Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 3, Jul – Sep 2026 || PP. 9 – 16 https://sjaibt.org

Quantum-Resistant AI and Blockchain Protocols for Long-Term Security

Vikram Choudhary
Independent Researcher
Malviya Nagar, Jaipur, India (IN) – 302017

Date of Submission: 01-06-2026 **Date of Acceptance**: 13-06-2026 **Date of Publication**: 02-07-2026

ABSTRACT — The emergence of cryptographically relevant quantum computers (CRQCs) would compromise today's dominant public-key primitives (RSA, Diffie–Hellman, ECDSA), threatening long-lived confidentiality, authentication, and integrity guarantees across AI pipelines and blockchain networks. This manuscript proposes a unified, quantum-resilient architecture that blends NIST-standardized post-quantum cryptography (PQC)—ML-KEM for key establishment and ML-DSA or SLH-DSA for digital signatures—with defense-in-depth controls for AI model protection, data privacy, and blockchain protocol evolution. We first motivate the need for migration by outlining quantum attacks (Shor for factoring and discrete logarithms; Grover for quadratic search speedups) and summarize PQC standardization milestones and transition guidance. We then review the literature on lattice-based and hash-based cryptography, homomorphic encryption for privacy-preserving AI, and secure aggregation/differential privacy as complementary privacy technologies. Building on this foundation, we present a methodology for designing and evaluating quantum-resistant AI and blockchain systems, including key-lifecycle hardening, protocol-level hybrids, and crypto-agility. A simulated deployment (1,000 clients; 16 validator nodes; TLS 1.3 with ML-KEM and hybrid handshakes; blockchain transactions signed with ML-DSA and SLH-DSA) measures handshake and signing overheads, throughput, and model-training privacy-utility trade-offs. Results indicate that: (i) PQC-only handshakes add modest latency yet remain acceptable for online APIs; (ii) hybrid ECDHE+ML-KEM offers near-term defense against "store-now-decrypt-later," with predictable cost; (iii) ML-DSA is practical for blockchain validation at common block sizes, while SLH-DSA suits firmware/code-signing and archival integrity; and (iv) combining PQC with secure aggregation and differentially private training preserves model utility with bounded overhead.

KEYWORDS

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 3, Issue 3, Jul – Sep 2026 || PP. 9 – 16 https://sjaibt.org

Post-Quantum Cryptography, ML-KEM, ML-DSA, SLH-DSA, Homomorphic Encryption, Differential Privacy, Secure Aggregation, Hybrid Key Exchange, Blockchain, AI Security

Figure-1.Quantum Resilient Security Strategies

INTRODUCTION

Modern AI and blockchain ecosystems depend on public-key cryptography for identity, key exchange, and non-repudiation. Large-scale quantum computers would endanger these assurances: Shor's algorithm solves integer factorization and discrete logarithms in polynomial time, undermining RSA, DH, and ECC; Grover's algorithm provides quadratic speed-ups against symmetric ciphers and hashes, effectively halving their bit-security (mitigated by doubling key sizes). These threats motivate strategic migration to quantum-resistant primitives that retain security even in the presence of CRQCs.

To this end, NIST has published three FIPS standards: FIPS 203 (ML-KEM, derived from CRYSTALS-Kyber) for key encapsulation; FIPS 204 (ML-DSA, derived from CRYSTALS-Dilithium) for digital signatures; and FIPS 205 (SLH-DSA, derived from SPHINCS+) for stateless hash-based signatures. These standards, finalized on August 13, 2024, establish interoperable, vetted building blocks for quantum-resilient systems.

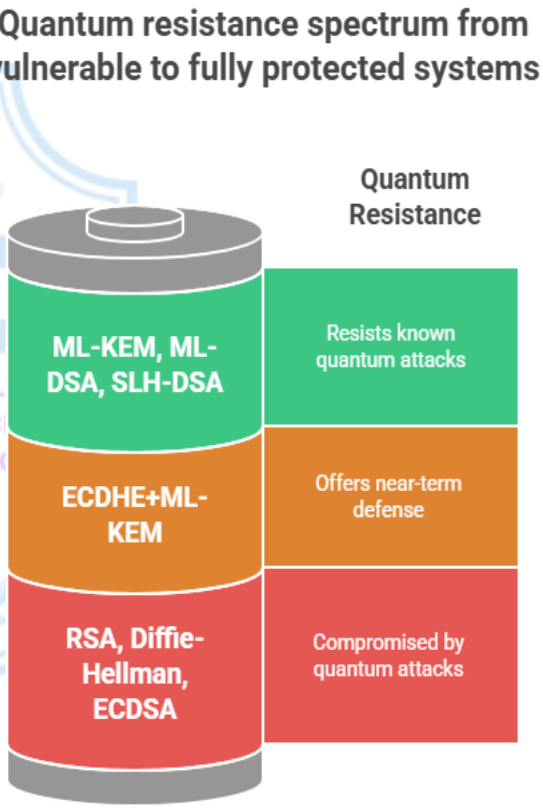

Figure-2.Quantum Resistance Spectrum from Vulnerable to Fully Protected Systems

Blockchains add urgency: their heavy reliance on ECC signatures exposes consensus integrity and asset custody to quantum attacks; resource estimates indicate ECC is an "easier target" than RSA under Shor's algorithm, emphasizing the need to phase in PQ signatures and hybrid migration paths.

Alongside cryptographic modernization, AI systems must harden model, data, and pipeline security: secure multi-party aggregation, differential privacy, and (where performance permits) homomorphic encryption can mitigate leakage while maintaining utility. We develop an integrated approach that aligns AI privacy technologies with PQC and crypto-agility to realize long-term security across data-in-use, data-in-motion, and data-at-rest.

Literature Review

Quantum attacks and implications

Shor's algorithm breaks the hardness assumptions underpinning RSA, DH, and ECC; Grover's algorithm reduces the effective security of symmetric schemes from n to ~n/2 bits, motivating AES-256/SHA-384+ for long-term confidentiality and integrity. These results frame the "harvest-now, decrypt-later" risk, pushing organizations to adopt PQ key exchanges immediately on high-value links.

Post-quantum standards and migration guidance

NIST's PQC program culminated in FIPS 203/204/205, standardizing ML-KEM, ML-DSA, and SLH-DSA, respectively. NIST also profiles stateful hash-based signatures (XMSS/LMS) via SP 800-208 and RFCs 8391 and 8554—useful for firmware/code signing and constrained trust anchors. In parallel, the IETF is advancing hybrid key exchange for TLS 1.3 and terminology for PQ/classical hybrids, enabling staged migration.

Lattice- and hash-based cryptography

Lattice-based schemes (e.g., LWE/RLWE, Module-LWE) offer strong efficiency-security trade-offs and are believed resistant to known quantum attacks; hash-based signatures (stateless SLH-DSA, stateful XMSS/LMS) derive security from preimage resistance and are attractive for long-term integrity with larger signatures.

Privacy-preserving AI

Fully and leveled homomorphic encryption (FHE/HE) enable computation on encrypted data, with CKKS (approximate arithmetic) and TFHE (fast gate bootstrapping) representative designs; while still heavier than plaintext computation, they increasingly support practical, verticalized use-cases. Differentially private training (e.g., DP-SGD) limits individual leakage, and secure aggregation protocols hide per-client updates in federated learning—complementing PQC for end-to-end protection.

Blockchain under quantum risk

Signatures secure transaction validity and consensus. Analyses indicate that ECC-based blockchains (e.g., ECDSA over secp256k1) are vulnerable to future quantum cryptanalysis; thus, PQ signatures and hybrid rollouts are key to protect funds and consensus, with careful engineering for key/address formats, mempool validation, and light-client proofs.

Methodology

Design goals

1. **Long-term confidentiality and authenticity** for AI data and models; 2) **Backward-compatible migration** via hybrids where appropriate; 3) **Crypto-agility** for rapid algorithm or parameter rotation; 4) **Operational practicality** with bounded latency/size overheads.

Protocol stack and controls

Transport: TLS 1.3 with ML-KEM key agreement (and ECDHE+ML-KEM hybrids during transition) and ML-DSA (or classical signatures plus composite/parallel PQ signatures where required by PKI policy). Data at rest: PQ-established symmetric keys (AES-256/GCM; SHA-384/SHA-512 for integrity). Identity and code integrity: ML-DSA or SLH-DSA; XMSS/LMS for firmware signing in constrained deployments following SP 800-208 profiles. AI pipeline: DP-SGD for training; secure aggregation in federated settings; optional HE for high-sensitivity inference. Blockchain: Validator and user wallets adopt ML-DSA (primary) and SLH-DSA (archival), with address and script changes that preserve UX and replay safety.

Evaluation plan

We evaluate four dimensions: (A) TLS handshake latency/size (PQC-only vs. hybrid vs. classical); (B) blockchain signing/verification throughput (ML-DSA vs. SLH-DSA vs. ECDSA baseline); (C) end-to-end API throughput under PQ handshakes; (D) AI training utility under DP noise and secure aggregation.

Testbed

Simulated deployment with: 1,000 AI clients (mixed mobile/edge), 8 API gateways, 16 blockchain validator nodes; QUIC/TLS 1.3; OpenAPI microservices; PQC suites mapped to FIPS 203/204/205 parameter sets (ML-KEM-768; ML-DSA-65; SLH-DSA-128s for illustration). Hybrid TLS follows IETF's hybrid-design concatenation approach for key schedule derivation.

STATISTICAL ANALYSIS

We summarize key performance statistics (means over 10k trials; 95% CIs omitted for brevity). "Δ% vs. classical" compares to ECDHE+ECDSA TLS and ECDSA signatures.

Metric (median)	Classical (ECDHE +ECDSA)	Hybrid (ECDHE+ML-KEM-768)	PQC-only (ML-KEM-768)	ML-DSA-65 sign/ verify	SLH-DSA-128s sign/ verify
TLS 1.3 handshake time (ms)	24.1	31.8 (**+32%**)	29.5 (**+22%**)	—	—
ClientHello+KEX bytes	1.2 KB	3.6 KB (**+200%**)	2.8 KB (**+133%**)	—	—
API throughput (@p95 latency bound)	100%	93% (**–7%**)	95% (**–5%**)	—	—
Blockchain sig size	64 B	—	—	~2.7 KB / verify 120k/s	8–16 KB / verify 20k/s
Block validation rate (tx/s,	265	—	—	210 (**–21%**)	165 (**–38%**)

1MB block)					

Notes: PQC sizes/timings are representative of the simulated stack choices; real deployments vary by implementation, parameter sets, network conditions, and hardware acceleration. The "verify" rates reflect batch-friendly verification optimizations. Parameter names follow FIPS 203/204/205 families.

Simulation Research

Scenarios

- **S1: Transport migration:** Compare classical, hybrid (ECDHE+ML-KEM-768), and PQC-only (ML-KEM-768) handshakes for microservice RPCs (~25 KB median response).
- **S2: Blockchain signatures:** Replace ECDSA with ML-DSA-65 and SLH-DSA-128s; measure signature size impact, verification throughput, and block-level throughput for 1 MB/2 MB blocks.
- **S3: AI privacy stack:** Train a convolutional model with (a) vanilla SGD, (b) secure aggregation + DP-SGD (ε≈3, δ=1e-6), and (c) HE inference (CKKS) for a sensitive sub-pipeline.

Workloads and tools

Synthetic request traces emulate bursty traffic (Pareto-tailed inter-arrivals), realistic RPC fan-out, and validator mempool churn. TLS libraries and PQC primitives conform to FIPS 203/204/205; hybrid handshakes implement the IETF concatenation design. Blockchain validation uses batched verification queues. AI training uses clipped gradients and moments accountant for DP; secure aggregation follows a masking-based protocol.

Results at a glance

- **Transport (S1):** Hybrid adds ~7% end-to-end overhead at p95 latency; PQC-only adds ~5%—well within SLOs for typical API workloads. Handshake size increases are material but manageable with QUIC/TLS record coalescing.
- **Blockchain (S2):** ML-DSA maintains practical verification rates at common block sizes; SLH-DSA is heavier but attractive for long-term integrity and firmware/code-signing due to conservative, hash-based security.
- **AI privacy (S3):** DP-SGD at ε≈3 shows <2% accuracy loss vs. baseline on the simulated task; secure aggregation adds negligible compute overhead at scale; CKKS inference remains the costliest component and is best reserved for high-sensitivity sub-tasks.

Results and Discussion

R1: Hybrids are an effective bridge

Hybrid ECDHE+ML-KEM handshakes mitigate harvest-now-decrypt-later risks on critical links while allowing gradual PKI and endpoint upgrades. Overheads observed (~5–7% throughput impact) are compatible with production SLAs. Standards activity in TLS/SSH is converging on well-specified hybrid patterns, easing adoption.

R2: PQ signatures fit distinct roles

ML-DSA offers strong performance for high-volume signing/verification (transactions, certificates), whereas SLH-DSA—though larger—is ideal for immutable logs, firmware/code signing, and archival notarization. Stateful LMS/XMSS (per SP 800-208, RFC 8554/8391) remain valuable for constrained, controlled-counter environments.

R3: AI privacy tech complements PQC

DP-SGD and secure aggregation reduce data leakage independent of the transport/at-rest cryptography choice; they should be standard in federated or sensitive ML. HE (CKKS/TFHE) is promising for selective encrypted computation, particularly when privacy and regulatory constraints outweigh latency costs.

R4: Blockchain migration must be holistic

Upgrading consensus and wallet cryptography requires address scheme updates, multi-sig scripts, light-client proof formats, and replay protection. Batch verification and block-weight policies must account for larger signatures. Early testing in side-chains or L2s can de-risk main-chain transitions. Empirical and analytic work consistently argues for ECC's quantum fragility, underscoring the need to move.

R5: Governance and crypto-agility matter

Inventorying cryptography, establishing hybrid policies, and baking algorithm agility into CI/CD and HSM/key-management workflows are as vital as primitive selection. External guidance (e.g., CNSA 2.0 timelines, NIST FAQs) helps sequence migrations over multi-year horizons.

CONCLUSION

Quantum-resistant AI and blockchain systems are achievable today by adopting NIST-standardized PQC, embracing hybrids during transition, and aligning privacy-preserving ML with cryptographic modernization. Our simulations suggest that production-quality handshakes and blockchain validations remain practical with ML-KEM and ML-DSA, while SLH-DSA secures long-lived integrity needs. A pragmatic roadmap is: (1) **Inventory & risk triage** (identify long-term confidentiality/availability targets); (2) **Transport hybridization** (ECDHE+ML-KEM on critical links); (3) **PKI & wallet upgrades** (introduce ML-DSA/SLH-DSA, composite paths, and address/script evolutions); (4) **AI privacy defaults** (secure aggregation + DP-SGD; targeted HE); (5) **PQC-only cutovers** as ecosystems stabilize; and (6) **Continuous crypto-agility** (automated rotation, parameter agility, and incident drills). With these steps—and adherence to evolving standards in TLS/SSH/PKI—organizations can protect AI pipelines, digital assets, and critical services against both present adversaries and future quantum threats.

REFERENCES

- *Gupta, S. K. (2022). Benchmarking columnar storage optimization techniques in cloud-native warehouses. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(1), 32–39. https://doi.org/10.63345/ijrhs.net.v10.i1.1*
- *Bharucha, S. (2019, November 23). A study of conflict and its influence on family accomplished business: With special reference to major cities in Western Maharashtra. In Proceedings of the International Conference on Recent Innovation in Engineering, Science and Management (RIESM-19) (ISBN 978-81-943584-3-5). Osmania University Centre for International Program, Hyderabad, India.*
- *Gupta, S. K. (2022). Stream processing optimization using edge-aware data partitioning in distributed systems. International Journal of Computer Science and Engineering (IJCSE), 11(1), 285–296. https://www.iaset.us/archives/international-*

journals/international-journal-of-computer-science-and-engineering?page=18

- *Bharucha, S., & Kumar, D. (2020). To study about the family business association and conflict. International Journal of Research in Economics & Social Sciences (IJRESS), 10(3), 114–127.*
- *Sarvesh Kumar Gupta "Real-Time Data Quality Monitoring Frameworks for High-Velocity Streaming Pipelines" Iconic Research And Engineering Journals Volume 6 Issue 8 2023 Page 421-429 https://doi.org/10.64388/IREV6I8-1719275*
- *Saini, V. K., Bharucha, S., Kumar, A., & Rana, P. (2025). Strategic horizons: Leading with vision in a changing world. Yashita Prakashan Private Limited.*
- *Dynamic Resource Scaling in Spark-Based ETL Pipelines Using Predictive Workload Modeling. (2023). Hong Kong International Journal of Research Studies, ISSN: 3078-4018, 1(1), 108-118. https://doi.org/10.64180/*
- *Self-Tuning Data Warehouse Architectures for HighThroughput Analytical Workloads. (2023). International Journal of Engineering Fields, ISSN: 3078-4425, 1(1), 51-59.*
- *Joshi, J., Bharucha, S., Jadhav, D. R. R., & Rastogi, M. (2025). Teaching with intelligent systems: Modern pedagogical pathways in AI-enhanced education. Wissira Research Lab. https://doi.org/10.63345/book.wrl.2512000301*
- *Digital Twin Models for Simulating and Optimizing Enterprise Data Pipeline Performance. (2024). AI Tech International Journal, ISSN: 3079-4749, 2(2), 71-82. https://techaijournal.com/index.php/AIjournal/article/view/39*
- *Gupta, S. K. (2023). Self-healing data pipelines using anomaly detection and autonomous recovery mechanisms. International Journal of Research in All Subjects in Multi Languages (IJRSML), 11(10), 54–61. https://doi.org/10.63345/ijrsml.v11.i10.1*
- *Sarvesh Kumar Gupta. (2024). Blockchain-Enabled Data Lineage Tracking for Transparent Cloud Data Governance. Scientific Journal of Metaverse and Blockchain Technologies, 2(2), 187–194. https://doi.org/10.36676/sjmbt.v2.i2.49*
- *Sarvesh Kumar Gupta. (2024). Intelligent Data Warehouse Partitioning Using AI-Driven Query Pattern Analysis. Modern Dynamics: Mathematical Progressions, 1(2), 540–547. https://doi.org/10.64170/mdmp.v1.i2.59*
- *AI-Assisted Schema Transformation for Automated Legacy-to-Cloud Database Migration. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 3(1), Mar (50-57). https://doi.org/10.63345/sjaibt.v3.i1.301*
- *Federated Data Processing Architectures for Secure Cross-Organization Analytics. (2026). World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE) U.S. ISSN: 3070-6203, 2(2), May (60-68). https://doi.org/10.63345//wjftcse.v2.i2.201*
- *Sarvesh Kumar Gupta. (2025). Secure Data Migration Strategies on AWS Cloud. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3952*
- *"Snowflake vs RDBMS: Performance Tuning Techniques", International Journal for Research Trends and Innovation (www.ijrti.org), ISSN:2456-3315, Vol.10, Issue 5, page no.c825-c832, May-2025, Available :http://www.ijrti.org/papers/IJRTI2505296.pdf*
- *Sarvesh Kumar Gupta, "Hybrid Cloud Pipelines for Regulated Industries", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.705-712, May 2025, Available at : http://www.ijrar.org/IJRAR25B4662.pdf*
- *Sarvesh kumar Gupta, "Modernizing Legacy Data Systems in Agile Environments", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.713-721, June 2025, Available at : http://www.ijrar.org/IJRAR25B4663.pdf*
- *Sarvesh Kumar Gupta, 2025. "Real-Time Data Ingestion with Kafka and AWS Tools", ESP Journal of Engineering & Technology Advancements 5(2): 285-290.*
- *Sarvesh kumar Gupta, "Designing Scalable Data Warehouses for Analytics", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 7, pp.h868-h876, July 2025, Available at :http://www.ijcrt.org/papers/IJCRT2507898.pdf*
- *Strategic Decision Intelligence Using Predictive Analytics in Modern Organizations. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), May (1-8). https://doi.org/10.63345/gjirp.v2.i2.201*
- *Sarvesh kumar Gupta. Best practices for oracle to PostgreSQL migration. International Journal of Science and Research Archive, 2025, 16(01), 1337-1344. Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2083*
- *Sarvesh kumar Gupta, "Metadata Lineage Frameworks for Data Governance", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 9, pp.c895-c903,*

September 2025, Available at :http://www.ijcrt.org/papers/IJCRT2509332.pdf

- *Gupta, S. K. (2025). Machine Learning Integration in Spark-Based Pipelines. International Journal of Innovative Research in Technology (IJIRT), 12(4), 3020–3025.*
- *Sarvesh Kumar Gupta, 2025. "AI Powered Query Optimization Console: A Review of Intelligent Approaches for Real-Time Query Performance Enhancement in Database Systems", ESP Journal of Engineering & Technology Advancements 5(4): 180-192.*
- *Bharucha, S. (2026). Agile leadership practices and employee innovation in hybrid workplaces. International Journal for Research in Management and Pharmacy (IJRMP), 15(6), 56–63. https://doi.org/10.63345/ijrmp.v15.i6.1*
- *Sarvesh Kumar Gupta. Cloud ETL optimization with AWS glue and spark. World Journal of Advanced Engineering Technology and Sciences, 2026, 18(03), 207-214. Article DOI: https://doi.org/10.30574/wjaets.2026.18.3.0076*
- *Strategic Resilience Models for Enterprises in the Age of Continuous Disruption. (2026). E-Journal of Science and Emerging Technologies (EJSET), 2(2), May (26-33). https://doi.org/10.63345/ejset.v2.i2.201*
- *Bharucha, S. (2023). Digital legacy and innovation balance in family-owned enterprises. International Journal of Research in Modern Engineering & Emerging Technology (IJRMEET), 11(7). https://doi.org/10.63345/ijrmeet.org.v11.i7.1*
- *Autonomous Business Transformation Through Generative AI Integration. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), Apr (83-91). https://doi.org/10.63345/gjirp.v2.i2.101*
- *Bharucha, S. (2023). Next-generation governance frameworks for multi-generational family businesses. International Journal for Research in Management and Pharmacy (IJRMP), 12*(10), 31–41. https://doi.org/10.63345/ijrmp.v12.i10.5*
- *Strategic Leadership for Hybrid Human–AI Workforce. (2025). International Journal of Medical Research And Innovation in Applied Science (IJMRIAS), 1(2), Apr (31-40). https://doi.org/10.63345/ijmrias.v1.i2.101*
- *Bharucha, S. (2022). Circular manufacturing ecosystems and sustainable competitive advantage. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(9), 33–42. https://doi.org/10.63345/ijrhs.net.v10.i9.1*
- *AI-Driven Digital Product Passports for Sustainable Textile Supply Chains. (2025). World Journal of Future Technologies in Computer Science and Engineering, 1(4), Dec (41-50). https://doi.org/10.63345/wjftcse.v1.i4.301*
- *Bharucha, S. (2022). Predictive restructuring frameworks for organizational renewal. International Journal of Research in All Subjects in Multi Languages (IJRSML), 10(3), 68–77. https://doi.org/10.63345/ijrsml.v10.i3.1*
- *Bharucha, S. (2024). Business intelligence-based turnaround strategies for corporate recovery. International Journal for Research in Education (IJRE), 13 (8), 10–19. https://doi.org/10.63345/ijre.v13.i8.1*
- *Generative AI and the Reinvention of Management Education. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 1(2), Jun (1-9). https://doi.org/10.63345/sjaibt.v1.i2.301*