BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE
ORIGINAL RESEARCH

Post-Quantum Cryptography Resilience in Telehealth Using Quantum Key Distribution

Don Roosan, PharmD, PhD[1], Rubayat Khan, PhD[2], Saif Nirzhor, PhD[3] and Fahmida Hai, BSc[4]

[1]Associate Professor, Department of Computer Science, Merrimack College, North Andover, Massachusetts, USA; [2]Research Scientist, University of Nebraska Medical Center, Omaha, Nebraska, USA; [3]Postdoctoral Researcher, University of Texas, Southwestern Medical Center, Dallas, Texas, USA; [4]Research Scientist, Tekurai Inc, San Antonio, USA

Corresponding Author: Don Roosan, Email: roosand@merrimack.edu

DOI: https://doi.org/10.30953/bhty.v8.379

Keywords: attribute-based encryption (ABE), blockchain, post-quantum cryptography, quantum key distribution, telehealth, zero-knowledge proofs

The Addendum after the References defines the acronyms.

Abstract

Objective: The authors propose and evaluate a novel cybersecurity architecture for telehealth that is resilient against future quantum computing cyber threats. By integrating post-quantum cryptography (PQC) with quantum key distribution (QKD) and privacy-preserving mechanisms, data confidentiality and immutability for patient records in a post-quantum era are ensured.

Methods: A multi-layered design approach was adopted. The PQC algorithms (e.g. CRYSTALS-Dilithium) were integrated at the blockchain consensus layer to resist quantum attacks. A directed acyclic graph (DAG)-based ledger managed high transaction throughput and latency constraints typical of telehealth. A QKD-enhanced key management protocol leveraged quantum channels for secure exchanges. Zero-knowledge proofs (ZKPs) and secure multiparty computation (MPC) verified transactions without exposing sensitive patient data. A granular access control model used attribute-based encryption and smart contracts to govern which participants could view or modify encrypted medical records.

Results: The prototype was developed within a simulated telehealth network comprising hospitals, clinics, and patient devices. The PQC signatures at the consensus layer provided effective resistance to both classical and anticipated quantum attacks. The QKD facilitated secure key distribution, while ZKPs and MPC enabled validation of healthcare transactions without compromising patient privacy. Despite increased computational overhead, the DAG approach efficiently handled parallel transactions, indicating improved scalability compared to traditional linear blockchains.

Conclusion: A QKD-enhanced, PQC-driven framework successfully addresses critical security and privacy requirements, safeguarding medical data from emerging quantum threats. Although overhead and infrastructural costs are significant, sustained cryptographic resilience and robust patient confidentiality underscore its suitability for next-generation healthcare systems. Future studies should explore additional optimizations, homomorphic encryption, and larger-scale pilots under regulatory standards.

Plain Language Summary

Quantum computers threaten current encryption methods used in telehealth. This research secures remote healthcare by combining post-quantum cryptography (PQC) and quantum key distribution (QKD) with privacy tools such as zero-knowledge proofs (ZKPs) and attribute-based encryption (ABE). A specialized directed acyclic graph (DAG) ledger handles many transactions at once, storing only cryptographic references on-chain while keeping large patient data off-chain. By using CRYSTALS-Dilithium, a PQC algorithm, the system remains resistant to both classical and quantum attacks. QKD locks down the exchange of keys, alerting participants if spying is detected. ZKPs and multiparty computation (MPC) let healthcare providers verify data and prove their authorization without revealing sensitive details. This layered approach ensures patient privacy and high security without

creating slowdowns. Although setting up QKD adds some complexity and cost, the solution aims to be future-proof and adaptable as quantum computers improve. Testing showed that storing only metadata on the ledger preserves privacy while maintaining system performance. Next steps include exploring fully homomorphic encryption for even stronger privacy and piloting the system in real-world settings to meet regulatory requirements. This work demonstrates how telehealth can remain both accessible and secure against emerging quantum threats.

Submitted: January 12, 2025; Accepted: March 16, 2025; Published: April 25, 2025

The rapid digital transformation in healthcare offers unprecedented access to medical services across vast distances.[1] By mitigating geographic barriers and enabling remote diagnostics, telehealth can significantly improve patient outcomes while reducing costs.[2] However, these benefits bring heightened security risks, as sensitive data must be protected from unauthorized access and tampering.[3,4] Classical cryptographic protocols, including Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), rely on computational problems that emerging quantum computers may solve.[5] The advent of quantum computing thus poses a critical threat to telehealth security, potentially exposing patient records to malicious decryption.[6,7]

Post-quantum cryptography (PQC) aims to address this vulnerability by leveraging cryptographic schemes resistant to quantum attacks.[5] Alongside PQC, blockchain platforms offer transparency and immutability, but they typically rely on classical signatures.[8,9] As quantum capabilities mature, transitioning to quantum-resistant methods such as lattice-based or hash-based cryptography becomes vital.[10,11] Additionally, quantum key distribution (QKD) can strengthen key exchange processes, offering real-time interception alerts.[12] Innovative solutions like zero-knowledge proofs (ZKPs) and secure multiparty computation (MPC) further preserve privacy by limiting data exposure.[13,14] Against this backdrop, this article presents a novel framework integrating PQC, QKD, and blockchain to maintain confidentiality, integrity, and scalability in telehealth.

Methods

Designing a blockchain architecture that can withstand the demands of telehealth while concurrently addressing quantum-era threats requires a multi-faceted approach. Telehealth data can be highly sensitive, making confidentiality and integrity paramount.[4] Simultaneously, the advent of quantum computing demands an upgrade from classical cryptography to post-quantum solutions.[7] To reconcile these requirements, the following methodology incorporates five core elements: a post-quantum-based consensus mechanism, a directed acyclic graph (DAG) ledger for scalability, QKD for secure key management, privacy-preserving tools such as ZKPs and secure MPC, and a robust access control model that integrates attribute-based encryption (ABE) with post-quantum cryptographic schemes. Collectively, these elements aim to ensure efficiency, quantum resistance, and privacy protection in telehealth systems.[13]

The first step involves selecting post-quantum digital signatures to replace or augment classical algorithms in the blockchain consensus. Digital signatures are essential for verifying user identities and ensuring transaction integrity in telehealth applications, where data transmitted can include prescription records, patient updates, or insurance authorizations.[7] Classical algorithms such as RSA or ECC might be compromised by quantum attacks like those facilitated by Shor's algorithm.[14] The PQC provides alternatives that remain secure against classical and quantum adversaries.[4] Notable candidates include CRYSTALS-Dilithium, Falcon, and SPHINCS+, each evaluated based on security level, signature size, verification speed, and ease of integration.[5,6] CRYSTALS-Dilithium, for example, demonstrates relatively compact signatures and robust protection, making it suitable for telehealth contexts that demand rapid transaction throughput and low latency. By testing algorithms in controlled environments that simulate telehealth traffic volumes, the proposed methodology identifies which scheme best sustains performance without compromising the system's security.

After choosing a suitable post-quantum signature algorithm, the second step addresses scalability through a DAG-based ledger. Linear blockchain architectures can become bottlenecks under heavy transaction loads typical in telehealth, such as when multiple providers update patient data or when large volumes of sensor information stream from wearable devices.[9] A DAG structure allows for parallel insertion of transactions, as each transaction references one or more predecessors instead of a single chain. This design choice enhances throughput and lowers latency.[7] The telehealth network, composed of nodes representing hospitals, clinics, diagnostic centers, and patient devices, is configured so that transactions can be confirmed in parallel, alleviating computational congestion.[13] In addition, the node structure supports concurrency by verifying multiple transactions simultaneously, thereby more efficiently handling the data fluctuations

Citation: Blockchain in Healthcare Today 2025, 8: 379 - https://doi.org/10.30953/bhty.v8.379

that occur throughout a typical day of telehealth operations. Once integrated, the DAG ledger undergoes rigorous performance assessments, measuring metrics such as transaction confirmation times and energy consumption.[9] These evaluations confirm whether the DAG-based approach is viable in practice for large-scale deployments.

The third methodological aspect tackles key management via QKD. Although adopting post-quantum algorithms protects transaction signatures, weaknesses in key exchange protocols could allow attackers to intercept or store encrypted traffic for later decryption once quantum resources become available.[1] The QKD leverages the fundamental principles of quantum mechanics, particularly photon-based transmissions, to securely distribute cryptographic keys between nodes.[10] Any eavesdropping attempt alters the quantum state, which legitimate participants can detect as anomalies in the transmissions.[4] Integrating QKD into the telehealth blockchain network requires installing specialized QKD devices at critical network points, such as major hospitals or data centers, and establishing secure optical links. Key lifecycle management protocols determine how often keys are rotated or revoked to maintain a minimal risk window if a key is compromised.[14] The methodology also considers a hybrid approach in which QKD-derived keys are used to encrypt or protect the post-quantum signature keys themselves, thereby reinforcing layered security.[7] After setup, the network is tested through penetration simulations to ensure that neither classical hacking methods nor partial interception can subvert the QKD-secured channels.

Once the cryptographic underpinnings are established, the fourth methodological step introduces privacy-preserving mechanisms: ZKPs and secure MPC. Healthcare data are often subject to strict regulations that mandate minimizing patient data exposure.[4] ZKPs enable one party to prove certain statements, such as their authorization to modify a medical record, without disclosing details about that record.[6] This means that a blockchain node can confirm another node's legitimacy to perform specific actions while maintaining confidentiality. Typical implementations may utilize zk-SNARKs or Bulletproofs, though each carries computational overhead that must be measured against system throughput. MPC permits multiple entities—for instance, different hospitals—to perform joint analytics on collectively pooled data without revealing sensitive inputs to each other.[11] In a telehealth environment, MPC may facilitate collaborative research among clinics to evaluate treatment outcomes, all while preserving patient anonymity and compliance with privacy laws.[13] Both ZKPs and MPC demand significant computational resources, which may be off-loaded to specialized nodes or cloud-based accelerators.[9] In parallel, the system orchestrates seamless integration of these techniques with post-quantum signatures and QKD-protected channels, ensuring end-to-end security despite elevated computational requirements.

The fifth step extends privacy protections with a robust access control framework that combines ABE and post-quantum cryptographic primitives. Simple encryption alone is insufficient if all authorized users can freely read all patient records, as telehealth systems typically require fine-grained controls based on professional roles, jurisdictions, or certifications.[6] ABE enforces granular policies by encoding roles or attributes into the ciphertext, thus ensuring that only entities matching the defined attributes can decrypt patient data.[7] In practical terms, this means that only a patient's primary physician or an authorized specialist might be granted decryption rights, whereas administrative staff might have more limited access. By combining ABE with post-quantum encryption, the system mitigates quantum threats to data confidentiality. The methodology also leverages smart contracts in the DAG ledger, which document each policy change or key revocation as an auditable transaction.[13] This creates a permanent and transparent record of when access rights are updated or revoked, thereby satisfying accountability requirements in healthcare environments. The policy logic encoded in these contracts allows administrators to adapt to changes in staff roles or regulations without re-encrypting large swaths of data, further contributing to overall system scalability.

The methodology concludes with an extensive validation procedure encompassing functional, integration, performance, security, and compliance testing. Functional testing isolates each component—such as digital signatures, QKD devices, or ABE modules—and evaluates whether it meets specified requirements.[13] Integration testing then examines the interplay among components, focusing on edge cases like large network traffic or partial node failures.[5] Performance benchmarking simulates telehealth workloads with real-time data streams, high concurrency, and diverse user actions, measuring whether the system can uphold service-level requirements for data availability.[9] Security assessments include both theoretical analyses—evaluating the system's post-quantum security guarantees—and practical penetration tests, where ethical hackers attempt to exploit potential weak points.[10] Finally, user experience considerations address how healthcare providers interact with features like ZKPs or ABE-based decryption. The methodology ensures the system remains user-friendly and efficient, to encourage real-world adoption in time-critical clinical workflows.[1]

This multi-step methodology provides a holistic strategy for fortifying telehealth platforms against quantum-era cybersecurity threats. By introducing post-quantum signatures into the blockchain consensus, adopting a DAG-based ledger for scalability, incorporating QKD to secure key exchanges, employing privacy-preserving techniques

such as ZKPs and MPC, and enforcing a granular ABE-driven access control model, the architecture addresses a wide spectrum of security, privacy, and scalability challenges.[7] Although each step adds to system complexity and potential operational overhead, the result is a robust and future-oriented infrastructure capable of handling the escalating demands of telehealth while preserving patient data confidentiality.[4] This blueprint thereby outlines a feasible path to quantum-safe telehealth implementations, offering a strategic balance between innovation and regulatory compliance. By bridging cryptographic theory with the practical realities of large-scale healthcare environments, the methodology aims to inspire further research, pilot programs, and iterative improvements as quantum computing continues to evolve.

Results

The proposed architecture was developed and tested within a simulated telehealth network comprising a diverse set of nodes representing hospitals, clinics, patient devices, and ancillary services. Nodes communicated through both classical and quantum-simulated channels, enabling the integration of a DAG-based ledger for high throughput and CRYSTALS-Dilithium for post-quantum digital signatures.[5,7] Additionally, a specialized QKD simulation layer was introduced among selected nodes, facilitating secure key exchanges and strengthening the resilience of the entire network.[10] To accommodate telehealth's unique scalability needs, off-chain storage was utilized for the majority of large patient data files, while only essential metadata and cryptographic references resided on the ledger.[13]

Before operational testing, each node was equipped with a software module to handle CRYSTALS-Dilithium signatures. This post-quantum signature scheme was integrated into the consensus algorithm to authenticate transactions and ensure that only verified participants could append new blocks or references to the ledger.[6] In practice, the DAG-based structure permitted parallel validation of multiple transactions from different hospitals or clinics. For instance, a cardiology clinic could update patient electrocardiogram (ECG) data, at the same time, an oncology department added a new pathology report. Preliminary performance measurements showed a significant reduction in latency per transaction compared to a linear blockchain, particularly when tens of transactions arrived in close succession.[9] Although the computational overhead associated with PQC-based verification was noticeable, results indicated that throughput remained robust enough for telehealth applications that require near real-time responses.[4]

A crucial element of the design involved employing a QKD simulation layer to manage key exchanges for critical operations. Within the architecture, each node participating in high-security transactions received quantum-generated keys used to encrypt or sign data, thereby minimizing the possibility of interception by an adversary with quantum decryption capabilities.[1] In the simulation, these keys were periodically rotated, ensuring that even if a key were compromised, the duration for which it could be exploited remained limited.[7] As part of the test environment, a hypothetical attacker was modeled to eavesdrop on the quantum channel. Detected anomalies in photon transmission immediately triggered an alert that revoked the compromised key, underscoring the effectiveness of QKD in maintaining quantum-safe communications.[10]

Figure 1 and Table 1 depict the overall system architecture, illustrating the relationship between the DAG ledger elements, the QKD management modules, and the cryptographic libraries that implement PQC. In addition, Figure 1 highlights where ZKPs and ABE modules interact with the ledger. The arrows within Figure 1 demonstrate how nodes submit or reference transactions in the DAG, how QKD channels distribute keys, and how signatures are validated with CRYSTALS-Dilithium. This figure serves as a conceptual map for understanding the data flows and security layers that converge in the system.

During system operation, patient data, which typically include medical images, laboratory reports, and continuous monitoring feeds, were stored off-chain to preserve ledger efficiency and user privacy.[14] Rather than uploading these sizable files to the DAG, the architecture maintained encrypted references or hashes on-chain. Such references were essential for immutability and verifiability, ensuring that any modification to patient records would be detected instantly by comparing on-chain hashes to off-chain data.[4,11] In addition, this design streamlined the blockchain itself, as the ledger maintained only transaction records, cryptographic verifications, and minimal metadata.

To further strengthen privacy, the system incorporated ZKPs for on-chain validation. The ZKPs enabled nodes to demonstrate the legitimacy of certain clinical transactions, such as a physician's authorization to modify a patient's records, without disclosing any additional patient data.[6] Each node possessed a local proof generator that, upon receiving a request to upload or modify a record reference, constructed a proof verifying the action's authenticity. Other nodes in the network then validated this proof before finalizing the transaction on the DAG.[13] In practice, this approach significantly reduced the threat of data leakage because no raw patient details were placed on the ledger. Moreover, early testing revealed that incorporating ZKPs introduced a moderate computational overhead, but this cost was deemed acceptable in light of the amplified confidentiality.[9]

In tandem with ZKPs, ABE regulated off-chain data access. Whenever an authorized provider attempted to

Citation: Blockchain in Healthcare Today 2025, **8**: 379 - https://doi.org/10.30953/bhty.v8.379

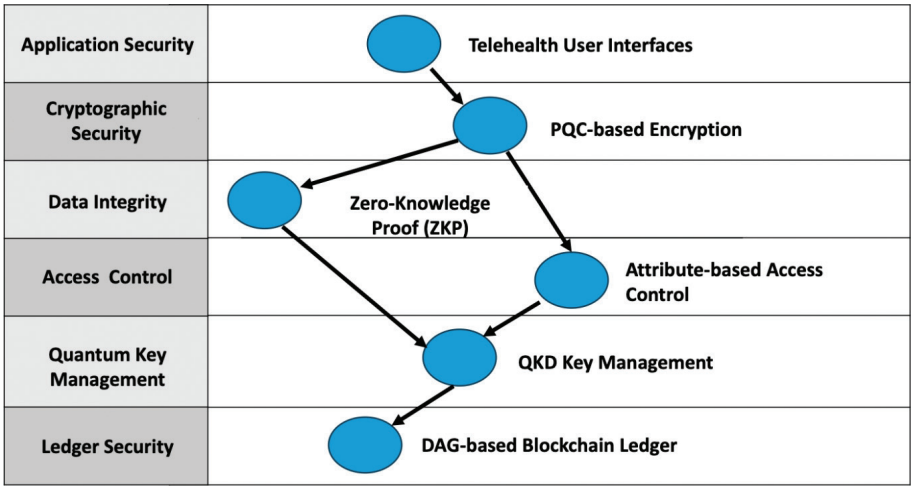

Fig. 1. Overview of the proposed telehealth architecture, showing the directed acyclic graph. DAG: directed acyclic graph-based ledger, PQC: post-quantum cryptography; QKD: quantum key distribution; ZKP: zero-knowledge proof.

Table 1. Security layers in the proposed telehealth architecture

Security Layers and Layer Name (as in Figure 1)	Key Objective	Principal Components	Brief Description
Level 1: Application Security	Ensure secure front-end interactions for telehealth users	• Telehealth user interfaces • Secure session management • User authentication	• Telehealth user interfaces sit at the top of the stack. • They handle all provider/patient interactions. • This layer focuses on protecting user credentials, authenticating sessions, and safeguarding front-end data.
Level 2: Cryptographic Security	Protect data in transit and at rest through quantum-safe cryptography	• PQC-based encryption • CRYSTALS-Dilithium (or other PQC algorithms) • Classical+Quantum hybrid schemes	• PQC-based encryption ensures resilience against both classical and quantum cryptanalysis. • CRYSTALS-Dilithium provides post-quantum signatures for secure, authenticated transactions.
Level 3: (Data Integrity / Access & Control)	Verify integrity of transactions and control who reads/modifies sensitive data	• ZKP • ABE	• ZKPs enable validation of operations (e.g. verifying a provider's authorization) without revealing sensitive details. • ABE ensures only authorized parties can decrypt/modify data based on their attributes.
Level 4: Quantum Key Management	Securely generate and distribute cryptographic keys, mitigating quantum-based eavesdropping	• QKD key management • Photon-based quantum channels • Ephemeral key rotation	• QKD leverages quantum properties to detect key interception in real time. • This layer refreshes keys periodically, ensuring minimal exposure if a key is compromised.
Level 5: Ledger Security	Provide high-throughput, tamper-resistant record-keeping and transaction validation	• DAG-based blockchain ledger • Parallel transaction handling • Consensus mechanism	• A DAG ledger supports parallel validations, improving scalability for telehealth data. Immutable blocks/"vertices" ensure accountability and traceability for patient records and clinical updates.

ABE: Attribute-based Encryption; DAG: directed acyclic graph-based ledger; QC: Quantum Cryptography; QKD: quantum key distribution; ZKP: zero-knowledge proofs.

retrieve off-chain patient information, the system required them to demonstrate relevant attributes such as medical specialty, institutional affiliation, or authorization level that conformed to the encryption policy.[6] If the system confirmed a match, the decryption keys were released, enabling the provider to view or update the records.[7] Simulated scenarios included multiple clinicians collaborating on a patient's care plan, wherein each clinician had partial privileges to different segments of the patient's health data. The granular level of control over record access proved effective in preventing unauthorized disclosures while facilitating seamless coordination among legitimate stakeholders.[1] Figure 2 illustrates the architecture of a telehealth system emphasizing security and privacy through various interconnected layers and components. Each node represents a critical module in the telehealth system, categorized into five primary layers: Application Security, Cryptographic Security, Data Integrity & Access Control, Quantum Key Management, and Ledger Security. The color coding of nodes indicates their respective layer, facilitating quick identification of their roles in the system.

Edges between nodes represent data flows and interactions within the system. These edges are differentiated by line styles and colors to signify different types of data flows, such as user data (red), session data (blue), auth data (green), encrypted data (purple), and others. For example, the interaction between "User Authentication" and "Zero-Knowledge Proof (ZKP)" ensures the validation of authentication processes (lime). Additional interactions, such as the "Feedback Loop" from the Consensus Mechanism back to the Telehealth User Interfaces, highlight the dynamic and iterative nature of telehealth system operations. These interactions aim to provide continuous updates and improvements based on the consensus achieved across the ledger system. The legend located below the graph explains the color coding of layers, while edge labels clarify the nature of data flows between nodes. This comprehensive visualization underscores the complexity and interdependence of telehealth components, which work together to ensure scalability, confidentiality, and post-quantum resilience in a secure and user-centric healthcare environment. By intertwining these components, the architecture ensures that each step in a transaction—from request submission to final ledger recording—remains verifiable, confidential, and resistant to quantum-level attacks.[5]

Preliminary performance metrics, gathered over a simulated 48-h period, reflected stable throughput even during peak loads when multiple nodes accessed and updated records simultaneously.[9] The overheads introduced by CRYSTALS-Dilithium signature verifications, QKD key exchanges, and ZKPs were generally offset by the DAG's parallel transaction handling and the strategic storage of large data sets off-chain.[4] Nodes engaged in frequent key rotations and policy checks without

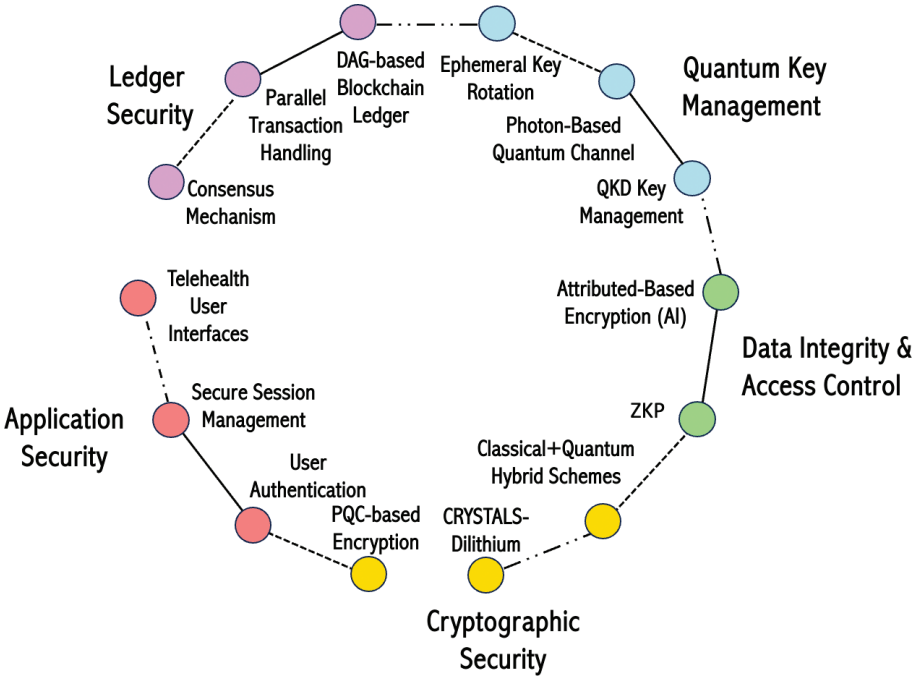

Fig. 2. Telehealth architecture with security and privacy layers, extended interactions, and data flows. AI: artificial intelligence; DAG: directed acyclic graph-based ledger; PQC: post-quantum cryptography; QKD: quantum key distribution; ZKD: zero-knowledge proofs.

Citation: Blockchain in Healthcare Today 2025, **8**: 379 - https://doi.org/10.30953/bhty.v8.379

experiencing unacceptable latency spikes, thus suggesting viability for real-world telehealth environments. Notably, the concurrent confirmation of transactions allowed separate departments—such as radiology and pharmacy—to process updates in real time without queueing delays commonly associated with linear blockchain systems.[13]

These results validate that merging post-quantum cryptographic algorithms, QKD-based key management, and privacy-centric tools into a DAG-based ledger can address telehealth's stringent requirements for data security, scalability, and confidentiality.[7] CRYSTALS-Dilithium signatures secured on-chain transactions, the QKD layer provided quantum-resilient key distribution, and ZKPs maintained the privacy of sensitive medical information.[6] Meanwhile, ABE enhanced access control over large off-chain files. Despite certain trade-offs in computational complexity, the overall architecture demonstrated strong potential for ensuring secure, high-throughput telehealth record management in a post-quantum future.[1,10]

Discussion

The results presented in this study illustrate how PQC with QKD can offer a viable solution to the security and privacy challenges facing telehealth platforms. Although the incorporation of PQC-based algorithms and QKD channels introduces additional computational overhead, the outcomes clearly underscore the efficacy of this design in protecting sensitive healthcare data from unauthorized access or tampering.[7] As shown in Figure 1 and Figure 2 in the preceding Results section, the interdependence of the DAG-based ledger, QKD key management modules, and privacy-preserving cryptographic libraries not only fortifies transaction confidentiality but also ensures that on-chain and off-chain components are harmoniously managed.[13] Given the inherently sensitive nature of telehealth data, which frequently includes diagnostic images, laboratory results, and personal patient identifiers, the heightened security offered by post-quantum techniques is a compelling factor driving the feasibility of this architecture.

One of the key takeaways from the experiments is the significant reduction in risk associated with quantum-based cryptographic attacks. Traditionally, many healthcare systems rely on classical encryption schemes such as RSA or ECC, which are predicted to be vulnerable once quantum computers reach sufficient computational power to run algorithms like Shor's.[14] By integrating PQC schemes, specifically CRYSTALS-Dilithium for digital signatures, the proposed framework addresses these quantum threats proactively.[5] Simultaneously, QKD establishes robust key exchange mechanisms that can alert legitimate network participants to any eavesdropping attempts.[10] Despite the overhead incurred by generating and distributing keys via QKD, the resilience conferred on the system significantly outweighs the added complexity, particularly when the stakes involve life-critical healthcare data.[4]

The overarching advantage of this combined approach—PQC plus QKD—lies in its emphasis on dual security. The PQC secures stored and in-transit data, while QKD ensures that cryptographic keys are not easily intercepted or compromised.[1] The synergy between these elements not only addresses present-day vulnerabilities but also anticipates future adversarial capabilities. Nonetheless, the overheads documented during testing suggest that real-world telehealth networks adopting this system might benefit from additional hardware optimizations or even cloud-based post-quantum accelerators.[9] The concept of offloading particularly heavy cryptographic functions to specialized nodes or services has already been explored in certain blockchain-based solutions, and it may prove crucial in maintaining the speed and efficiency necessary for time-sensitive medical operations.[7]

Another key facet illuminated by this research is the layered approach to privacy. While blockchains inherently provide immutability, there is concern that storing unencrypted data on-chain poses a risk to patient confidentiality.[4] By storing large files or highly sensitive data off-chain and placing only hashes or references on the DAG, the architecture reduces chain data volume and improves privacy.[11] This off-chain model can align with broader digital health equity goals, when combined with augmented reality or mixed reality solutions, which are aimed at underserved communities, ensuring equitable access without compromising security.[15–18] Furthermore, secure MPC extends privacy protections by enabling multiple healthcare entities to collaborate on data analyses—such as comparing anonymized patient outcomes or evaluating treatment efficacy—without ever sharing underlying personal data.[13] Although these protocols come with notable computational costs, they represent a crucial trade-off for compliance with privacy regulations and the ethical handling of patient information.[6]

At the same time, the DAG-based design alleviates transaction bottlenecks by allowing for simultaneous validations.[9] Conventional linear blockchains can struggle under heavy telehealth workloads, especially when many providers concurrently update records. The research demonstrates that enabling parallel confirmations prevents lengthy queues, which could otherwise delay critical information updates in patient management. In large-scale deployments, however, more sophisticated node synchronization protocols might be required to handle conflicting transactions.[7] For instance, two hospitals might accidentally submit differing updates to the same patient record around the same time, necessitating a robust conflict resolution mechanism that does not compromise the immutability or integrity of the ledger.[13]

It is important to acknowledge that DAG-based ledgers, while providing distinct advantages in terms of parallel transaction processing, are not the only means of achieving high throughput for updating patient records. Traditional linear blockchains can incorporate advanced smart contract designs or parallel execution frameworks to process multiple attributes of a single patient record, concurrently.[19] Techniques such as block partitioning, where a single block is logically divided into sub-blocks, allow different sets of transactions to be verified in parallel, thereby mitigating bottlenecks that arise from sequential consensus mechanisms.[20] Despite these possibilities, a DAG-based approach naturally facilitates concurrency and minimizes transaction contention. However, it can introduce complexities in transaction ordering and finality, leading to potential security concerns if not carefully managed. For instance, reconciling conflicting transactions in DAG architectures might require specialized conflict resolution protocols, and ensuring coherence of clinical data across multiple sites may necessitate elaborate synchronization strategies. A balanced assessment would thus compare the overhead of handling intricate DAG consensus rules to the optimizations available in a traditional linear blockchain.

By weighing throughput advantages against potential security or ordering complexities, telehealth system designers can tailor their choice of ledger architecture to the specific scalability demands and regulatory constraints of healthcare environments. Beyond technical intricacies, there is also a substantial social and ethical dimension to adopting blockchain-based solutions in healthcare. The immutability of blockchain ledgers reassures stakeholders that patient data and clinical records have not been surreptitiously altered.[13] This immutability fosters greater trust among clinicians, patients, insurers, and regulatory bodies. Conversely, it also raises concerns about data permanence. Even if sensitive content is encrypted, the mere existence of certain metadata on the chain might be deemed problematic under stricter interpretations of privacy laws, such as Health Insurance Portability and Accountability Act in the United States or the GDPR in the European Union.[4] The proposed solution attempts to strike a balance by combining encryption, off-chain storage, and advanced cryptographic proofs like ZKPs and MPC, thereby ensuring that immutability does not equate to unwarranted transparency.[6]

One potential hurdle is the physical and infrastructural demand of setting up QKD channels, particularly for hospital networks that span disparate regions. Although significant investments from governmental and industry partners have begun to reduce these barriers, establishing the fiber optic lines or satellite-based QKD solutions at scale is still costly.[10] Furthermore, key management protocols become more complex with frequent rotations and distribution to potentially thousands of clinical endpoints.[1] Nonetheless, the value offered by quantum-safe communications may justify these expenses over the long term, especially as the overall threat landscape expands and regulatory demands for data protection intensify.[7]

While this study demonstrates a promising quantum-safe approach for telehealth, several limitations must be acknowledged. The reliance on specialized hardware, such as QKD devices, can significantly increase infrastructural costs, especially for geographically dispersed healthcare facilities. Additionally, the DAG-based ledger introduces potential complexities in ensuring transaction ordering and finality, necessitating robust conflict resolution mechanisms. The simulation environment might not capture all real-world variables, including inconsistent network conditions, human factors, and regulatory constraints. Off-chain data storage still raises trust issues regarding external data repositories, which may be vulnerable to physical attacks or insider threats. Implementing privacy-preserving methods like ZKPs and MPC requires substantial computational overhead, potentially affecting response times in critical clinical scenarios. Finally, ensuring system interoperability with existing telehealth platforms and electronic health record systems remains challenging.

Looking ahead, there are numerous avenues for enhancement. Fully homomorphic encryption (FHE) may be integrated to allow computations on encrypted data without ever decrypting it, taking privacy-preserving analytics a step further.[11] Simultaneously, artificial intelligence–enhanced dashboards and caregiver support applications could streamline communication between providers and families, particularly in dementia care or bolster decision-making through data visualization.[21–24] Coupled with advanced PQC algorithms, FHE would enable more sophisticated machine learning or data mining processes without exposing any raw records, which is crucial in telehealth studies involving genomic data or predictive analytics. Additionally, the inclusion of secure enclaves or trusted execution environments could isolate sensitive computations from untrusted parts of the network.[6] These enclaves could serve as a middle layer between the blockchain ledger and off-chain data repositories, offering another protective barrier against potential breaches.

In terms of validating this architecture in real-world scenarios, the next logical step is to conduct a fully operational proof-of-concept that aligns with healthcare regulations.[13] This could involve partnering with actual hospitals or healthcare systems willing to pilot the architecture, implementing partial data sets and controlled QKD channels to measure performance, compliance, and scalability in situ.[9] Such a pilot could also uncover potential user-interface issues that might not surface in a controlled laboratory simulation, allowing for iterative refinements. Ultimately, regulatory oversight would be pivotal to

Citation: Blockchain in Healthcare Today 2025, 8: 379 - https://doi.org/10.30953/bhty.v8.379

ensure that patient rights and ethical considerations are respected throughout the data lifecycle, including collection, storage, analytics, and eventual archival or deletion.[4]

Overall, the proposed architecture paves the way for a new era of telehealth data security, one that anticipates the impending reality of quantum computing while adhering to stringent privacy demands. The synergy of PQC, QKD, ZKPs, MPC, and a DAG-based design offers a comprehensive response to quantum threats, cryptographic vulnerabilities, and privacy concerns.[7] By adopting off-chain storage strategies, ABE, and parallel transaction processing, the system supports high-throughput telehealth operations without sacrificing confidentiality.[6] As quantum computing evolves, maintaining proactive strategies that integrate advanced cryptographic methods will become vital. Therefore, this research not only demonstrates the feasibility of a PQC- and QKD-enhanced blockchain architecture but also proposes a framework adaptable to upcoming technological and regulatory landscapes. In doing so, it addresses immediate challenges and lays a foundation for continued innovation aimed at safeguarding patient records and sensitive clinical interactions in the post-quantum era.[1,10]

Conclusion

In an era where AI and quantum computing poses imminent risks to traditional cryptographic protocols, the need for robust, future-proof security in telehealth systems has become paramount.[5,7] The architecture presented in this study addresses these concerns by integrating PQC at the consensus layer, harnessing QKD for secure key exchanges, and employing privacy-preserving techniques such as ZKPs and secure MPC. As illustrated in Figure 1 and Figure 2, the synergy of these components yields a system that maintains immutability and confidentiality, thereby ensuring that patient records are kept private while updates to the ledger remain verifiable.[6,13] Although performance assessments indicate an increase in computational overhead, particularly in the generation and validation of post-quantum signatures as well as the deployment of QKD channels, the ability to withstand potential quantum attacks ultimately justifies these resource investments.[10]

The DAG-based approach described here further enhances scalability by enabling parallel transaction validation, which is essential in large telehealth networks where timely patient data access can be a matter of critical clinical importance.[9] In tandem, a granular smart contract–based access control model ensures that only authorized entities can view or modify sensitive medical information, thereby embedding compliance with privacy regulations.[4]

Future applications might integrate AI-driven medication management or therapy adherence tools, bridging security innovations with patient-centric outcomes.[25–27] Taken as a whole, this post-quantum blockchain architecture demonstrates strong potential for deployment in real-world telehealth settings. While additional optimizations and real-life pilot studies remain necessary, the research underscores that achieving quantum resistance, privacy preservation, and operational scalability within a single platform is not only feasible but also timely. This integrated approach thus offers a forward-looking blueprint for safeguarding patient care in the face of rapid technological change.[1]

Funding

None.

Conflicts of Interest

No relevant disclosures.

Contributors

Fahmida Hai and Don Roosan contributed to conceptualization, methodology, software, data analysis, and writing the original draft. Fahmida Hai, Rubayat Khan, Saif Nirzhor, and Don Roosan contributed to investigation, review and editing, supervision, and project administration. All authors read and agreed to the published version of the manuscript.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

Data are not available on request due to [privacy/ethical] restrictions.

Acknowledgments

We are grateful to Merrimack College for support.

Application of AI-Generated Text or Related Technology

None reported by the authors.

References

1. Jeyaraman N, Jeyaraman M, Yadav S, Ramasubramanian S, Balaji S. Revolutionizing healthcare: the emerging role of quantum computing in enhancing medical technology and treatment. Cureus. 16(8):e67486. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11416048/
2. Zastrozhin MS, Sorokin AS, Agibalova TV, Grishina EA, Antonenko AP, Rozochkin IN, et al. Using a personalized clinical decision support system for bromdihydrochlorphenylbenzodiazepine dosing in patients with anxiety disorders based on the pharmacogenomic markers. Hum Psychopharmacol Clin Exp. 2018;33(6):e2677. https://doi.org/10.1002/hup.2677
3. Roosan D, Chok J, Baskys A, Roosan MR. PGxKnow: a pharmacogenomics educational Hololens application of augmented reality and artificial intelligence. Pharmacogenomics. 2022 Mar 1;23(4):235–45. https://doi.org/10.2217/pgs-2021-0120

4. Odeh A, Abdelfattah E, Salameh W. Privacy-preserving data sharing in telehealth services. Appl Sci. 2024 Jan;14(23):10808. https://doi.org/10.3390/app142310808
5. Opiłka F, Niemiec M, Gagliardi M, Kourtis MA. Performance analysis of post-quantum cryptography algorithms for digital signature. Appl Sci. 2024 Jan;14(12):4994. https://doi.org/10.3390/app14124994
6. Rao YS, Srivastava V, Mohanty T, Debnath SK. Designing quantum-secure attribute-based encryption. Clust Comput. 2024 Dec 1;27(9):13075–91. https://doi.org/10.1007/s10586-024-04546-9
7. Pandey S, Bhushan B, Hameed AA. Securing Healthcare 5.0: Zero-Knowledge Proof (ZKP) and Post Quantum Cryptography (PQC) solutions for medical data security. In: CKK Reddy, T Sithole, M Ouaissa, Ö Özer, MM Hanafiah, editors. Soft computing in industry 50 for sustainability. Cham: Springer Nature, 2024; p. 339–55.
8. Roosan D, Clutter J, Kendall B, Weir C. Power of heuristics to improve health information technology system design. ACI Open. 2022 Dec 9;06:e114–22. https://doi.org/10.1055/s-0042-1758462
9. Kumar N, Reiffers-Masson A, Amigo I, Rincón SR. The effect of network delays on distributed ledgers based on directed acyclic graphs: a mathematical model. Perform Eval. 2024 Jan 1;163:102392. https://doi.org/10.1016/j.peva.2023.102392
10. Yang J, Jiang Z, Benthin F, Hanel J, Fandrich T, Joos R, et al. High-rate intercity quantum key distribution with a semiconductor single-photon source. Light Sci Appl. 2024 Jul 2;13(1):150. https://doi.org/10.1038/s41377-024-01488-0
11. Dhokrat JG, Pulgam N, Maktum T, Mane V. A framework for privacy-preserving multiparty computation with homomorphic encryption and zero-knowledge proofs. Informatica. 2024;48(21):1–14. https://doi.org/10.31449/inf.v48i21.6562
12. Roosan D, Law AV, Roosan MR, Li Y. Artificial intelligent context-aware machine-learning tool to detect adverse drug events from social media platforms. J Med Toxicol. 2022 Oct 1;18(4):311–20. https://doi.org/10.1007/s13181-022-00906-2
13. Roosan D, Roosan MR, Kim S, Law AV, Sanine C. Applying Artificial Intelligence to create risk stratification visualization for underserved patients to improve population health in a community health setting [Internet]. Research Square; 2022 [cited 2025 Jan 6]. Available from: https://www.researchsquare.com/article/rs-1650806/v1
14. Roosan D, Chok J, Li Y, Khou T. Utilizing quantum computing-based large language transformer models to identify social determinants of health from electronic health records. In: 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET) [Internet].* 2024 [cited 2025 Jan 6]; p. 1–6. Available from: https://ieeexplore.ieee.org/document/10698600
15. Roosan D. Integrating artificial intelligence with mixed reality to optimize health care in the metaverse. In: V Geroimenko, editor. Augmented and virtual reality in the metaverse. Cham: Springer Nature Switzerland, 2024; p. 247–64.
16. Roosan D. The promise of digital health in healthcare equity and medication adherence in the disadvantaged dementia population. Pharmacogenomics. 2022 Jun;23(9):505–8. https://doi.org/10.2217/pgs-2022-0062
17. Wu Y, Li Y, Baskys A, Chok J, Hoffman J, Roosan D. Health disparity in digital health technology design. Health Technol. 2024 [cited 2025 Jan 5];1–11. Available from: https://rdcu.be/dvAWv
18. Roosan D, Wu Y, Chok J, Sanine C, Khou T, Li Y, et al. Artificial intelligence-powered large language transformer models for opioid abuse and social determinants of health detection for the underserved population. In: Proceedings of the 13th international conference on data science, technology and applications—DATA. SciTePress, 2024; p. 15–26. (ISBN 978-989-758-707-8; ISSN 2184-285X).
19. U.S. Patent No. 11829494B2. 2023 [cited 2025 Jan 5]. Available from: https://patents.google.com/patent/US11829494B2
20. U.S. Patent No. 11556658B2. 2023 [cited 2025 Jan 5]. Available from: https://patents.google.com/patent/US11556658B2
21. Li Y, Phan H, Law AV, Baskys A, Roosan D. Gamification to improve medication adherence: a mixed-method usability study for MedScrab. J Med Syst. 2023 Oct 20;47(1):108. https://doi.org/10.1007/s10916-023-02006-2
22. Roosan D, Kim E, Chok J, Nersesian T, Li Y, Law AV, et al. Development of a dashboard analytics platform for dementia caregivers to understand diagnostic test results. In: E Pino, R Magjarevi, P de Carvalho, editors. International conference on biomedical and health informatics 2022. Cham: Springer Nature Switzerland, 2022; p. 143–53.
23. Roosan D, Law AV, Karim M, Roosan M. Improving team-based decision-making using data analytics and informatics: Protocol for a collaborative decision support design. JMIR Res Protoc. 2019;8(11):e16047. https://doi.org/10.2196/16047 (PMID: 31774412)
24. Islam R, Weir CR, Jones M, Del Fiol G, Samore MH. Understanding complex clinical reasoning in infectious diseases for improving clinical decision support design. BMC Med Inform Decis Mak. 2015;15:1–12. https://doi.org/10.1186/s12911-015-0221-z
25. Islam R, Weir C, Del Fiol G. Clinical complexity in medicine: a measurement model of task and patient complexity. Methods Inf Med. 2016;55(1):14–22. https://doi.org/10.3414/ME15-01-0031
26. Islam R, Weir CR, Del Fiol G. Heuristics in managing complex clinical decision tasks in experts' decision making. In: 2014 IEEE international conference on healthcare informatics. Verona: IEEE, 2014; p. 186–93.
27. Roosan D, Padua P, Khan R, Khan H, Verzosa C, Wu Y. Effectiveness of ChatGPT in clinical pharmacy and the role of artificial intelligence in medication therapy management. J Am Pharm Assoc (2003). 2024;64(2):422–8.e8. https://doi.org/10.1016/j.japh.2023.11.023

Addendum

Acronyms defined in the article
ABE: attribute-based encryption
DAG: directed acyclic graph-based ledger
ECC: elliptic curve cryptography
FHE: fully homomorphic encryption
MPC: multiparty computation
PQC: post-quantum cryptography
QKD: quantum key distribution
RSA: Rivest-Shamir-Adleman
ZKPs: Zero-knowledge proofs