (QU-APC-2026).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Agarwal, N.; Kankanampati, P.K.; Chamrathy, S.S.; Khan, I.; Jain, A.; Almusawi, M. Blockchain and quantum cryptography-based hybrid security for Healthcare 5.0 systems. In *Proceedings of the 3rd International Conference Computing, Communication, Perception and Quantum Technology (CCPQT)*, Zhuhai, China, 25–27 October 2024; IEEE: New York, NY, USA, 2024. [CrossRef]
2. Alam, S.; Shuaib, M.; Sam, S.M.; Hassan, N.H.; Usman, S.; Samy, G.N. Effect of quantum computing on blockchain-based EHR systems. In *Proceedings of the 2022 4th International Conference on Smart Sensors and Application (ICSSA)*, Kuala Lumpur, Malaysia, 26–28 July 2022; pp. 16–21. [CrossRef]
3. Gajjar, H.; Jivani, D.; Trivedi, C.; Gupta, R.; Jadav, N.K.; Tanwar, S.; Rodrigues, J.J. Blockchain and quantum-based collaborative communication framework for telehealth. In *Proceedings of the 2024 IEEE International Conference on E-health Networking, Application & Services (HealthCom)*, Nara, Japan, 18–20 November 2024. [CrossRef]
4. Prajapat, S.; Kumar, P.; Das, A.K.; Muhammad, G. Generative AI-enabled quantum encryption for IoT-based healthcare using blockchain. *IEEE Internet Things J.* **2025**, *12*, 24541–24551. [CrossRef]
5. Mondal, S.; Das, S.; Golder, S.S.; Bose, R.; Sutradhar, S.; Mondal, H. AI-driven big data analytics for personalized medicine in healthcare: Integrating federated learning, blockchain, and quantum computing. In *Proceedings of the 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAQSA)*, Nagpur, India, 20–21 December 2024; IEEE: New York, NY, USA, 2024; pp. 1–6. [CrossRef]
6. Hireche, R.; Mansouri, H.; Pathan, A.S.K. Security and privacy management in Internet of Medical Things (IoMT): A synthesis. *J. Cybersecur. Priv.* **2022**, *2*, 640–661. [CrossRef]
7. IBM Security. *Cost of a Data Breach Report 2023*; IBM Corp.: Armonk, NY, USA, 2023. Available online: <https://www.ibm.com/reports/data-breach> (accessed on 11 August 2026).
8. Health Service Executive. *Conti Cyberattack on the HSE Ireland: Independent Post Incident Review*; PwC Ireland: Dublin, Ireland, 2021. Available online: <https://about.hse.ie/publications/conti-cyber-attack-on-the-hse-independent-post-incident-review/> (accessed on 11 August 2026).
9. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
10. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health data applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef]
11. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56. [CrossRef]
12. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
13. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based EHR system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
14. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef]
15. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing in mobile healthcare applications. In *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, Canada, 8–13 October 2017; pp. 1–5. [CrossRef]
16. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
17. Grover, L.K. A Fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*; Association for Computing Machinery: New York, NY, USA, 1996; pp. 212–219. [CrossRef]
18. IBM Research. *IBM Quantum Development Roadmap 2023–2033*; IBM Corp.: Armonk, NY, USA, 2023. Available online: <https://www.ibm.com/roadmaps/quantum/> (accessed on 11 August 2026).
19. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Martinis, J.M. Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505–510. [CrossRef]
20. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Moher, D. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Br. Med. J.* **2021**, *372*, n71. [CrossRef]
21. Hasselgren, A.; Kravetska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef] [PubMed]

22. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. GDPR-compliant personal data management: A blockchain-based solution. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1746–1761. [\[CrossRef\]](#)
23. Jalali, M.S.; Landman, A.B.; Gordon, W.J. Telemedicine, privacy, and information security in the age of COVID-19. *J. Am. Med. Inform. Assoc.* **2021**, *28*, 671–672. [\[CrossRef\]](#)
24. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [\[CrossRef\]](#)
25. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334. [\[CrossRef\]](#)
26. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* **2020**, *8*, 21091–21116. [\[CrossRef\]](#)
27. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [\[CrossRef\]](#)
28. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [\[CrossRef\]](#)
29. Musamih, A.; Salah, K.; Jayaraman, R.; Arshad, J.; Debe, M.; Al-Hammadi, Y.; Ellahham, S. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* **2021**, *9*, 9728–9743. [\[CrossRef\]](#)
30. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. [\[CrossRef\]](#)
31. Benchoufi, M.; Ravaud, P. Blockchain technology for improving clinical research quality. *Trials* **2017**, *18*, 335. [\[CrossRef\]](#)
32. Oktian, Y.E.; Lee, S.G.; Lee, H.J. BorderChain: Blockchain-based access control framework for the Internet of Things endpoint. *IEEE Access* **2021**, *9*, 3592–3615. [\[CrossRef\]](#)
33. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for EHR access control using blockchain. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [\[CrossRef\]](#)
34. Fernandez-Carames, T.M. From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for IoT. *IEEE Internet Things J.* **2019**, *7*, 6457–6480. [\[CrossRef\]](#)
35. Gyongyosi, L.; Imre, S. A survey on quantum computing technology. *Comput. Sci. Rev.* **2019**, *31*, 51–71. [\[CrossRef\]](#)
36. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*, 10th anniv. ed.; Cambridge University Press: Cambridge, MA, USA, 2010. [\[CrossRef\]](#)
37. Flöther, F.F. The state of quantum computing applications in health and medicine. *Res. Dir. Quantum Technol.* **2023**, *1*, e10. [\[CrossRef\]](#)
38. Emani, P.S.; Warrell, J.; Anticevic, A.; Bekiranov, S.; Gandal, M.; McConnell, M.J.; Harrow, A.W. Quantum computing at the frontiers of biological sciences. *Nat. Methods* **2021**, *18*, 701–709. [\[CrossRef\]](#)
39. Elaraby, A. Quantum medical images processing foundations and applications. *IET Quantum Commun.* **2022**, *3*, 201–213. [\[CrossRef\]](#)
40. Ur Rasool, R.; Ahmad, H.F.; Rafique, W.; Qayyum, A.; Qadir, J.; Anwar, Z. Quantum computing for healthcare: A review. *Future Internet* **2023**, *15*, 94. [\[CrossRef\]](#)
41. FIPS 203; Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2024. [\[CrossRef\]](#)
42. FIPS 204; Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2024. [\[CrossRef\]](#)
43. FIPS 205; Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2024. [\[CrossRef\]](#)
44. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [\[CrossRef\]](#)
45. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2018**, *2*, 79. [\[CrossRef\]](#)
46. Mosca, M. Cybersecurity in an era of quantum computers: It's time to act. *IEEE Secur. Priv.* **2018**, *16*, 38–41. [\[CrossRef\]](#)
47. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [\[CrossRef\]](#)
48. Mavroedis, V.; Vishi, K.; Zych, M.D.; Jøsang, A. The impact of quantum computing on present cryptography. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 405–414. [\[CrossRef\]](#)
49. Alagic, G.; Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Smith-Tone, D. *Status Report on the Third Round of the NIST PQC Standardization Process*; NISTIR 8413-upd1; NIST: Gaithersburg, MD, USA, 2022. [\[CrossRef\]](#)
50. National Institute of Standards and Technology. *NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards*; NIST: Gaithersburg, MD, USA, 2024. [\[CrossRef\]](#)

51. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Di Pietro, R.; Erbad, A. A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 967–1002. [[CrossRef](#)]
52. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [[CrossRef](#)] [[PubMed](#)]
53. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Wallden, P. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [[CrossRef](#)]
54. Yin, J.; Li, Y.H.; Liao, S.K.; Yang, M.; Cao, Y.; Zhang, L.; Pan, J.W. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **2020**, *582*, 501–505. [[CrossRef](#)]
55. Ma, X.; Xu, F.; Xu, H.; Tan, X.; Qi, B.; Lo, H.K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **2013**, *87*, 062327. [[CrossRef](#)]
56. Jennewein, T.; Simon, C.; Weihs, G.; Weinfurter, H.; Zeilinger, A. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **2000**, *84*, 4729. [[CrossRef](#)]
57. Hu, J.W. Enhancing healthcare data-sharing security with blockchain and post-quantum cryptography. *J. Mech. Med. Biol.* **2025**, *25*, 2540040. [[CrossRef](#)]
58. Yadav, V.; Hajarnis, P.; Minu, R.I. Unlocking clinical trial efficiency and security with blockchain and quantum technology. In *Proceedings of the 2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), Erode, India, 20–22 January 2025*; IEEE: New York, NY, USA, 2025; pp. 161–165. [[CrossRef](#)]
59. Sardar, T.H.; Dar, S.A.; Indhumathi, R.; Dhasmana, G.; Guru Prasad, M.S.; Kumar, P. Integrating blockchain and quantum key exchange with deep learning for enhanced medical data security. *Procedia Comput. Sci.* **2025**, *259*, 1208–1217. [[CrossRef](#)]
60. Sun, X.; Kulicki, P.; Sopek, M. Lottery-like blockchain protocol for quantum-safe decentralised EHR management. *Entropy* **2022**, *24*, 1830. [[CrossRef](#)]
61. Rathee, G.; Iqbal, R.; Waqar, O.; Bashir, A.K. Secure blockchain-based hybrid framework for IoT in healthcare. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5953–5961.
62. Albanese, G.; Calbimonte, J.P.; Schumacher, M.; Calvaresi, D. Dynamic consent management for clinical trials via private blockchain technology. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 4909–4926. [[CrossRef](#)]
63. Das, B.; Holcomb, A.; Mosca, M.; Pereira, G. PQFabric: A permissioned blockchain secure from both classical and quantum attacks. In *Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021*; pp. 1–9. [[CrossRef](#)]
64. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [[CrossRef](#)]
65. Ebrahimi, S.; Bayat-Sarmadi, S.; Mosanaei-Boorani, H. Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT. *IEEE Internet Things J.* **2019**, *6*, 5500–5507. [[CrossRef](#)]
66. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Pan, J.W. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [[CrossRef](#)]
67. Azuma, K.; Economou, S.E.; Elkouss, D.; Hilaire, P.; Liu, L.; Lo, H.K.; Tzitrin, I. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.* **2023**, *95*, 045006. [[CrossRef](#)]
68. Kannwischer, M.J.; Rijneveld, J.; Schwabe, P.; Stoffelen, K. pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4. IACR Cryptol ePrint Arch. 2019. 2019/844. Available online: <https://eprint.iacr.org/2019/844> (accessed on 11 August 2026).
69. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Yellick, J. Hyperledger Fabric: A distributed OS for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference, Porto, Portugal, 23–26 April 2018*; pp. 1–15. [[CrossRef](#)]
70. Christo, M.S.; Anigo Merjora, A.; Partha Sarathy, G.; Priyanka, C.; Raj Kumari, M. An Efficient Data Security in Medical Report using Block Chain Technology. In *2019 International Conference on Communication and Signal Processing (ICCSP)*; IEEE: New York, NY, USA, 2019. [[CrossRef](#)]
71. Wu, G.; Wang, Y. The security and privacy of blockchain-enabled EMR storage management scheme. In *2020 16th International Conference on Computational Intelligence and Security (CIS)*; IEEE: New York, NY, USA, 2020. [[CrossRef](#)]
72. Bhavin, M.; Tanwar, S.; Sharma, N.; Tyagi, S.; Kumar, N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *J. Inf. Secur. Appl.* **2021**, *56*, 102673. [[CrossRef](#)]
73. Mirtskhulava, L.; Iavich, M.; Razmadze, M.; Gulua, N. Securing Medical Data in 5G and 6G via Multichain Blockchain Technology using Post-Quantum Signatures. In *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*; IEEE: New York, NY, USA, 2021. [[CrossRef](#)]
74. Qu, Z.; Zhang, Z.; Zheng, M. A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things. *Inf. Sci.* **2022**. [[CrossRef](#)]
75. Chen, X.; Xu, S.; Qin, T.; Cui, Y.; Gao, S.; Kong, W. AQ–ABS: Anti-Quantum Attribute-based Signature for EMRs Sharing with Blockchain. In *2022 IEEE Wireless Communications and Networking Conference (WCNC)*; IEEE: New York, NY, USA, 2022. [[CrossRef](#)]
76. El Azzaoui, A.; Sharma, P.; Park, J. Blockchain-based delegated Quantum Cloud architecture for medical big data security. *J. Netw. Comput. Appl.* **2022**, *198*, 103304. [[CrossRef](#)]

77. Liu, X.; Luo, Y.; Yang, X.; Wang, L.; Zhang, X. Lattice-Based Proxy-Oriented Public Auditing Scheme for Electronic Health Record in Cloud-Assisted WBANs. *IEEE Syst. J.* **2022**, *16*, 2968–2978. [\[CrossRef\]](#)
78. Xu, G.; Xu, S.; Cao, Y.; Yun, F.; Cui, Y.; Yu, Y.; Xiao, K. PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios. *Secur. Commun. Netw.* **2022**, *2022*, 3368819. [\[CrossRef\]](#)
79. Bansal, A.; Arju, Esha; Mehra, P.S. A Post-Quantum Consortium Blockchain Based Secure EHR Framework. In *2023 International Conference on IoT, Communication and Automation Technology (ICICAT)*; IEEE: New York, NY, USA, 2023. [\[CrossRef\]](#)
80. Venkatesh, R.; Hanumantha, B. A privacy-preserving quantum blockchain technique for electronic medical records. *IEEE Eng. Manag. Rev.* **2023**, *51*, 137–144. [\[CrossRef\]](#)
81. Selvarajan, S.; Mouratidis, H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Sci. Rep.* **2023**, *13*, 7107. [\[CrossRef\]](#)
82. Dasari, K.; Dongari, S.P.; Chirra, A.R.; Devireddy, S.S.; Boddireddy, H.R.; Mahmoud, M. Demystifying Quantum Blockchain for Healthcare. In *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*; IEEE: New York, NY, USA, 2023. [\[CrossRef\]](#)
83. Bovellev, R.; Campbell, R. Healthcare Blockchain Quantum Computing Threats and Opportunities. *Blockchain Healthc. Today* **2023**, *6*, 263. [\[CrossRef\]](#)
84. Yadav, D.K.; Yadav, D.; Pal, Y.; Chaudhary, D.; Sahu, H.; Manasa, A.S.L. Post Quantum Blockchain Assisted Privacy Preserving Protocol for Internet of Medical Things. In *2023 IEEE World Conference on Applied Intelligence and Computing (AIC)*; IEEE: New York, NY, USA, 2023. [\[CrossRef\]](#)
85. Zhao, Z.; Li, X.; Luan, B.; Jiang, W.; Gao, W.; Neelakandan, S. Secure Internet of Things (IoT) using a novel Brooks Iyengar quantum Byzantine Agreement-centered blockchain Networking (BIQBA-BCN) model in smart healthcare. *Inf. Sci.* **2023**, *629*, 440–455. [\[CrossRef\]](#)
86. Karthikeyan, D. Secure Medical Data Transmission In Iot Healthcare: Hybrid Encryption, Post-Quantum Cryptography, and Deep Learning-Enhanced Approach. In *2023 Global Conference on Information Technologies and Communications (GCITC)*; IEEE: New York, NY, USA, 2023. [\[CrossRef\]](#)
87. Gupta, R.; Gupta, S.; Jadav, N.K.; Kakkar, R.; Tanwar, S. SORT: Blockchain and Onion Routing-Based Secure Telesurgery Framework for Healthcare 4.0. In *2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC)*; IEEE: New York, NY, USA, 2023. [\[CrossRef\]](#)
88. Alsubai, S.; Alqahtani, A.; Garg, H.; Sha, M.; Gumaei, A. A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records. *Complex Intell. Syst.* **2024**, *10*, 6117–6141. [\[CrossRef\]](#)
89. Venkatesh, R. A Lightweight Quantum Blockchain-Based Framework to Protect Patients Private Medical Information. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 3577–3584. [\[CrossRef\]](#)
90. Sabrina, F.; Sohail, S.; Tariq, U. A review of post-quantum privacy preservation for IoMT using blockchain. *Electronics* **2024**, *13*, 2962. [\[CrossRef\]](#)
91. Kodete, C.S.; Thuraka, B.; Pasupuleti, V. A Systematic Review of AI-Driven and Quantum-Resistant Security Solutions for Cyber-Physical Systems: Blockchain, Federated Learning, and Emerging Technologies. In *2024 International Conference on Computer and Applications (ICCA)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
92. Seng, V.L.K.; Wan, A.T.; Newaz, S.H.S.; Tsuchiya, T. Blockchain-Based Key State Management for IoT Devices in Post-Quantum Era. In *2024 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
93. Barj, S. CP-ABE-LWE-Based Smart Contract: A Novel Post-Quantum Smart Contract-Based Decentralized Application (DApp) for E-Health Records Management. In *2024 International Conference on Ubiquitous Networking (UNet)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
94. Venkatesh, R.; Hanumantha, B.S. Electronic medical records protection framework based on quantum blockchain for multiple hospitals. *Multimed. Tools Appl.* **2024**, *83*, 42721–42734. [\[CrossRef\]](#)
95. Venkatesh, R.; Darandale, S. Enhancing Healthcare Security with Quantum Blockchain: Electronic Medical Records Protection. In *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
96. Ramya, P.; Pooja, A.; Kumari, K.A. Ensuring Health Monitoring with Smart Glucometer using Ring Learning with Errors (RLWE) and Blockchain Integration for Enhanced Security. In *2024 First International Conference on Software, Systems and Information Technology (SSITCON)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
97. Zhukabayeva, T.; Rehman, A.U.; Tariq, N.; Benkhelifa, E. Hyperledger Fabric-Based Post Quantum Cryptography for Healthcare Application Using Discrete Event Simulation. *IEEE Access* **2024**, *12*, 192482–192493. [\[CrossRef\]](#)
98. Qu, Z.; Shi, W.; Liu, B.; Gupta, D.; Tiwari, P. IoMT-Based Smart Healthcare Detection System Driven by Quantum Blockchain and Quantum Neural Network. *IEEE J. Biomed. Health Inform.* **2024**, *28*, 3317–3328. [\[CrossRef\]](#)
99. Soni, L.; Chandra, H.; Gupta, D. Post-quantum attack resilience blockchain-assisted data authentication protocol for smart healthcare system. *Softw. Pract. Exp.* **2024**, *54*, 2170–2190. [\[CrossRef\]](#)

100. Qu, Z.; Meng, Y.; Liu, B.; Muhammad, G.; Tiwari, P. QB-IMD: A Secure Medical Data Processing System With Privacy Protection Based on Quantum Blockchain for IoMT. *IEEE Internet Things J.* **2024**. [\[CrossRef\]](#)
101. Akoramurthy, B.; Surendiran, B. QHealth: A Blockchain Based Smart Healthcare Consensus Method. In *2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IconSCEPT)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
102. Jain, K.; Singh, M.; Gupta, H.; Bhat, A. Quantum Resistant Blockchain-based Architecture for Secure Medical Data Sharing. In *2024 3rd Int Conf Applied Artificial Intelligence and Computing (ICAAIC)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
103. Prajapat, S.; Kumar, P.; Kumar, D.; Das, A.K.; Hossain, M.S.; Rodrigues, J.J.P.C. Quantum Secure Authentication Scheme for Internet of Medical Things Using Blockchain. *IEEE Internet Things J.* **2024**, *11*, 38496–38507. [\[CrossRef\]](#)
104. Grønli, T.; Lakhan, A.; Younas, M. Quantum-blockchain healthcare system for invasive and no-invasive-IoMT data. In *International Conference on Mobile Web and Intelligent Information Systems*; Springer: Cham, Switzerland, 2024. [\[CrossRef\]](#)
105. Mazumdar, H.; Chakraborty, C.; Venkatakrishnan, S.B.; Kaushik, A.; Gohel, H.A. Quantum-Inspired Heuristic Algorithm for Secure Healthcare Prediction Using Blockchain Technology. *IEEE J. Biomed. Health Inform.* **2024**, *28*, 3371–3378. [\[CrossRef\]](#)
106. Das, S.; Mondal, S.; Golder, S.S.; Sutradhar, S.; Bose, R.; Mondal, H. Quantum-Resistant Security for Healthcare Data: Integrating Lamport n-Times Signatures Scheme with Blockchain Technology. In *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
107. Balasubramaniam, A.; Surendiran, B. QUMA: Quantum unified medical architecture using blockchain. *Informatics* **2024**, *11*, 33. [\[CrossRef\]](#)
108. Hireche, R.; Mansouri, H.; Harbi, Y.; Pathan, A.K. Robust Group Authentication Using Quantum Cryptography and Smart Contract for IoMT. In *2024 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*; IEEE: New York, NY, USA, 2024. [\[CrossRef\]](#)
109. Zhu, D.; Sun, Y.; Li, N.; Song, L.; Zheng, J. Secure electronic medical records sharing scheme based on blockchain and quantum key. *Clust. Comput.* **2024**, *27*, 3037–3054. [\[CrossRef\]](#)
110. He, L.; Rao, S.; Tian, K.; Liu, Y.; Wang, J.; Liu, S.; Lu, X. A Post-Quantum Blockchain and Autonomous AI-Enabled Scheme for Secure Healthcare Information Exchange. *IEEE J. Biomed. Health Inform.* **2025**, *29*, 6883–6891. [\[CrossRef\]](#)
111. Thakre, G.; Raut, R.; Verma, P. A Review on AI—Enhanced Security in Blockchain and Cloud-Based Electronic Healthcare Records Systems. In *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*; IEEE: New York, NY, USA, 2025. [\[CrossRef\]](#)
112. Farouk, A.; Behera, B.K.; Ahmed, E.A. Design and Implement a Quantum Blockchain Framework to Secure 6G Communication for Consumer Applications. *IEEE Trans. Consum. Electron.* **2025**, *1*, 8417–8424. [\[CrossRef\]](#)
113. Bagchi, P.; Bisht, A.; Das, A.K.; Saxena, N.; Hossain, M.S. Designing Quantum-Safe Lattice-Based Multi-Authority CP-ABE Scheme for Blockchain-Enabled IoT-Based Consumer Healthcare Electronics. *IEEE Trans. Consum. Electron.* **2025**, *71*, 4983–4994. [\[CrossRef\]](#)
114. Selvagayathri, S.; Sasirekha, P.; Pranav, M.; Devi, M.V.; Rajasekaran, C. Next-Gen Healthcare Security: Quantum-Inspired Blockchain and Digital Twin Synergy. In *2025 International Conference on Advanced Computing Technologies (ICoACT)*; IEEE: New York, NY, USA, 2025. [\[CrossRef\]](#)
115. Roosan, D.; Khan, R.; Nirzhor, S.; Hai, F. Post-Quantum Cryptography Resilience in Telehealth using Quantum Key Distribution. *Blockchain Heal. Today* **2025**, *8*, 379. [\[CrossRef\]](#)
116. Commey, D.; Hounsino, S.G.; Crosby, G.V. Post-Quantum Secure Blockchain-Based Federated Learning Framework for Healthcare Analytics. *IEEE Netw. Lett.* **2025**. [\[CrossRef\]](#)
117. Natarajan, M.; Bharathi, A.; Varun, C.S.; Selvarajan, S. Quantum secure patient login credential system using blockchain for electronic health record sharing framework. *Sci. Rep.* **2025**, *7*, 126–129. [\[CrossRef\]](#)
118. Pongallu, D.R.; Arun, S.S.; Verma, R. SecureMedZK—A Blockchain-based Approach with Zero-Knowledge Rollups for Secure EHR. In *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*; IEEE: New York, NY, USA, 2025. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.