

Quantum-Proof Blockchain and Artificial Intelligence: An End-to-End Reference Architecture for Post-Quantum Distributed Ledger Resilience

Ian Staley
Independent Researcher, USA

Correspondence: ian.t.staley@gmail.com

Received: 17 Apr 2026 **Accepted:** 01 June 2026 **Published:** 06 July 2026

Abstract

Quantum computing's accelerating trajectory threatens the cryptographic foundations of every major blockchain network. Recent research demonstrates that fewer than 500 000 physical qubits could break ECC-256 in approximately nine minutes, while expert surveys place a 28–49% probability of a cryptographically relevant quantum computer (CRQC) emerging within ten years. This paper presents a layered reference architecture for end-to-end quantum-resilient distributed ledger systems, making three contributions: (1) a structured threat analysis applying STRIDE across blockchain architectural layers and post-quantum cryptography (PQC) migration phases; (2) a seven-layer reference architecture with per-layer interface specifications and dependency graph; and (3) a multi-chain quantum readiness assessment covering twelve major networks with fintech-specific migration strategies for decentralised finance (DeFi), stablecoins, tokenised real-world assets (RWA), and decentralised identity (DID). A critical finding is that blockchain's primary quantum risk is real-time signature forgery upon CRQC arrival, not retroactive harvest-now-decrypt-later (HN DL) attacks on signatures. Cross-chain bridges, data availability layers, and Lightning Network payment channels are identified as the most critically neglected quantum attack surfaces.

Keywords: *Post-quantum cryptography, Blockchain security, Quantum-resistant consensus, Crypto-agility, AI security orchestration*

JEL Classifications: *G20, O33, L86*

1. Introduction

The vulnerability of blockchain cryptography to quantum computing was first systematically assessed for distributed ledger technology (DLT) by Campbell [1], who evaluated the Elliptic Curve Digital Signature Algorithm (ECDSA) across Bitcoin, Ethereum, and enterprise blockchains against quantum threats and proposed lattice-based alternatives. Shor's algorithm [2] efficiently solves the elliptic curve discrete logarithm problem (ECDLP) underpinning ECDSA (secp256k1) and EdDSA (Ed25519), enabling private key derivation from exposed public keys. Grover's algorithm [3] provides quadratic speedup on preimage search, reducing SHA-256's preimage resistance from 256 to 128 bits; for collision resistance, the Brassard–Høyer–Tapp algorithm reduces effective security from 128 to approximately 85 bits. Neither reduction breaks SHA-256 outright, but both narrow the security margin for proof-of-work (PoW) mining and could create centralisation pressure favouring quantum-equipped miners.

The threat timeline has compressed dramatically. Google Quantum AI's March 2026 disclosure demonstrated that fewer

than 500 000 physical qubits could compromise ECC-256 in approximately nine minutes [4], while the Global Risk Institute 2025 survey found that 28–49% of experts rated the probability of a CRQC emerging within ten years as significant [5]. Cambridge's Centre for Alternative Finance reported that only 0.35% of blockchain-related GitHub activity references post-quantum algorithms [6]. Campbell [7] quantified the throughput implications: current testnet implementations on permissioned systems show 52–57% throughput degradation with PQC signatures, creating a “timeline collision” where the 10- to 15-year threat horizon collides with the reality that decentralised communities may require 10–15 years to accept the associated capacity loss.

Applying Mosca's inequality [8] – if X (data shelf life) + Y (migration time) > Z (time to CRQC), migration must begin immediately – the Federal Reserve Board [9] concluded that blockchain's permanent, immutable records remain vulnerable to retroactive attack [10]. However, a critical nuance identified by Thaler [11] reshapes this calculus: HN DL applies to encryption (confidentiality), not signatures (integrity). Blockchain signatures are not retroactively vulnerable – an

attacker cannot retroactively forge a past signature to steal funds. The real threat is real-time signature forgery once a CRQC arrives. HNDL does apply to privacy coins (Zcash, Monero) where encrypted transaction data can be retroactively deanonymised. Approximately 6.9 million Bitcoin (BTC) reside in quantum-vulnerable addresses with exposed public keys [12]. In Ethereum's account-based model, any address that has sent a transaction has its public key permanently recorded on-chain; Google Quantum AI [4] identified the top 1000 wallets holding approximately 20.5 million ETH with permanently exposed keys.

Building on the STRIDE-based blockchain security assessment of Baseri et al. [13] and the risk management principles of Campbell [14], this paper advances the literature beyond existing surveys [7, 13–17] through three contributions: (1) a structured threat analysis applying STRIDE and Mosca's Theorem [8] to blockchain; (2) a seven-layer reference architecture with per-layer interface specifications; and (3) a multi-chain quantum readiness assessment with fintech-specific migration strategies.

1.1 Research Questions

RQ1: What is the comprehensive quantum threat surface across blockchain architectural layers, and how should adversary capabilities be formally modelled? RQ2: What architectural patterns enable end-to-end quantum resilience from off-chain infrastructure through cross-chain interoperability, incorporating NIST-standardised and emerging PQC primitives? RQ3: What governance mechanisms, regulatory mandates, and migration strategies are required for fintech applications including DeFi, stablecoins, tokenised RWA, and DID?

1.2 Survey Methodology

This study employs a structured literature review. We searched IEEE Xplore, ACM Digital Library, Springer, Elsevier ScienceDirect, IACR ePrint Archive, arXiv, and the JBBA back catalogue (<https://jbba.scholasticahq.com>) using queries combining “post-quantum,” “quantum-resistant,” and “quantum-safe” with “blockchain,” “distributed ledger,” “smart contract,” and “consensus.” Primary sources were restricted to 2020–2026, with the following foundational works included regardless of date: Shor (1994) [2], Grover (1996) [3], Regev (2009) [18], Lyubashevsky et al. (2010) [19], Langlois and Stehlé (2015) [20], Ben-Sasson et al. (2018) [21], Chalkias et al. (2018) [22], Campbell (2019a, 2019b) [1, 16], and Campbell (2020) [14]. This process yielded 107 primary references. Industry context sources (vendor announcements, regulatory guidance, news reporting) are included where necessary but do not bear the weight of empirical claims.

1.3 Related Surveys and Positioning

Table 1 positions this work against prior surveys. This work is distinguished by its integration of threat modelling, PQC

primitive assessment, and architectural specification within a single layered framework, incorporating AI orchestration and fintech-specific analysis not found in any individual prior survey. Additional surveys by Mallick et al. [23] and Wicaksana et al. [24] provide complementary perspectives on quantum disruption and blockchain security infrastructure respectively. Notably, Campbell's body of JBBA work [1, 7, 14, 16] provides foundational treatment of post-quantum DLT cryptography, hybrid PKI migration, and enterprise risk frameworks that this paper extends into a comprehensive multi-layer architecture.

2. Formal Quantum Threat Analysis

Building on the risk management framework established by Campbell [14] for enterprise DLT in the PQC era, and the STRIDE-based blockchain security assessment of Baseri et al. [13], we define a structured threat analysis across three adversary capability tiers.

Table 1. Comparison with existing post-quantum blockchain surveys

Feature	Campbell [1, 7]	Baseri [13]	Yang [25]	Busch [26]	Khod. [27]	Taher. [17]	This Work
STRIDE threat analysis	X	✓	X	X	X	X	✓
PQ-ZKPs (STARKs, lattice)	X	X	X	X	X	X	✓
Side-channel attacks on PQC	X	X	X	X	X	X	✓
Layered architecture	X	X	X	X	X	X	✓
AI orchestration layer	X	X	X	X	X	X	✓
Multi-chain readiness	X	✓	X	X	✓*	X	✓
DeFi/stablecoin analysis	X	X	X	X	X	X	✓
Hybrid PQC migration	✓	✓*	X	X	X	X	✓
Exotic PQ signatures	X	X	X	✓	X	X	✓*
Throughput analysis	✓	✓*	X	X	✓*	X	✓

✓ = comprehensive coverage; ✓* = partial coverage; X = not covered

Table 2. Quantum adversary capability tiers and blockchain impact

Adversary Tier	Capability	Algorithm Threat	Blockchain Impact	Timeline Est.
Classical	Side-channel, impl. flaws	None (ECDLP intractable)	Key mgmt attacks only	Present
Quantum-Advantaged	Hundreds of noisy qubits	Grover (quadratic)	PoW centralisation risk	2025–2030
Full CRQC	Millions of physical qubits	Shor (polynomial ECDLP)	All ECDSA/EdDSA broken	2029–2040

2.1 Adversary Capability Tiers

A Classical Adversary exploits implementation flaws, side-channel leakage, and poor key management but cannot break ECDSA or RSA mathematical foundations in polynomial time. A Quantum-Advantaged Adversary (partial CRQC, hundreds of noisy qubits) achieves quadratic speedup via Grover's algorithm, effectively halving symmetric security (e.g., AES-128 reduced to 64-bit effective security), but cannot yet execute Shor's algorithm at meaningful key sizes. A Full CRQC Adversary executes Shor's algorithm to break ECDSA, RSA, and DSA in polynomial time and can derive private keys from any exposed public key [2, 4, 28]. Table 2 summarises the three adversary capability tiers and their corresponding blockchain impact and estimated timelines.

2.2 STRIDE Analysis

Following Baseri et al. [13], we apply STRIDE aligned with NIST SP 800-30 across seven architectural layers in three transition phases (pre-transition, hybrid migration, post-transition). The full $6 \times 7 \times 3$ STRIDE matrix is provided in Appendix A. The three most critical threat categories are: Spoofing (validator identity forgery via Shor-derived private keys in Proof-of-Stake (PoS) consensus), Tampering (transaction modification during block propagation exploiting the window between broadcast and confirmation), and Information Disclosure (the HNDL paradigm for encrypted/shielded data and retroactive deanonymisation of privacy coin transactions [9, 10]). Denial of Service threats include blockchain state bloat from enlarged PQC signatures [7, 29]. Elevation of Privilege threatens smart contract admin keys and governance mechanisms. Repudiation risks arise from the possibility of quantum-forged signatures undermining transaction non-repudiation guarantees.

2.3 Mosca's Theorem Applied to Blockchain

Mosca's inequality [8] states: if $X + Y > Z$, migration must begin immediately. Table 3 applies this framework across blockchain asset classes, incorporating Campbell's [7] throughput degradation data and the HNDL-signatures distinction from Thaler [11].

2.4 Quantum Attack Cost Economics

Qubit requirements have collapsed dramatically. Cheviguard et al. [28] at EUROCRYPT 2026 reduced P-256 requirements to 1 193 logical qubits (a 44% reduction from prior estimates of 2 124). The

Table 3. Mosca's Theorem parameters for blockchain asset classes

Asset Class	Shelf Life (X)	Migration (Y)	X + Y	CRQC Window (Z)	Status
Bitcoin (store of value)	20+ yr	5–10 yr	25–30	4–15 yr	OVERDUE
Privacy coins (shielded)	10–50 yr	3–5 yr	13–55	4–15 yr	OVERDUE
Smart contract admin keys	5–20 yr	2–5 yr	7–25	4–15 yr	URGENT
Tokenised RWA (30yr bonds)	30+ yr	3–7 yr	33–37	4–15 yr	OVERDUE
Lightning channels	Days – months	N/A (structural)	N/A	4–15 yr	REDESIGN

Google Quantum AI whitepaper [4] demonstrated fewer than 500 000 physical qubits on superconducting architecture with approximately 9-minute runtime – a $20\times$ reduction from prior estimates. A companion analysis showed approximately 26 000 physical qubits on neutral-atom architecture could break ECC-256 in approximately 10 days. ECC is now decisively easier to break than RSA; P-256 requires fewer qubits than RSA-3072.

3. Seven-Layer Quantum-Resilient Reference Architecture

The proposed layered reference architecture organises quantum-resilient blockchain into seven distinct layers, extending Campbell's [16] hybrid classical/PQ PKI design and risk management framework [14], and synthesising findings from NIST SP 1800-38, the QuantumShield-BC framework [30], QLink [31], and Cloud Security Alliance guidelines [32]. Table 5 specifies the per-layer interface contracts and PQC requirements. Each subsequent section addresses one or more layers in detail, with the relevant cryptographic primitives, threat vectors, and chain-specific readiness woven into the architectural context. Table 4 summarises the chronological evolution of physical-qubit requirement estimates for breaking ECC-256.

Figure 1. Seven-layer reference architecture for end-to-end quantum-resilient distributed ledger systems, spanning off-chain key custody through cross-chain interoperability and AI-assisted security orchestration.

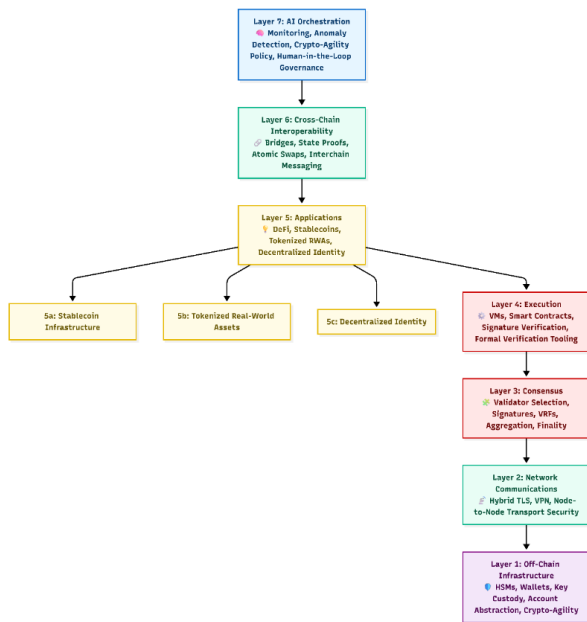


Figure 1. Seven-layer architecture

The dependency graph is as follows: L1 provides key material consumed by all higher layers. L2 provides secure communications required by L3. L3 provides finality consumed by L4. L4 provides state transition execution for L5. L6 spans multiple L1–L5 stacks across chains. L7 operates as a cross-cutting monitoring and orchestration fabric consuming telemetry from all layers and issuing policy updates. A quantum compromise at any lower layer propagates upward: a breach of L1 key management compromises all dependent layers.

4. Post-Quantum Cryptographic Primitives

NIST finalised three PQC standards on 13 Aug 2024 [33], providing the cryptographic foundation for Layers 1 and 4. Yokubov and Gan [34] provided early JBBA-published performance benchmarks comparing pre-standardisation PQC candidates in blockchain contexts, establishing baseline expectations for the performance trade-offs now confirmed by NIST standardisation.

4.1 NIST-Standardised Algorithms

FIPS 203 (ML-KEM) [37] standardises lattice-based key encapsulation. ML-KEM-768 produces 1184-byte public keys and 1088-byte ciphertexts; on ARM Cortex-M0+ it runs 17× faster than ECDH P-256 [38]. FIPS 204 (ML-DSA) [39] standardises lattice-based digital signatures. ML-DSA-44 produces 2420-byte signatures and 1312-byte public keys – a 38× combined size increase over ECDSA – but signing completes in 100–200 microseconds [15, 38]. FIPS 205 (SLH-DSA) [40] provides stateless hash-based signatures with compact public keys (32–64 bytes) but signatures of 7856–49 856 bytes, unsuitable for high-throughput blockchain. FN-DSA (draft FIPS 206), based on FALCON, offers 666-byte signatures (only 10×

ECDSA) with 897-byte public keys [41], but requires floating-point arithmetic susceptible to side-channel attacks [42, 43]. HQC was selected as a code-based KEM backup in March 2025 [44], with NIST SP 800-227 [45] providing hybrid KEM guidance. Table 6 compares candidate PQC signature algorithms across public-key size, signature size, signing time, and suitability for blockchain workloads.

Table 4. Qubit requirement estimates for breaking ECC-256 (chronological)

Year	Physical Qubits	Architecture	Runtime	Source
2022	~13 million	Superconducting	~8 hours	Webber et al. [35]
2023	~9 million	Superconducting	~4 hours	Litinski [36]
Mar 2026	<500 000	Superconducting	~9 minutes	Babbush et al. [4]
Mar 2026	~26 000	Neutral atom	~10 days	Babbush et al. [4]
EUROCRY PT 2026	1193 logical	Arch-indep.	Variable	Chevignard [28]

Table 5. Seven-layer architecture: interface specifications and PQC requirements

Layer	Function	Primary PQC Requirement	Depends On	Key Interface
L1: Off-Chain	Key mgmt, wallets, DID, HSMs	ML-DSA/FN-DSA key generation	—	Key material → L2, L4
L2: Network	Node-to-node TLS, P2P gossip	ML-KEM hybrid key exchange	L1 (node identity)	Secure channel → L3
L3: Consensus	Block production, validation	PQ-VRF, PQ validator sigs	L2 (comms), L1 (keys)	Finality signal → L4
L4: Execution	VM, smart contracts, precompiles	PQC precompiles, PQ-ZKPs	L3 (finality), L1 (keys)	State transitions → L5
L5: Application	DeFi, tokens, RWA, DID	PQC tx signatures, hybrid auth	L4 (execution)	User-facing ops
L6: Cross-Chain	Bridges, atomic swaps, relays	PQ bridge validator sigs	L1–L5 (per chain)	Cross-chain proofs
L7: AI Orchestration	Monitoring, crypto-agility, IDS	AI-driven algorithm selection	L1–L6 (telemetry)	Policy → all layers

Table 6. PQC signature algorithm comparison for blockchain workloads

Algorithm	Public Key	Signature	Combined	Sign Time *	Size Ratio	Best For
ECDSA (secp256k1)	33 B	64 B	97 B	~0.01 ms	1×	Current baseline
ML-DSA-44 (FIPS 204)	1312 B	2420 B	3732 B	~0.1 ms	38×	General signing
ML-DSA-65 (FIPS 204)	1952 B	3309 B	5261 B	~0.15 ms	54×	Higher security
FN-DSA-512 (Draft)	897 B	666 B	1563 B	Variable	16×	Size-constrained
SLH-DSA-128s (FIPS 205)	32 B	7856 B	7888 B	5–50 ms	81×	Low-freq signing
XMSS (SP 800-208)	~64 B	~2500 B	~2564 B	~1 ms	26×	Stateful (blockchain)

*Signing times measured on x86-64 with OpenSSL (ECDSA) and reference implementations (PQC); ARM benchmarks in [38].

4.2 Lattice Cryptography Foundations

All three primary NIST standards build on lattice problems. The Learning with Errors (LWE) problem [18] operates over general lattices. Ring-LWE [19] reduces keys to $O(n)$ using polynomial rings. Module-LWE [20] interpolates between both, hedging against potential ideal lattice attacks. ML-KEM relies on Module-LWE with $q = 3329$; ML-DSA combines Module-LWE and Module-SIS via Fiat-Shamir with rejection sampling; FN-DSA uses NTRU-SIS. No known quantum algorithm solves standard lattice problems in polynomial time. These problems are conjectured to be resistant to quantum attack based on the absence of efficient reductions to the Hidden Subgroup Problem over Abelian groups, though no formal proof of quantum hardness exists [15].

4.3 Hash-Based Signatures and Blockchain State Management

XMSS (RFC 8391) and LMS (RFC 8554), profiled in NIST SP 800-208, are stateful hash-based schemes producing 2.5–5 KB signatures. The The Blockchained Post-Quantum Signatures (BPQS) construction [22] exploits blockchain as a state manager: the immutable append-only log naturally tracks one-

time key usage. Solana's Winternitz Vault [47] uses truncated Keccak256, creating new vaults with fresh keys per transaction.

4.4 Exotic Post-Quantum Signatures

Buser et al. [26] survey PQ exotic signatures across four categories: account management (multi-/aggregate), consensus efficiency (threshold), scriptless blockchain (adaptor), and privacy (ring/blind). JPMorgan published threshold ML-DSA [48] – the first threshold signature scheme fully compatible with ML-DSA. NTT's Ringtail [49] achieved two-round PQ threshold signing from standard LWE across five continents in 2.5 seconds. For Boneh–Lynn–Shacham (BLS) aggregate signature replacement, Drake et al. [50] propose leanXMSS with STARK-based aggregation achieving approximately 250× compression.

5. Post-Quantum Zero-Knowledge Proofs

Zero-knowledge proof (ZKP) systems underpin Layer 4 execution for privacy and scalability. Their quantum safety varies fundamentally by construction. Table 7 assesses the quantum safety of major zero-knowledge proof systems and their production status.

5.1 zk-SNARK Quantum Vulnerability

Groth16 and PLONK depend on elliptic curve pairings over BLS12-381 or BN254, directly breakable by Shor's algorithm [2, 4]. Critically, Thaler [11] established that ZK proofs are immune to HNDL: the zero-knowledge property ensures nothing about the secret witness is revealed, so there is no confidential information to harvest. Past proofs remain valid; only post-CRQC forgery of new false proofs becomes possible.

5.2 zk-STARKs as Native Post-Quantum Proofs

zk-STARKs [21] rely exclusively on collision-resistant hash functions via FRI [51] and Merkle tree commitments. STARK proof sizes range from 45–200 KB (100–1000× larger than Groth16) with verification costs of approximately 1–2.5 million gas on Ethereum. StarkNet is the only major production Layer 2 (L2) that is natively quantum-resistant end-to-end.

5.3 Lattice-Based ZKPs and Folding Schemes

The Ishai-Su-Wu construction [52] achieves 16 KB proof size for 2^{20} constraints – 10.3× shorter than Aurora but 131× longer than Groth16. LatticeFold [53] is the first lattice-based folding scheme, using Ajtai commitments over Module-SIS with performance comparable to HyperNova. LatticeFold+ [54] delivers approximately 5× faster proving. Symphony [55] compresses 1000+ NP statements with sub-200 KB proofs.

5.4 L2 Rollup Quantum Safety

STARK-based rollups (quantum-safe): StarkNet, StarkEx, Polygon Miden. SNARK-based rollups (quantum-vulnerable): zkSync Era (PLONK), Scroll (KZG-based), Linea, Loopring. Polygon zkEVM uses a hybrid STARK→SNARK pipeline where the final SNARK wrapper reintroduces vulnerability.

6. Side-Channel Attacks on PQC Implementations

The gap between mathematical security and deployed security is critical for blockchain validator nodes. Ravi et al. [56] provide a comprehensive taxonomy classifying attacks on ML-KEM and ML-DSA by target procedure, operation (NTT, polynomial multiplication, sampling), and technique. Table 8 summarises documented side-channel attacks against NIST PQC algorithm implementations.

Table 7. ZKP systems quantum safety assessment

ZKP System	Basis	Proof Size	Quantum-Safe?	Production Status
Groth16	EC pairings (BLS12-381)	128–192 B	No (Shor)	zkSync, Loopring
PLONK	EC pairings (BN254)	400–800 B	No (Shor)	Scroll, Aztec
zk-STARKs	Hash functions (FRI)	45–200 KB	Yes	StarkNet, StarkEx
Ishai-Su-Wu	Lattices (Module-SIS)	~16 KB	Yes	Research only
LatticeFold	Lattices (Ajtai)	~50–200 KB	Yes	Research only

Table 8. Side-channel attacks on NIST PQC algorithms

Target	Attack Type	Traces	Success Rate	Source
ML-DSA	Deep-learning-assisted on <code>unpack_sk()</code>	1	9% (full s_1)	Wang [57]
ML-DSA	NTT + SIS lattice reduction	5,000	100% in 2.4 min	Qiao [59]
ML-KEM	5th-order masked, copy-paste	16	Key recovery	Dubrova et al. [57, 58]
FN-DSA	EM side-channel (FFT)	Single	Partial key	Karabulut [42]
FN-DSA	Power analysis (ChipWhisperer)	5,000	Full key recovery	Guerreau [43]

6.1 Key Attack Results

Wang et al. [57] achieved 9% probability of recovering the complete ML-DSA secret vector from a single power trace on ARM Cortex-M4, approaching 100% with multiple traces. Olaluwe et al. [58] documented how deep learning enables cross-device portability and bypasses low-order masking. FALCON's floating-point arithmetic creates persistent vulnerabilities: Karabulut and Aysu [42] demonstrated electromagnetic side-channel attacks, while Guerreau et al. [43] achieved full Falcon-512 key recovery with 5000 power traces. Qiao et al. [59] combined NTT leakage with SIS lattice reduction to recover ML-DSA keys using 5000 traces in 2.4 minutes – a 400× speedup over prior attacks.

6.2 Countermeasure Overhead

First-order masking slows operations approximately 2.5–3×, with complete masking up to 40× [56]. For ML-DSA, NTT masking and shuffling impose 12–197% overhead on key generation and 32–490% on signing. For blockchain validators processing thousands of attestations per epoch, this compounds the throughput degradation quantified by Campbell [7] (52–57% on permissioned testnet), making hardened PQC implementations essential for nodes controlling billions in staked value.

7. Blockchain Throughput Degradation and Mitigations

Campbell [7] provided the most detailed analysis of PQC throughput impact on Bitcoin and Ethereum, demonstrating 52–57% throughput degradation on permissioned testnet implementations and estimating 60–70% degradation in permissionless networks. Solana's Project Eleven testnet demonstrated 90% speed reduction when substituting Ed25519 with PQC signatures [60]. Mitigations include off-chain signature storage with on-chain hash commitments; PQC EVM precompiles demonstrated by LACChain/IDB at approximately 1,200 gas for Falcon-512 [61]; STARK-based signature aggregation [50]; JPMorgan's threshold ML-DSA [48]; and FPGA acceleration [15].

8. Layers 1–2: Off-Chain Infrastructure and Network Communications

Layer 1 encompasses quantum-safe key management, wallet infrastructure, and DID. Campbell's [16] hybrid classical/PQ PKI design for Hyperledger Fabric demonstrated the first enterprise blockchain integration of post-quantum key exchange alongside classical ECDSA, establishing the dual-key paradigm now adopted by multiple projects. Thales Luna HSM v7.9 [62] natively supports ML-KEM, ML-DSA, and LMS-HSS. Entrust nShield 5 [63] provides CAVP-validated support. Crypto4A remains the only vendor with a genuinely quantum-safe internal HSM architecture [64]. Account-abstraction wallets (ERC-4337, EIP-7702) enable upgrade to PQC without protocol changes [65, 66]. Critically, CCSS v9.0

[67] – the primary industry custody standard – contains no mention of PQC migration. Layer 2 requires quantum-safe TLS 1.3 using hybrid key exchange [68]. The Open Quantum-Safe project [69] provides liboqs. BIS Project Leap [70] transmitted payment messages via quantum-resistant VPN with no significant performance impact.

9. Layers 3–4: Consensus and Execution

QuantumShield-BC [30] proposed Quantum Byzantine Fault Tolerance (Q-BFT) using quantum random number generation (QRNG) for unbiased leader selection, reporting 7000+ transactions per second (TPS) with 100 validators. QRL 2.0 [71, 72] demonstrates ML-DSA-based PoS consensus. Post-quantum verifiable random functions (VRFs) are essential for fair validator selection: X-VRF [73] achieved 449 TPS using XMSS, while LB-VRF [74] provides lattice-based VRFs. No efficient PQC equivalent to BLS signature aggregation exists, requiring STARK-based aggregation [50]. On the execution layer, QRL's Quantum Resistant Virtual Machine (QRVM) forks the EVM to execute Hyperion contracts [72]. The poqeth project [75] proposed optimistic PQ signature verification at approximately 1200 gas. Aptos proposed AIP-137 selecting SLH-DSA [76]. Data availability layers using KZG polynomial commitments (EIP-4844, Celestia, Avail) are directly breakable by Shor's algorithm; FRI [51] provides the quantum-safe alternative but with logarithmic proof sizes versus KZG's constant 48 bytes.

10. Layers 5–7: Application, Cross-Chain, and AI Orchestration

10.1 Application Layer: DeFi and Stablecoin Vulnerability

Google Quantum AI [4] confirmed that approximately \$200 billion in stablecoins and tokenised assets depend on vulnerable admin keys. Oracle signature forgery (Chainlink's OCR uses ECDSA) could trigger cascading liquidations. Non-upgradeable smart contracts are permanently vulnerable. A quantum-resilient DeFi identity framework [77] demonstrated integration with six major protocols. Canton Network's BOLTS Technologies' QFlex pilot [77] operationalised crypt agility at the transaction level – defined as the architectural property enabling individual transactions to select among multiple signature algorithms without protocol-level changes. Circle announced a four-phase PQ roadmap for Arc blockchain [79]; BTQ Technologies proposed QSSN [80], a dual-signature framework preserving ERC-3643 compatibility.

10.2 Application Layer: Tokenised RWA and Decentralised Identity

The RWA market reached approximately \$24 billion by mid-2025, projected to \$16 trillion by 2030 [81]. ERC-3643 depends on ONCHAINID with ECDSA; no quantum migration roadmap exists. W3C Verifiable Credentials are quantum-vulnerable. eIDAS 2.0 mandates EU Digital Identity

Wallet deployment by November 2026, but prototypes use RSA/ECC [82, 83]. Machine identity ratios of 82:1 (CyberArk [84]) mean non-human DIDs need quantum-safe authentication from inception.

10.3 Cross-Chain Interoperability

Cross-chain bridges are the most neglected quantum attack surface. QLink [31] proposes a Layer-3 quantum-safe bridge using Dilithium/Falcon with HSM-sealed keys. Algorand State Proofs use Falcon for quantum-safe cross-chain verification [85]. The QCG-ST framework [86] demonstrates quantum-safe atomic swaps. Campbell [7] identifies cross-chain interoperability as a critical migration challenge for hybrid PQC schemes.

10.4 AI Orchestration

AI functions as a cross-cutting fabric following the pattern: "AI recommends, smart contracts constrain, humans govern." AI-driven security orchestration – the use of machine learning systems to monitor, detect, and coordinate cryptographic migration across heterogeneous blockchain environments – is architecturally essential. QASB-IDS [87] integrates CNN-LSTM with PQ blockchain for intrusion detection. Quantum Restricted Boltzmann Machines demonstrated superior accuracy for Ethereum attack classification [88]. CISA mandated automated cryptography discovery tools [89]; IBM Guardium Quantum Safe provides cryptographic posture management – monitoring enterprise cryptography use, uncovering cryptographic vulnerabilities, and prioritising remediation across conventional and quantum-enabled risks [90]. VOPPA [91] proposes AI governance ensembles. PQS-BFL [92] integrates ML-DSA-65 for federated learning; QuantumTrust-FedChain [93] reported 98.3% anomaly detection accuracy.

10.5 Privacy-Preserving Technologies

Fully homomorphic encryption (FHE) is inherently quantum-safe: BGV, CKKS, and TFHE all build on lattice problems. Shamir Secret Sharing is information-theoretically secure. However, threshold ECDSA protocols (GG18/GG20) are critically vulnerable because both ECDSA and Paillier encryption are broken by Shor. Trusted execution environments (TEEs) face hardware rather than cryptographic quantum risks; attestation keys require PQC migration. Table 9 summarises the quantum resilience of major privacy-preserving technologies.

11. Payment Channel Quantum Vulnerability

Lightning Network channels require continuous public key exposure – a fundamentally different threat from on-chain transactions. Wertheimer [94] assessed that Lightning is structurally incompatible with post-quantum security and that BIP-360 does not address Lightning's vulnerability. Hash-locked time contracts (HTLCs) present a dual security profile: hash preimage revelation is quantum-resilient, but underlying

ECDSA/Schnorr signatures are fully vulnerable to Shor. Ethereum state channels share identical risk.

Table 9. Privacy-preserving technologies quantum resilience

Technology	Basis	Quantum-Safe?	Migration?
FHE (BGV, CKKS, TFHE)	Lattice (Ring-LWE)	Yes	No
Shamir Secret Sharing	Polynomial interpolation	Yes	No
Threshold ECDSA (GG18/GG20)	ECDSA + Paillier	No	Critical
zk-STARKs	Hash functions	Yes	No
zk-SNARKs (Groth16)	EC pairings	No	Critical
TEEs (SGX, SEV-SNP)	Hardware isolation	Partial	Attestation only

12. Multi-Chain Quantum Readiness Assessment

Table 10 presents the multi-chain quantum readiness assessment as of April 2026.

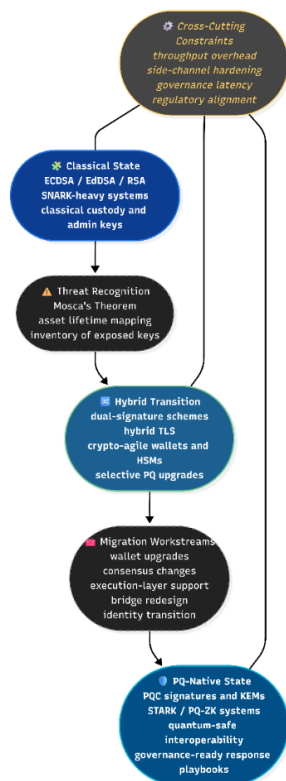


Figure 2. Conceptual migration pathway from classical cryptographic dependence to hybrid transition architectures and eventually PQ-native blockchain systems, constrained by performance, governance, and regulatory factors.

Table 10. Multi-chain quantum readiness (April 2026)

Chain	PQC Initiative	Readiness	Key Challenge
QRL	PQC since genesis (2018); QRVM [71, 72]	Production	Adoption
Algorand	Falcon mainnet tx Nov 2025 [85]	Advanced	Signature size
Ethereum	EIP-8141; PQ research team [65, 66, 95]	Planning	BLS replacement
Bitcoin	BIP 360 assigned Feb 2026; no Core impl. [96]	Early	Governance (7–10 years)
XRPL	ML-DSA on AlphaNet Dec 2025 [97]	Testing	Validator migration
Solana	Winternitz Vault [47]; testnet [60]	Testing	90% speed loss
Aptos	AIP-137: SLH-DSA proposed [76]	Proposal	Governance
Sui	Crypto-agility design [98]	Design	No concrete PQC
Canton	BOLTS pilot [78]	Pilot	Enterprise adoption
Stellar/BNB/LayerZero	None announced	None	No public roadmap

13. Governance, Regulation, and Migration

13.1 Governance Emergency Response

Grayscale [99] framed Bitcoin's quantum challenge as governance-bound rather than engineering-bound. BIP-360 was assigned and merged into the official BIP repository in February 2026, establishing the specification for Pay-to-Merkle-Root outputs; as of April 2026, no Bitcoin Core

implementation exists, and the activation timeline remains undetermined [96]. Emergency proposals include Dryja's commit-reveal scheme [100], QRAMP hard-fork migration, and Hourglass V2 rate-limiting [101]. Buterin's emergency plan [65] involves chain reversion and STARK-based seed-phrase recovery proofs. Lightning Labs CTO Osuntokun built a zk-STARK wallet rescue prototype [102]: proof generation in approximately 55 seconds, 1.7 MB proof size, verification under 2 seconds.

13.2 Regulatory Mandates

The U.S. leads with NSM-10 mandating federal PQC migration by 2035; NSA CNSA 2.0 [103] mandates compliance for new acquisitions by January 1, 2027. The EU targets 2030 for critical use cases [104]. BIS Paper No. 158 established a three-step framework [105]. The WEF noted 98% of central banks (CBDCs) exploring DLT face quantum vulnerability [106]. The SEC received PQFIF [107]. NIST CSWP 39 [108] provides the crypto-agility framework. Ethereum's account-abstraction path exemplifies gradual opt-in PQC adoption [66, 95].

13.3 Hybrid Migration Strategy

Campbell [7] provided the most detailed analysis of hybrid PQC migration for Bitcoin and Ethereum, demonstrating that the optimal strategy employs dual classical+PQC signatures during the transition period. NIST SP 800-227 [45] supports hybrid key exchange. The Bouncy Castle library [109] supports dual-key X.509 certificates combining ECDSA with ML-DSA. A critical timeline collision looms: quantum threat estimates (4–10 years) may arrive before blockchain communities can complete migration (10–15 years based on historical governance patterns [7]).

14. Limitations and Future Work

This study has several limitations. First, the rapidly evolving quantum hardware landscape means resource estimates may shift; our qubit projections rely on March 2026 data. Second, throughput degradation figures are based on limited testnet implementations [7], not mainnet production loads. Third, we lack access to proprietary quantum computing roadmaps. Fourth, the reference architecture has not been validated through laboratory implementation.

Post-quantum maximal extractable value (MEV) dynamics represent a significant open research gap. PQC signatures are 16–81× larger than ECDSA (Table 6), meaning block utilisation could drop substantially at equivalent gas limits. This would reshape sandwich attack economics (higher minimum profitable trade size at reduced block capacity), reduce per-block MEV opportunities, widen frontrunning windows as larger transactions propagate more slowly through mempools, and alter Proposer-Builder Separation supply chains. A quantitative analysis modelling break-even

costs for MEV strategies under PQC signature regimes is needed.

Additional future directions include: empirical measurement of PQC throughput on production networks; formal verification tools for quantum-vulnerable smart contract patterns; PQ-native BLS aggregate signature replacements; quantum risk insurance models; QRNG integration for provably fair PoS validator selection [73, 74]; and investigation of quantum blockchain paradigms (QKD-based consensus) as alternatives to classical PQC migration [25].

15. Conclusion

This paper presents a comprehensive layered reference architecture for quantum-resilient blockchain, addressing gaps identified through systematic comparison against eight peer surveys and five foundational JBBA publications. Three findings are particularly actionable. First, FN-DSA (Falcon) offers the optimal PQC signature profile for blockchain (16× ECDSA versus ML-DSA's 38×), but its draft status creates a temporal gap during which ML-DSA must serve as the workhorse despite heavier throughput penalties [7, 41, 29]. Second, cross-chain bridges, data availability layers, and Lightning Network payment channels represent critically neglected quantum attack surfaces [31, 94]. Third, the HNDL-signatures distinction [11] fundamentally reshapes urgency: blockchain's primary risk is real-time signature forgery, not retroactive decryption, meaning migration timelines for signatures can be more deliberate while privacy coin encryption must be upgraded immediately.

Governance speed – not engineering capability – is the binding constraint. Bitcoin's BIP-360 activation may require 7+ years [7, 96] while quantum threat windows compress to 4–10 years [4, 5, 28]. With qubit requirements collapsing by 20× and the 52–57% throughput penalty quantified [7], every delay adds permanently vulnerable data to immutable ledgers. The seven-layer architecture presented here provides a blueprint, but implementation demands coordinated action across standards bodies, blockchain governance communities, hardware vendors, and regulators.

Appendix A: STRIDE × Layer × Phase Threat Matrix (Summary)

The following table provides a condensed view of the full $6 \times 7 \times 3$ STRIDE threat matrix. Each cell indicates the primary quantum threat for that STRIDE category, architectural layer, and migration phase (Pre = pre-PQC transition; Hyb = hybrid; Post = post-PQC). Cells marked “—” indicate negligible additional quantum risk.

Table A1. STRIDE matrix (condensed) — Layer 1 Off-Chain through Layer 4 Execution

STRIDE	Layer	Pre-Transition	Hybrid	Post-Transition
Spoofing	L1 Off-Chain	Key theft via impl. flaws	Dual-key mgmt complexity	SCA on PQC keys
Spoofing	L3 Consensus	Validator impersonation	Classical key fallback risk	PQ-VRF manipulation
Tampering	L4 Execution	Smart contract exploits	Sig type confusion	PQC precompile bugs
Info Disclosure	L1 Off-Chain	HNDL on encrypted data	Migration metadata leak	—
Info Disclosure	L5 Application	Privacy coin deanonymization (HNDL)	Partial migration exposure	—
DoS	L2 Network	—	Bandwidth from dual sigs	PQC sig bloat (38–81×)
DoS	L3 Consensus	—	—	Attestation aggregation cost
Elev. Privilege	L5 Application	Admin key compromise	Hybrid admin key mgmt	SCA on admin PQC keys
Repudiation	L4 Execution	Signature forgery (CRQC)	Ambiguous sig validity	—

Competing Interests:

None declared.

Ethical approval:

Not applicable.

Author's contribution:

Sole author conceived, researched, and prepared the manuscript.

Funding:

None declared.

Acknowledgements and GenAI Disclosure:

The author used ChatGPT (OpenAI) for limited language editing, structural refinement, and formatting assistance during manuscript preparation. All source selection, interpretation, argumentation, verification, and final responsibility for the manuscript remain with the author.

References

- [1] R. E. Campbell Sr., "Evaluation of post-quantum distributed Ledger cryptography," *The Journal of The British Blockchain Association, JBBA*, vol. 2, no. 1, 2019. doi: 10.31585/jbba-2-1-(4)2019.
- [2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci., IEEE*, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.
- [3] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219. doi: 10.1145/237814.237866.
- [4] R. Babbush, A. Zalcman, C. Gidney, M. Broughton, T. Khattar, H. Neven, T. Bergamaschi, J. Drake, and D. Boneh, "Securing elliptic curve cryptocurrencies against quantum vulnerabilities: Resource estimates and mitigations," *arXiv:2603.28846 [quant-ph]*, Mar. 2026. [Online]. Available: <https://arxiv.org/abs/2603.28846>.
- [5] M. Mosca and M. Piani, "Quantum threat timeline report 2025," *Global Risk Institute / evolutionQ*, Mar. 2026. [Online]. Available: <https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025/>.
- [6] Cambridge Centre for Alternative Finance, "Why quantum matters now for blockchain," *Cambridge Judge Business School*, 2025. [Online]. Available: <https://www.jbs.cam.ac.uk/2025/why-quantum-matters-now-for-blockchain/>.
- [7] R. E. Campbell Sr., "Hybrid post-quantum signatures for bitcoin and ethereum: A protocol-level integration strategy," *JBBA*, vol. 9, no. 1, Dec. 2025. doi: 10.31585/jbba-9-1-(2)2026.
- [8] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Secur. Prin.*, vol. 16, no. 5, pp. 38–41, 2018. doi: 10.1109/MSP.2018.3761723.
- [9] J. Mascelli and J. Rodden, "Harvest now decrypt later: Examining PQC and data privacy risks for DLT networks," *Federal Reserve Board, FEDS* 2025-093, 2025. doi: 10.17016/FEDS.2025.093.
- [10] Palo Alto Networks, "Harvest Now, Decrypt Later (HNDL): The quantum-era threat," 2024. [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl>.
- [11] J. Thaler, "Quantum computing and blockchains: Matching urgency to actual threats," *a16z crypto*, Dec. 5, 2025. [Online]. Available: <https://a16zcrypto.com/posts/article/quantum-computing-misconceptions-realities-blockchains-planning-migrations/>.
- [12] M. Allende et al., "Quantum-resistance in blockchain networks," *Sci. Rep.*, vol. 13, art. 5664, Apr. 2023. doi: 10.1038/s41598-023-32701-6.
- [13] Y. Baseri, A. Hafid, Y. Shahsavari, D. Makrakis, and H. Khodaiemehr, "Blockchain security risk assessment in quantum era, migration strategies and proactive defense," *IEEE Commun. Surv. Tutor.*, 2025. doi: 10.1109/COMST.2025.3621113.

- [14] R. E. Campbell Sr., "The need for cyber resilient enterprise distributed Ledger risk management framework," *The Journal of The British Blockchain Association JBBA*, vol. 3, no. 1, Mar. 2020. doi: 10.31585/jbba-3-1-(5)2020.
- [15] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, "Post-quantum cryptography and quantum-safe security: A comprehensive survey," arXiv:2510.10436, 2025. [Online]. Available: <https://arxiv.org/abs/2510.10436>.
- [16] R. E. Campbell Sr., "Transitioning to a hyperledger fabric quantum-resistant classical hybrid public key infrastructure," *The Journal of The British Blockchain Association, JBBA*, Jul. 2019. doi: 10.31585/jbba-2-2-(4)2019.
- [17] H. Taherdoost, "A comprehensive review of quantum-resistant architectures for blockchain security," *MDPI Sci*, vol. 8, no. 2, art. 47, Feb. 2026. doi: 10.3390/sci8020047.
- [18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, 2009. doi: 10.1145/1568318.1568324.
- [19] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," EUROCRYPT 2010. doi: 10.1007/978-3-642-13190-5_1.
- [20] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Des. Codes Cryptogr.*, vol. 75, pp. 565–599, 2015. doi: 10.1007/s10623-014-9938-4.
- [21] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," IACR ePrint 2018/046, 2018. [Online]. Available: <https://eprint.iacr.org/2018/046>.
- [22] G. Chalkias et al., "Blockchained post-quantum signatures," IACR ePrint 2018/658; IEEE Blockchain 2018. [Online]. Available: <https://eprint.iacr.org/2018/658>.
- [23] S. Mallick et al., "Quantum disruption: An SoK of how post-quantum attackers reshape blockchain security and performance," arXiv:2512.13333 [cs.CR], Dec. 2025. [Online]. Available: <https://arxiv.org/abs/2512.13333>.
- [24] A. Wicaksana, "A survey on quantum-safe blockchain security infrastructure," *Comput. Sci. Rev.*, vol. 57, art. 100752, Elsevier, 2025. doi: 10.1016/j.cosrev.2025.100752.
- [25] Z. Yang et al., "A survey and comparison of post-quantum and quantum blockchains," *IEEE Commun. Surv. Tutor.*, vol. 26, pp. 967–1002, 2024. doi: 10.1109/COMST.2023.3325761.
- [26] R. Buser et al., "A survey on exotic signatures for post-quantum blockchain: Challenges and research directions," *ACM Comput. Surv.*, vol. 55, no. 12, art. 262, 2023. doi: 10.1145/3572771.
- [27] H. Khodaiemehr et al., "Navigating the quantum computing threat landscape for blockchains: A comprehensive survey," *Comput. Sci. Rev.*, Elsevier, 2025. doi: 10.1016/j.cosrev.2025.100846.
- [28] C. Chevnigard, P.-A. Fouque, and A. Schrottenloher, "Reducing the number of qubits in quantum discrete logarithms on elliptic curves," EUROCRYPT 2026, IACR ePrint 2026/280. [Online]. Available: <https://eprint.iacr.org/2026/280>.
- [29] A. G. Schemitt, H. F. da Silva, R. C. Lunardi, C. V. Neu, A. F. Zorzo, and S. S. Kanhere, "Assessing the impact of post-quantum digital signature algorithms on blockchains," arXiv:2510.09271, Oct. 2025. [Online]. Available: <https://arxiv.org/abs/2510.09271>.
- [30] N. R. Reddy et al., "Quantum secured blockchain framework for enhancing post quantum data security (QuantumShield-BC)," *Sci. Rep.*, vol. 15, art. 31048, 2025. doi: 10.1038/s41598-025-16315-8.
- [31] J. V. B. Da Silva, A. Gupta, M. Singh, and I. Singh, "QLink: Quantum-safe bridge architecture for blockchain interoperability," arXiv:2512.18488, Dec. 2025. [Online]. Available: <https://arxiv.org/abs/2512.18488>.
- [32] Cloud Security Alliance, "Standards for quantum-safe security and the financial industry," Sep. 2023. [Online]. Available: <https://cloudsecurityalliance.org/blog/2023/09/20/standards-for-quantum-safe-security-and-the-financial-industry>.
- [33] NIST, "Post-quantum cryptography FIPS approved," CSRC, Aug. 2024. [Online]. Available: <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>.
- [34] B. Yokubov and L. Gan, "A performance comparison of post-quantum algorithms in blockchain," *The Journal of The British Blockchain Association, JBBA*, vol. 6, no. 1, Sep. 2022. doi: 10.31585/jbba-6-1-(1)2023.
- [35] M. Webber, V. Elfving, S. Weidt, and W. K. Hensinger, "The impact of hardware specifications on reaching quantum advantage in the fault-tolerant regime," *AVS Quantum Sci.*, vol. 4, no. 1, art. 013801, 2022. doi: 10.1116/5.0073075.
- [36] D. Litinski, "How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates," arXiv:2306.08585 [quant-ph], 2023.
- [37] NIST, "FIPS 203: Module-lattice-based Key-Encapsulation Mechanism Standard (ML-KEM)," Aug. 2024. doi: 10.6028/NIST.FIPS.203.
- [38] R. Chhetri, "Benchmarking NIST-Standardised ML-KEM and ML-DSA on ARM Cortex-M0+: Performance, memory, and energy on the RP2040," arXiv:2603.19340, Mar. 2026. [Online]. Available:

- <https://arxiv.org/abs/2603.19340>.
- [39] NIST, “FIPS 204: Module-Lattice-based Digital Signature Standard (ML-DSA),” Aug. 2024. doi: 10.6028/NIST.FIPS.204.
- [40] NIST, “FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA),” Aug. 2024. doi: 10.6028/NIST.FIPS.205.
- [41] W. Buchanan, “Get ready for FN-DSA: Slower than dilithium but smaller keys/Ciphertext,” Medium, 2024. [Online]. Available: <https://billatnapier.medium.com/get-ready-for-fn-dsa-slower-than-dilithium-but-smaller-keys-ciphertext-924b18ece7b1>.
- [42] E. Karabulut and A. Aysu, “FALCON down: Breaking FALCON post-quantum signature scheme through side-channel attacks,” DAC 2021. doi: 10.1109/DAC18074.2021.9586131.
- [43] C. Guerreau et al., “Improved power analysis attacks on FALCON,” IACR ePrint 2023/224, 2023. [Online]. Available: <https://eprint.iacr.org/2023/224>.
- [44] NIST, “HQC announced as a 4th round selection,” CSRC, Mar. 2025. [Online]. Available: <https://csrc.nist.gov/news/2025/hqc-announced-as-a-4th-round-selection>.
- [45] NIST, “SP 800-227: Recommendations for key-encapsulation mechanisms,” Sep. 2025. doi: 10.6028/NIST.SP.800-227.
- [46] NIST, “SP 800-208: Recommendation for stateful hash-based signature schemes,” Oct. 2020. doi: 10.6028/NIST.SP.800-208.
- [47] Solana Winternitz Vault, D. Little (Zeus Network), Jan. 2025. [Online]. Available: <https://getblock.io/blog/what-is-solana-winternitz-vault-full-guide/>.
- [48] C. Bienstock, L. de Castro, D. Escudero, A. Polychroniadou, and Y. Takahashi, “Quorus: Efficient, scalable threshold ML-DSA signatures from MPC,” IACR ePrint 2025/1163. [Online]. Available: <https://eprint.iacr.org/2025/1163>.
- [49] C. Boschini, D. Kaviani, R. W. F. Lai, G. Malavolta, A. Takahashi, and M. Tibouchi, “Ringtail: Practical two-round threshold signatures from learning with errors,” in Proc. IEEE S&P 2025, pp. 149–164. doi: 10.1109/SP61157.2025.00070.
- [50] J. Drake et al., “Hash-based multi-signatures for post-quantum Ethereum,” *IACR Commun. Cryptol.*, vol. 2, no. 1, Art. no. 13, 2025. doi: 10.62056/acy7qip10.
- [51] E. Ben-Sasson et al., “Fast Reed-Solomon interactive oracle proofs of proximity (FRI),” ICALP 2018. doi: 10.4230/LIPIcs.ICALP.2018.14.
- [52] Y. Ishai, H. Su, and D. Wu, “Shorter and faster post-quantum designated-verifier zkSNARKs from lattices,” ACM CCS 2021, IACR ePrint 2021/977. doi: 10.1145/3460120.3484572.
- [53] B. Chen and D. Boneh, “LatticeFold: A lattice-based folding scheme and its applications to succinct proof systems,” ASIACRYPT 2025, IACR ePrint 2024/257. [Online]. Available: <https://eprint.iacr.org/2024/257>.
- [54] B. Chen and D. Boneh, “LatticeFold+: Faster, simpler, shorter lattice-based folding,” CRYPTO 2025, IACR ePrint 2025/247. [Online]. Available: <https://eprint.iacr.org/2025/247>.
- [55] B. Chen, “Symphony: Scalable SNARKs in the random oracle model from lattice-based high-arity folding,” IACR ePrint 2025/1905. [Online]. Available: <https://eprint.iacr.org/2025/1905>.
- [56] S. Ravi, S. Chattopadhyay, J. D’Anvers, and A. Baksi, “Side-channel and fault-injection attacks over lattice-based PQ schemes: Survey and new results,” *ACM TECS*, vol. 23, no. 2, art. 35, 2024. doi: 10.1145/3603170.
- [57] R. Wang, K. Ngo, J. Gärtner, and E. Dubrova, “Single-trace side-channel attacks on CRYSTALS-Dilithium: Myth or reality?,” Cryptology ePrint Archive, Paper 2023/1931, 2023. [Online]. Available: <https://eprint.iacr.org/2023/1931>.
- [58] O. Olaluwe et al., “Machine learning and side-channel attacks on post-quantum cryptography,” IACR ePrint 2025/1754, 2025. [Online]. Available: <https://eprint.iacr.org/2025/1754>.
- [59] R. Qiao et al., “When NTT meets SIS: Efficient side-channel attacks on dilithium and kyber,” IACR ePrint 2023/1866, 2023. [Online]. Available: <https://eprint.iacr.org/2023/1866>.
- [60] CoinDesk, “Solana’s post-quantum push reveals harsh tradeoff: Security vs speed,” Apr. 2026. [Online]. Available: <https://www.coindesk.com/tech/2026/04/04>.
- [61] M. Allende López, D. López León, S. Cerón et al., “Quantum-resistance in blockchain networks,” Inter-American Development Bank / LACChain, Jun. 2021. doi: 10.18235/0003313.
- [62] Thales, “Luna HSM v7.9 delivers PQC readiness at scale,” Jun. 2025. [Online]. Available: <https://cpl.thalesgroup.com/blog/encryption/luna-hsm-pqc-quantum-safe-encryption>.
- [63] Entrust, “nShield HSMs PQC algorithms achieve CAVP validation,” Aug. 2025. [Online]. Available: <https://www.entrust.com/company/newsroom/entrust-nshield-hsms-achieve-validation-from-nist-cryptographic-algorithm-validation-program>.
- [64] ABI Research, “What does quantum-safe really mean for HSM vendors?,” 2025. [Online]. Available: <https://www.abiresearch.com/blog/quantum-security-for-hardware-security-modules-hsms>.
- [65] V. Buterin, “How to hard-fork to save most users’ funds

- in a quantum emergency,” Ethereum Research, Mar. 9, 2024. [Online]. Available: <https://ethresear.ch/t/how-to-hard-fork-to-save-most-users-funds-in-a-quantum-emergency/18901>.
- [66] Ethereum Foundation, “Post-quantum ethereum,” 2025. [Online]. Available: <https://pq.ethereum.org/>.
- [67] C4, “CryptoCurrency Security Standard (CCSS) v9.0,” Dec. 2024. [Online]. Available: <https://cryptoconsortium.org/standards-2/>.
- [68] IETF, “draft-ietf-tls-hybrid-design-16: Hybrid key exchange in TLS 1.3,” Sep. 2025. [Online]. Available: <https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/>.
- [69] Open Quantum Safe Project, “TLS integration,” 2025. [Online]. Available: <https://openquantumsafe.org/applications/tls.html>.
- [70] BIS, “Project leap: Quantum-resistant VPN tunnel,” 2025. [Online]. Available: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.
- [71] QRL Foundation, “QRL 2.0: Building the bridge to the next era,” 2026. [Online]. Available: <https://www.theqrl.org/blog/qrl-2.0-building-the-bridge-to-the-next-era/>.
- [72] QRL Foundation, “QRL launches post-quantum smart contract testnet,” Mar. 2026. [Online]. Available: <https://www.theqrl.org/press/qrl-launches-testnet-v2>.
- [73] M. Buser et al., “Post-quantum VRF from symmetric primitives in PoS Blockchain (X-VRF),” ESORICS 2022. doi: 10.1007/978-3-031-17140-6_2.
- [74] M. F. Esgin, V. Kuchta, A. Sakzad, R. Steinfeld, Z. Zhang, S. Sun, and S. Chu, “Practical post-quantum few-time verifiable random function with applications to algorand,” in Proc. FC 2021, LNCS 12675, pp. 560–578, Springer. doi: 10.1007/978-3-662-64331-0_29.
- [75] L. Grassi et al., “poqeth: Efficient post-quantum signature verification on ethereum,” 2024. [Online]. Available: <https://www.researchgate.net/publication/388268875>.
- [76] CryptoNews, “Aptos proposes quantum-resistant signatures (AIP-137),” 2025. [Online]. Available: <https://cryptonews.com/news/aptos-proposes-quantum-resistant-signatures-to-future-proof-blockchain-security/>.
- [77] A. I. Alutaibi, “Quantum-resilient blockchain for secure digital identity verification in DeFi,” *Computers, Materials & Continua (CMC)*, vol. 85, no. 1, pp. 875–903, 2025. doi: 10.32604/cmc.2025.067078.
- [78] Chainwire, “BOLTS launches quantum-resilience pilot on canton network,” Dec. 2025. [Online]. Available: <https://chainwire.org/2025/12/10/bolts-launches-quantum-resilience-pilot-on-canton-network>.
- [79] CryptoNews, “Circle unveils quantum-resistant roadmap for arc blockchain,” Apr. 2026. [Online]. Available: <https://cryptonews.com/news/circle-quantum-resistant-roadmap-arc-blockchain/>.
- [80] BTQ Technologies, “Future-proofing stablecoins: How BTQ’s QSSN secures digital money for the quantum era,” 2026. [Online]. Available: <https://www.btg.com>.
- [81] S. Kumar, R. Suresh, B. Kronfellner, A. Kaul (BCG), and D. Liu (ADDX), “Relevance of on-chain asset tokenization in ‘crypto winter,’” Boston Consulting Group and ADDX, Sep. 2022. [Online]. Available: <https://web-assets.bcg.com/1e/a2/5b5f2b7e42dfad2cb3113a291222/on-chain-asset-tokenization.pdf>.
- [82] F. Schardong, A. A. Giron, F. L. Müller, and R. Custódio, “Post-quantum electronic identity: Adapting OpenID connect and OAuth 2.0 to the post-quantum era,” in Proc. CANS 2022, LNCS 13641, pp. 371–390, Springer. doi: 10.1007/978-3-031-20974-1_20.
- [83] OpenID Foundation, “Post-quantum identity standards,” 2025. [Online]. Available: <https://openid.net/post-quantum-identity-standards/>.
- [84] CyberArk, “Machine identity security report 2025,” 2025. [Online]. Available: <https://www.cyberark.com/state-of-machine-identity-security-report/>.
- [85] Algorand, “Technical brief: Quantum-resistant transactions on Algorand with Falcon signatures,” Nov. 2025. [Online]. Available: <https://algorand.co/blog/technical-brief-quantum-resistant-transactions-on-algorand-with-falcon-signatures>.
- [86] J. A. J. Alsayaydeh, M. F. Yusof, N. A. Yahaya, V. Kovtun, and S. G. Herawan, “A novel framework for secure cryptocurrency transactions using quantum crypto guard (QCG-ST),” *PeerJ Comput. Sci.*, vol. 11, art. e3030, 2025. doi: 10.7717/peerj-cs.3030.
- [87] N. Hussain, S. Li, A. Hussain, Z. Ullah, and M. Jamjoom, “Quantum-aware secure blockchain intrusion detection system for industrial IoT networks,” *Sci. Rep.*, vol. 15, 2025. doi: 10.1038/s41598-025-31985-0.
- [88] A. S. Rajawat, S. B. Goyal, M. Kumar, and S. Kumar, “Quantum deep neural network based classification of attack vectors on the ethereum blockchain,” *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 11, no. 6, 2024. doi: 10.4108/eetsis.5572.
- [89] CISA, “Strategy for migrating to automated PQC discovery and inventory tools,” Sep. 2024. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/strategy-migrating-automated-post-quantum-cryptography-discovery-and-inventory-tools>.
- [90] IBM, “Streamlining PQC migrations with AWS and IBM consulting,” 2025. [Online]. Available: <https://www.ibm.com/new/product-blog/streamlining-post-quantum-cryptography-migrations-with-aws-and-ibm-consulting>.
- [91] D. Ghiurău, “Rethinking blockchain governance with AI: The VOPPA framework,” *MDPI Computers*, vol. 14, no. 10,

- art. 425, Oct. 2025. doi: 10.3390/computers14100425.
- [92] D. Commey and G. V. Crosby, "PQS-BFL: A post-quantum secure blockchain-based federated learning framework," *Expert Syst. Appl.*, vol. 312, art. 131449, May 2026. doi: 10.1016/j.eswa.2026.131449.
- [93] S. Alharbi, "QuantumTrust-FedChain: A blockchain-aware quantum-tuned federated learning system for cyber-resilient industrial IoT in 6G," *MDPI Future Internet*, vol. 17, no. 11, art. 493, 2025. doi: 10.3390/fi17110493.
- [94] U. Wertheimer, "Lightning network 'helplessly broken' against quantum computers," *CryptoNews*, Apr. 2026. [Online]. Available: <https://cryptonews.net/news/bitcoin/32664483/>.
- [95] *Crypto Times*, "Ethereum's quantum defense? Vitalik Buterin Backs EIP-8141 upgrade," Mar. 2026. [Online]. Available: <https://www.cryptotimes.io>.
- [96] *Bitcoin Magazine*, "Bitcoin advances toward quantum resistance with BIP 360," Feb. 2026. [Online]. Available: <https://bitcoinmagazine.com/news/bitcoin-advances-toward-quantum-resistance>.
- [97] 24/7 Wall St., "Is Ripple (XRP) quantum-safe? A top XRPL validator published a full audit," Apr. 2026. [Online]. Available: <https://247wallst.com/investing/2026/04/11/is-ripple-xrp-quantum-safe-a-top-xrpl-validator-just-published-a-full-audit/>.
- [98] Suipiens, "Sui blockchain gears up for the quantum future," 2025. [Online]. Available: <https://suiapiens.com/blog/sui-blockchain-gears-up-for-the-quantum-future/>.
- [99] *CoinDesk*, "Grayscale says bitcoin's quantum problem is governance, not engineering," Apr. 2026. [Online]. Available: <https://www.coindesk.com/tech/2026/04/07>.
- [100] T. Dryja, "Post-quantum commit / reveal Fawkescoin variant as a soft fork," *Bitcoin Dev. Mailing List*, May 28, 2025. [Online]. Available: <https://mailing-list.bitcoindevs.xyz/bitcoinddev/cc2f8908>
- [101] H. Beast et al., "Hourglass V2: BIP for quantum migration rate limiting," *GitHub*, 2026. [Online]. Available: <https://github.com/cryptoquick/bips/blob/hourglass-v2/bip-hourglass-v2.mediawiki>.
- [102] O. Osuntokun (Lightning Labs CTO), "Quantum-resistant wallet rescue prototype," *CoinDesk*, Apr. 2026. [Online]. Available: <https://www.coindesk.com/tech/2026/04/09>.
- [103] NSA, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)," 2022. [Online]. Available: <https://media.defense.gov/2022/Sep/07/2003071834>.
- [104] *Industrial Cyber*, "EU coordinated effort to switch critical infrastructure to quantum-resistant encryption by 2030," 2025. [Online]. Available: <https://industrialcyber.co/regulation-standards-and-compliance/eu-begins-coordinated-effort-for-member-states-to-switch-critical-infrastructure-to-quantum-resistant-encryption-by-2030/>.
- [105] *PostQuantum*, "Quantum-readiness roadmap: BIS calls finance to prepare," 2025. [Online]. Available: <https://postquantum.com/quantum-policy/bis-quantum-roadmap-banking/>.
- [106] WEF and Accenture, "Safeguarding CBDC systems in the post-quantum computing age," May 2024. [Online]. Available: <https://www.weforum.org/stories/2024/05/safeguarding-central-bank-digital-currency-systems-post-quantum-age/>.
- [107] SEC, "Post-Quantum Financial Infrastructure Framework (PQFIF)," Sep. 2025. [Online]. Available: <https://www.sec.gov/files/cft-written-input-daniel-bruno-corvelo-costa-090325.pdf>.
- [108] NIST, "Considerations for achieving crypto agility: Strategies and practices (CSWP 39)," Dec. 2025. doi: 10.6028/NIST.CSWP.39. [Online]. Available: <https://www.nist.gov/publications/considerations-achieving-crypto-agility-strategies-and-practices>.
- [109] *Bouncy Castle*, "A PQC Almanac," Sep. 2025. [Online]. Available: <https://downloads.bouncycastle.org/csharp/docs/PQC-Almanac.pdf>.