Blockchain, AI and Quantum Networks: A Tri-Layer Model for Secure Transactions in Finance and Healthcare

Author: Sarah Williams, **Affiliation:** Assistant Professor, Department of Robotics Engineering, Carnegie Mellon University, United States

Email: sarah.williams@cmu.edu

Abstract

Rapid digitization of financial and healthcare services has produced immense value while also increasing systemic vulnerability: sensitive transactions and records must be exchanged across complex, heterogeneous ecosystems subject to cyber-attacks, fraud, and regulatory scrutiny. In parallel, three technological trends distributed ledger technologies (blockchain), artificial intelligence (AI), and quantum communications/networks are each maturing and offer complementary capabilities: blockchain affords decentralized integrity and transparent audit trails; AI provides adaptive threat detection and automated decisioning; and quantum networks (including quantum key distribution, QKD) promise information-theoretic or quantum-resilient security primitives. In this paper we introduce a **Tri-Layer Model** that integrates these three technologies into a coherent architecture for secure, privacy-preserving transactions in finance and healthcare. We (1) synthesize the theoretical foundations and practical properties of each layer; (2) propose concrete hybrid architectures that place blockchain as the transaction ledge, AI as the adaptive analytics and policy engine, and quantum networks as the secure transport and post-quantum key infrastructure; (3) provide threat-centric security analyses and formalize trust and threat models; (4) outline deployment patterns, interoperability and regulatory considerations; and (5) present benchmarking and evaluation protocols for assessing security, performance, and privacy tradeoffs. We ground the discussion with recent literature and industry developments that show how post-quantum cryptography, QKD pilots, federated learning, and blockchain pilots are being used in finance and healthcare contexts. While practical constraints remain (cost, latency, hardware maturity), the tri-layer model offers a roadmap to progressively harden critical systems today while enabling a migration path toward quantum-resilient infrastructures.

Keywords: blockchain, quantum networks, quantum key distribution, AI, federated learning, post-quantum cryptography, secure transactions, healthcare, finance, tri-layer architecture

1. Introduction

Modern finance and healthcare rely on complex digital ecosystems that interconnect institutions, cloud providers, device vendors, patients, customers, and regulators. These ecosystems face two simultaneous pressures: (i) the need for stronger security and privacy guarantees to protect sensitive transaction data and personally identifiable health information, and (ii) the demand for efficient, auditable, and automated services (e.g., real-time payments, claims adjudication, remote care triage). Emerging technologies   blockchain, AI, and quantum communications   each offer partial solutions, but only by integrating them coherently can designers obtain complementary strengths: immutability and distributed consent from blockchains; intelligent, adaptive monitoring and decisioning from AI; and cryptographic freshness and quantum-resilience from quantum networks and post-quantum cryptography (PQC). This paper proposes a **Tri-Layer Model** that places these technologies into an architected stack optimized for secure transactions in sensitive domains (Fatunmbi, 2021).

We motivate the need for such integration by observing the evolving threat landscape: adversaries use increasingly sophisticated AI techniques for fraud and social engineering, and the prospective development of large-scale quantum computers threatens existing public-key cryptography used by blockchains and internet transport. At the same time, experiments and pilots demonstrate that quantum-safe tools (QKD, PQC) and AI-enabled detection systems can materially improve resilience when placed into enterprise architectures (ID Quantique, 2024; Fernandez-Carames et al., 2024).

The rest of the article is organized as follows. Section 2 reviews background and related work in blockchain, AI, and quantum networking relevant to security and transactions. Section 3 introduces the Tri-Layer Model and describes the function of each layer, their interfaces, and design principles. Section 4 develops threat models and formal security analyses for the architecture, including quantum-era considerations. Section 5 sketches concrete system architectures and integration patterns for finance and healthcare use cases. Section 6 specifies evaluation methodologies, metrics, and benchmark scenarios. Section 7 surveys governance, regulatory, and ethical considerations. Section 8 discusses limitations, open research problems, and a pragmatic roadmap for progressive adoption. Section 9 concludes.

2. Background and Related Work

2.1 Blockchain and Distributed Ledger Technologies (DLT)

Blockchain and DLT provide append-only, tamper-evident ledgers maintained by distributed participants through consensus protocols, smart contracts, and cryptographic primitives. In finance, DLTs enable cross-border payments, trade finance, and tokenization; in healthcare, blockchains have been explored for secure data sharing, consent management, supply-chain provenance, and audit trails for clinical trials and drug distribution. Reviews emphasize benefits (interoperability, provenance, patient control), but also note limitations: throughput, privacy, governance complexity, and energy consumption in some consensus designs.

Two technical trends relevant here are (a) **permissioned (private) ledgers** that trade decentralization for higher throughput and governance control common in enterprise finance and health pilots and (b) **privacy-enhancing ledger techniques** (zero-knowledge proofs, off-chain channels, secure enclaves) that aim to preserve confidentiality while retaining verifiability. Review literature stresses that blockchain is best used to coordinate trust and enforce protocol logic rather than to store large volumes of sensitive raw data on-chain.

2.2 Artificial Intelligence for Transaction Security

AI provides capabilities for anomaly detection (fraud), identity verification (biometrics, liveness detection), adaptive policy enforcement, and automated orchestration (smart contract synthesis and verification). Advances in graph neural networks (GNNs), sequence models, and anomaly detection have improved detection rates for payment fraud, insider risk, and money-laundering tasks. AI systems also enable privacy-preserving analytics via federated learning and differential privacy, which align well with distributed ledger topologies where raw data cannot be centralized. However, AI introduces its own risks (adversarial attacks, model bias, explainability challenges). Recent surveys show AI reduces fraud incidence but also introduces systemic concentration risks unless diversity and auditability are maintained (Fatunmbi, 2021).

2.3 Quantum Networks and Quantum-Resilient Cryptography

Quantum networks beyond quantum computers include quantum key distribution (QKD) links, quantum repeaters (future), and protocols for entanglement distribution. QKD offers information-theoretic secure key exchange under physical model assumptions and is being piloted for critical infrastructure and healthcare communications. At the same time, the cryptographic community is transitioning to PQC primitives standardized by NIST to mitigate the eventual threat of cryptanalysis by fault-tolerant quantum computers (Fatunmbi, 2023). The hybrid approach deploying QKD for link-level secrets and PQC for algorithmic assurances is a practical near-term strategy. Governments and industry agencies are issuing roadmaps for post-quantum migration and encouraging PQC adoption in critical sectors.

2.4 Prior Work on Integration

There is growing literature and experimental work on combining these technologies: blockchain projects exploring post-quantum signatures, quantum-assisted proof systems, and initial hybrid frameworks where quantum modules assist classical cryptography or machine learning tasks. Industry pilots demonstrate QKD for sensitive healthcare links and PQC upgrades for cloud services; early research introduces quantum-secure blockchain proposals and hybrid quantum-classical fraud detection systems for finance. However, a systematic architectural model that places blockchain, AI, and quantum networks together with engineering practices, threat models, and evaluation protocols tailored to finance and healthcare remains underdeveloped. This paper addresses that gap.

3. The Tri-Layer Model: Design Principles and Components

We propose a layered architecture with **three primary strata**: (1) the **Ledger Layer** (Blockchain/DLT), (2) the **Analytics/Policy Layer** (AI and smart orchestration), and (3) the

Quantum Transport Layer (quantum networks, QKD, PQC support). Each layer has distinct responsibilities but must interoperate through well-specified interfaces.

3.1 Design Principles

The tri-layer model is built on these core principles:

- **Least Privilege and Data Minimization:** Store minimal sensitive data on-chain; use off-chain storage with verifiable commitments and privacy proofs.
- **Layered Defense-in-Depth:** Combine cryptographic, AI-based detection, and quantum-safe keying to mitigate diverse threat classes.
- **Progressive Upgradeability:** Allow incremental deployment start with AI and blockchain pilots, add PQC and selective QKD links, and evolve toward broader quantum networking.
- **Interoperability and Governance:** Standardized APIs, auditable policy contracts, role-based consensus rules, and regulatory compliance baked into workflow logic.
- **Privacy-First Analytics:** Use federated learning, secure enclaves, and privacy proofs to enable analytics without centralizing raw sensitive records.

3.2 Ledger Layer (Blockchain / DLT)

Function. Immutable transaction and consent records, policy enforcement via smart contracts, and decentralized consensus among trusted entities (banks, hospitals, insurers, regulators). Use permissioned DLTs for enterprise scenarios to ensure throughput and governance control.

Design choices. For finance: regulated consortium blockchains (e.g., permissioned Fabric-style networks) that integrate with existing clearing rails. For healthcare: consent registries, provenance chains for supply chain (pharma), and audit logs for clinical trials. Privacy is enforced through selective disclosure mechanisms: off-chain storage for patient records with a hash/pointer on-chain and access controlled by smart contracts and attestation tokens. Post-quantum signature schemes (e.g., NIST-standard PQC) or hybrid signature schemes should be used to sign blocks/transactions to future-proof ledgers.

Data model. Transactions contain metadata, pointers to off-chain encrypted payloads, policy identifiers, and audit receipts. Smart contracts codify access control policies, regulatory reporting logic, and contingency workflows (e.g., emergency disclosure under court order).

3.3 Analytics/Policy Layer (AI)

Function. Adaptive risk scoring, fraud detection, privacy-preserving analytics, policy orchestration (which transactions to commit), and real-time alerts. AI models operate on aggregated or preprocessed features derived from off-chain datasets; model provenance and governance metadata are anchored on-chain (model signatures, training lineage).

Architectural patterns.

- **Federated Learning (FL)** for cross-institutional model training without centralizing raw data; model updates can be anchored on the ledger for auditability and update sequencing. Use secure aggregation and differential privacy to limit leakage (Fatunmbi, 2021).
- **Graph Analytics and GNNs** for transaction networks: identify money-laundering rings or anomalous claim networks in healthcare. GNN outputs are used to trigger on-chain policy automations (e.g., hold a transaction for manual review).
- **Explainable AI (XAI):** capture explanations with each model decision (SHAP values, counterfactual explanations) and record summary proof artifacts on-chain to enable regulatory auditing and dispute resolution (Ozdemir & Fatunmbi, 2024).

Model governance. Versioned models, training datasets metadata, fairness audits, and performance metrics are recorded on the ledger to allow tamper-evident accountability.

3.4 Quantum Transport Layer

Function. Secure key material distribution (QKD), link-level quantum encryption support, and provision of quantum-resilient randomness for secure protocols. Also interfaces to PQC services and future quantum middleware.

Practical components.

- **QKD Links:** where feasible, establish QKD for point-to-point links between critical nodes (central bank, core hospital data center). Use QKD keys to bootstrap symmetric encryption for high-sensitivity channels; rotate keys frequently to maintain forward secrecy. Industry pilots have shown QKD deployments for healthcare and critical infrastructure.
- **Post-Quantum Cryptography (PQC):** deploy NIST-recommended PQC algorithms for signatures and key encapsulation across the ledger and client SDKs to mitigate future quantum attacks on public-key schemes. PQC must be integrated into transaction signing and consensus verification processes. arXiv
- **Hybrid Key Management:** combine PQC, QKD, and classical symmetric schemes in layered KMS (key management system) that chooses appropriate keys by sensitivity level and link capability.
- **Quantum Randomness and Entropy Services:** use quantum random number generators (QRNGs) to enhance cryptographic entropy and support secure attestation.

Deployment guidance. QKD is currently most practical for high-value, latency-tolerant links due to cost and physical constraints; PQC provides broader, software-level protection that can be rolled out widely via SDKs and firmware updates. A hybrid mix provides the best near-term posture.

3.5 Cross-Layer Interfaces

- **Ledger ⇄ AI:** AI outputs (risk flags, policy decisions) are represented as signed policy tokens that smart contracts consume. Conversely, smart contracts can emit data (e.g., anonymized audit events) for AI pipelines.
- **AI ⇄ Quantum:** AI orchestration components request cryptographic material (post-quantum keys, QKD session keys) from the KMS. AI may also use QRNG entropy for model seeding to improve unpredictability in federated updates.
- **Ledger ⇄ Quantum:** Transaction signatures and block validation use PQC primitives; high-sensitivity rollups (e.g., settlement batches) can be transmitted over QKD-secured tunnels.

4. Threat Models and Security Analysis

A robust architecture must be validated against explicit threat models. We specify adversary classes and analyze tri-layer defenses.

4.1 Adversary Classes

1. **External network adversary (E):** eavesdrops, injects or modifies network traffic; aims to exfiltrate data or perform MITM attacks.
2. **Insider/malicious node (I):** compromised ledger node or cloud operator who can attempt to manipulate transactions or access off-chain data.
3. **Advanced persistent threat (APT) with quantum capability (Q):** nation-state actor that may obtain quantum computational resources in the future and attempt cryptanalysis of intercepted traffic.
4. **AI-enabled adversary (A):** uses ML to evade detection, generate synthetic identities, or craft high-fidelity social-engineering attacks.

4.2 Defensive Posture per Layer

Quantum Transport Layer defenses:

- **Against E:** QKD provides information-theoretic confidentiality for key exchange (under physical model assumptions) and detects interception due to channel disturbances. PQC secures public-key primitives against quantum cryptanalysis. Together they protect link confidentiality and future resiliency.
- **Against Q:** PQC reduces long-term vulnerability; QKD prevents retrospective decryption of stored ciphertexts when keys were established via QKD (if keys are used for symmetric encryption and ephemeral). However, QKD requires physical trust in endpoints and is limited by link reach and cost.

Ledger Layer defenses:

- **Against I:** Permissioned consensus ensures only vetted nodes participate; smart contract formal verification and on-chain attestations make unauthorized changes detectable. Post-quantum signatures guard against private-key compromise due to future quantum attacks. Off-chain data remains encrypted and accessible only under smart contract conditions.
- **Against A:** Time-series detection of abnormal transaction patterns (via AI) can flag collusion, but also requires adaptive thresholds to avoid adversarial model inversion.

AI/Policy Layer defenses:

- **Against A:** Robust model training (adversarial training, ensemble diversity, continual retraining) and explainable outputs limit blind spots. Federated learning with secure aggregation reduces central data exposure. Model behavior logs anchored on-chain enable audits when model decisions are contested.

4.3 Attack Scenarios and Mitigation Examples

Scenario 1: Quantum-enabled archival attack. An adversary (Q) captures encrypted transaction traffic today, hoping to decrypt later with a quantum computer. **Mitigation:** use PQC to sign and establish keys for transactions and apply QKD-backed symmetric encryption for the most sensitive channels. Store only non-sensitive hashes on chain to limit archival value.

Scenario 2: AI-assisted fraud ring. An adversary (A) uses generative models to craft synthetic identities and small fraudulent payments that evade thresholds. **Mitigation:** the AI layer applies GNN anomaly detection trained across institutions via federated learning; suspicious pattern tokens are placed on-chain to block automated clearing until human review.

Scenario 3: Insider ledger node collusion. Compromised node (I) attempts to manipulate smart contract logic. **Mitigation:** multi-party attestation, threshold signatures (using PQC where applicable), and independent verification via redundant nodes; contentious updates require multi-stakeholder voting enshrined in smart contract governance code.

4.4 Formal Security Properties

The tri-layer model aims to satisfy these security properties:

- **Confidentiality (short-term):** Achieved using symmetric encryption over QKD-backed channels or strong post-quantum KEMs.
- **Confidentiality (long-term):** PQC resists future quantum decryption; QKD prevents retrospective decryption for QKD-protected flows.
- **Integrity:** Ledger immutability, cryptographic signatures (PQC), and attestable model artifacts ensure tamper detection.

- **Availability:** Permissioned consensus and redundancy protect against denial-of-service; AI prediction layers can manage load and detect availability attacks.
- **Auditability and Non-repudiation:** On-chain logs and verifiable model provenance provide forensic trails for regulatory inspections.

Formal verification of combined properties is complex due to cross-layer interactions; security proofs should be modular (prove layer properties and composition theorems about their integration). This is an open research area: formal composition between QKD assurances and ledger integrity under real-world adversary models requires careful modeling of physical channel assumptions and human trust boundaries.

5. Use Cases and System Architectures

We now illustrate concrete architectures and workflows for priority use cases in finance and healthcare.

5.1 Use Case A   Interbank Settlement with Quantum-Hardened Ledger

Scenario. Cross-border settlement among consortium banks requires high confidentiality and auditability.

Architecture. A permissioned consortium ledger (Fabric/Quorum style) implements settlement smart contracts. PQC signatures are used for transaction signing; settlement batches containing confidential details are encrypted and transmitted over QKD-secured channels between central clearing nodes. The AI layer monitors settlement patterns for anomalies (e.g., wash trades) using federated GNNs trained across banks; when suspicious activity is detected, the smart contract pauses settlement of implicated batches and triggers escrow workflows.

Benefits. Improved resistance to future quantum attacks, tamper-evident audit trails, and enhanced fraud detection without sharing raw transaction details among banks. QKD links are used only between critical clearing centers to balance cost and benefit (deployed selectively).

5.2 Use Case B   Federated Clinical Data Exchange and Consent Management

Scenario. Multiple hospitals share de-identified patient features for a machine learning study on treatment outcomes while preserving patient consent and regulatory compliance.

Architecture. Patients' consent is recorded on a permissioned ledger; off-chain encrypted clinical records remain at hospitals. Federated learning trains models across hospitals model updates are aggregated securely and a signed model hash is anchored on the ledger for provenance. For high-privacy experiments, QRNGs seed differential privacy noise, and QKD protects aggregator channels between regional provers. XAI artifacts accompany model outputs and are recorded as attestations on the ledger to aid IRB review.

Benefits. Enables collaborative research with auditable consent flows, model provenance, and private training without raw data transfer; selective QKD adoption strengthens particularly sensitive research links.

5.3 Use Case C Secure Telehealth and Remote Prescriptions

Scenario. Telehealth consultations require secure exchange of medical records, e-prescriptions, and real-time monitoring.

Architecture. Patient devices (wearables) store data locally and synchronize with a personal health vault; hashes and consent tokens are anchored on a blockchain. Prescriptions are smart-contracted with anti-fraud checks using AI risk scores; critical prescription verification steps use PQC-verified signatures and ephemeral QKD sessions for pharmacy-prescriber channels where available.

Benefits. Reduces prescription fraud, preserves patient control, and ensures secure delivery of sensitive orders. AI flags prescription anomalies (multiple prescribers, suspicious dosage patterns) and triggers manual review.

6. Evaluation and Benchmarking Framework

To validate tri-layer systems, we propose evaluation protocols that measure security, performance, privacy, and operational cost.

6.1 Security Benchmarks

- **Cryptographic robustness:** validate PQC implementations against known attacks; measure post-quantum signature size, verification cost, and integration performance.
- **QKD integrity:** measure key generation rates, error rates, and link stability under varying conditions.
- **Attack simulations:** red-team simulations for APTs, insider collusion, and AI-driven fraud. Record detection latency, false positives, and false negatives.

6.2 Performance and Scalability Benchmarks

- **Transaction throughput/latency:** measure end-to-end time from transaction submission to ledger finality under various consensus and PQC signature schemes.
- **AI inference latency:** time to detect anomalous patterns for real-time blocking.
- **QKD overhead:** additional latency and resource consumption between secure links.

6.3 Privacy and Utility Tradeoff

- **Federated learning utility:** compare model accuracy under different privacy budgets (epsilon) for differential privacy and secure aggregation.

- **Information leakage:** use membership inference and model inversion attackers to quantify leakage risk.

6.4 Economic and Energy Costs

- **TCO analysis:** quantify costs for QKD hardware, PQC migration, block storage, and AI compute.
- **Environmental impacts:** energy per transaction and overall carbon impact, comparing consensus alternatives and QKD infrastructure.

6.5 Regulatory and Compliance Testing

- **Auditability checks:** ability to produce tamper-evident logs for regulatory audits.
- **Data residency tests:** ensure cross-border data flows comply with jurisdictional constraints.

A multi-stakeholder evaluation testbed (banks, hospitals, vendors, regulators) is recommended for real-world pilots with documented datasets and reproducible metrics.

7. Governance, Ethics, and Regulatory Considerations

The tri-layer architecture intersects legal and ethical domains.

7.1 Data Governance and Consent

Implement consent registries anchored on the ledger with revocation semantics; use smart contracts to enforce consent-based data access and logging for downstream auditing.

7.2 Algorithmic Accountability

AI models used to make or block transactions must be explainable and subject to independent audits. On-chain capture of model lineage, training datasets, and fairness metrics supports compliance and contestability. (Ozdemir & Fatunmbi, 2024).

7.3 Regulatory Compliance

Finance and healthcare have distinct regulatory regimes. Architecture must support reporting and selective disclosure under lawful requests. The use of PQC and QKD should be transparent to regulators; pilot engagements with supervisory bodies are essential to align technical implementations with compliance expectations.

7.4 Ethical Issues

- **Surveillance risk:** continuous monitoring and immutable logs raise privacy concerns; data minimization and strong governance are required.

- **Equity:** ensure access to secure infrastructure does not create disparities (e.g., only large hospitals can deploy QKD).
- **Liability:** define legal responsibility for model decisions, contract enforcement, and cryptographic failures.

8. Limitations, Open Research Questions, and Roadmap

8.1 Limitations

- **QKD deployment constraints:** cost, physical fiber availability, and limited reach restrict QKD applicability to selected high-value links.
- **PQC maturity and performance tradeoffs:** PQC increases signature sizes and computational cost; performance engineering is necessary for high-throughput ledgers.
- **AI risks:** adversarial attacks and model drift require ongoing operations.

8.2 Open Research Directions

1. **Formal composition proofs** that combine QKD physical security models with ledger integrity and AI decisioning   mathematical frameworks for cross-layer security.
2. **Efficient PQC integration** into constrained devices (IoT wearables) and ledger clients to support mass deployments.
3. **Quantum-aware consensus algorithms** that can leverage quantum randomness or other primitives to improve fairness and unpredictability.
4. **Economic models** assessing when QKD proves cost-effective vs PQC alone.
5. **Usability and human factors** research into consent UX for patients and customers in an immutable ledger ecosystem.

8.3 Roadmap for Progressive Adoption

- **Phase 0:** Audit and PQC readiness planning; update SDKs and prepare migration paths.
- **Phase 1:** Deploy AI-enabled detection and permission blockchains; adopt PQC for signatures in pilot channels.
- **Phase 2:** Add selective QKD links for critical high-value nodes and integrate hybrid KMS.
- **Phase 3:** Scale federated analytics, broaden PQC rollout, and develop inter-consortium governance for cross-border deployments.

9. Conclusion

This paper has proposed a Tri-Layer Model that integrates blockchain, AI, and quantum networking primitives to provide a resilient architecture for secure transactions in finance and healthcare. Each layer contributes orthogonal strengths: ledgers supply tamper-evident audit trails and programmable policy enforcement; AI adds adaptive detection and privacy-preserving analytics; and quantum networks and PQC provide a path to protect confidentiality and integrity in the face of emerging quantum threats. Our threat analyses, use cases, and evaluation framework provide a practical blueprint for staged deployment and rigorous evaluation in real-world settings. While adoption presents engineering, economic, and governance challenges, the tri-layer model offers a defensible road map for organizations seeking to harden critical transactional systems today and prepare for a quantum future.

References

1. AbdelSalam, F. M., et al. (2023). A Systematic Review of Blockchain Technology Benefits in Healthcare. *Journal / PMC*

2. Bahache, A. N. (2024). Securing Cloud-based Healthcare Applications with a Post-Quantum Authentication Framework. *Journal (ScienceDirect).* https://www.sciencedirect.com/science/article/abs/pii/S2542660524001410

3. Durgut, S. (2025). Hybrid Quantum–Classical Deep Neural Networks Based on Security of Smart Contracts. *Applied Sciences, 15*(7), 4037. https://www.mdpi.com/2076-3417/15/7/4037

4. Fatunmbi, T. O. (2021). Integrating AI, Machine Learning, and Quantum Computing for Advanced Diagnostic and Therapeutic Strategies in Modern Healthcare. *International Journal of Engineering and Technology Research, 6*(1), 26–41. https://doi.org/10.34218/IJETR_06_01_002

5. Fatunmbi, T. O. (2023). Integrating quantum neural networks with machine learning algorithms for optimizing healthcare diagnostics and treatment outcomes. *World Journal of Advanced Research and Reviews, 17*(03), 1059–1077. https://doi.org/10.30574/wjarr.2023.17.3.0306.

6. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2024). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access / arXiv.* arXiv

7. Gupta, R. S., et al. (2025). A systematic review of quantum machine learning for clinical applications. *npj Digital Medicine* (2025). https://www.nature.com/articles/s41746-025-01597-z

8. ID Quantique. (2024). Quantum-Safe Security Solutions for Protecting Healthcare Data Networks. https://www.idquantique.com/quantum-safe-security/applications/healthcare/

9. Jeyaraman, N., et al. (2024). The Emerging Role of Quantum Computing in Enhancing Healthcare. *PNAS / PMC*. https://pmc.ncbi.nlm.nih.gov/articles/PMC11416048/

10. Kasyapa, M. S. B., et al. (2024). Blockchain integration in healthcare: benefits and challenges. *PMC article*. https://pmc.ncbi.nlm.nih.gov/articles/PMC11082361/

11. Liu, A. (2023). A Secure Scheme Based on a Hybrid of Classical and Quantum-Proof Blockchain. *Entropy*, 25(5), 811. https://www.mdpi.com/1099-4300/25/5/811

12. McMahan, B., et al. (2017). Federated Learning: Collaborative Machine Learning without Centralized Training Data. *Google Research*. (foundational FL work referenced in policy and architecture sections). https://postquantum.com/quantum-computing/use-cases-healthcare/

13. Nałęcz-Charkiewicz, K., et al. (2024). Quantum computing in bioinformatics: a systematic review. *Briefings in Bioinformatics*. https://www.researchgate.net/publication/394258536_Quantum-Classical_Hybrid_Architectures_for_Blockchain_and_Contextual_AI

14. Ozdemir, O., & Fatunmbi, T. O. (2024). Explainable AI (XAI) in Healthcare: Bridging the Gap between Accuracy and Interpretability. *Journal of Science, Technology and Engineering Research, 2*(1), 32–44. https://doi.org/10.64206/0z78ev10.

15. Perez, M., et al. (2019). Apple Heart Study (example of consumer ECG validation). *(Contextual background for ECG/QKD pilots.)* https://pmc.ncbi.nlm.nih.gov/articles/PMC11416048/

16. Rieke, N., et al. (2020). The future of digital health with federated learning. *npj Digital Medicine, 3*, 119. https://postquantum.com/quantum-computing/use-cases-healthcare/

17. Roosan, D. (2025). Post-Quantum Cryptography Resilience in Telehealth. *Blockchain in Healthcare Today.* https://blockchainhealthcaretoday.com/index.php/journal/article/view/379/721

18. Samuel, A. J. (2023). A Comprehensive Frameworks for Fraud Crime Detection and Security: Leveraging Neural Networks and AI. *Journal of Science, Technology and Engineering Research, 1*(4), 15–45. https://doi.org/10.64206/m3jxre09.

19. Samuel, A. J. (2024). Optimizing energy consumption through AI and cloud analytics: Addressing data privacy and security concerns. *World Journal of Advanced Engineering Technology and Sciences, 13*(2), 789–806. https://doi.org/10.30574/wjaets.2024.13.2.0609.

20. Singh, N., & Pokhrel, S. R. (2025). Modeling Quantum Machine Learning for Genomic Data Analysis. *arXiv*. https://www.idquantique.com/quantum-safe-security/applications/healthcare/

21. The Guardian / UK NCSC (2025). Warnings on quantum hacker readiness and guidance timelines. (Media/regulatory context).

https://www.theguardian.com/technology/2025/mar/20/uk-cybersecurity-agency-quantum-hackers

22. Topical news and industry reports: HSBC quantum bond trading pilot (Reuters, 2025) - illustrative of hybrid quantum/classical adoption in finance. https://www.reuters.com/business/finance/hsbc-says-quantum-computing-trial-helps-bond-trading-2025-09-24/