Toward Post-Quantum Safe Blockchains: Comparison of Consensus Families

Mehrab Hosain
Louisiana Tech University
Ruston, LA, USA
mho020@latech.edu

Matthew Ogbe
Louisiana Tech University
Ruston, LA, USA
mio001@latech.edu

Manki Min
Louisiana Tech University
Ruston, LA, USA
mankimin@latech.edu

***Abstract*—Quantum adversaries invalidate classical discrete-log–based digital signatures used on the consensus path, necessitating post-quantum cryptography (PQC). This survey reviews blockchain consensus through a post-quantum lens, restricting analysis to cryptographic elements that directly gate safety and finality. Using only the provided corpus, we map standardized post-quantum primitives to consensus-critical roles across Proof-of-Work, chain-based Proof-of-Stake, committee-based BFT, and DAG families. The dominant impact is on signatures and quorum certificates(QC): multi-kilobyte artifacts and immature aggregation and threshold support stress bandwidth and verification where many attestations are required. Hashing remains sound with larger digests (e.g., 512-bit), and leader and committee randomness is fragile due to immature PQ-VRFs.**

***Index Terms*—Post-quantum cryptography, Blockchain, Consensus protocols, Digital signatures**

I. Introduction

Consensus determines the safety, liveness, and performance of public blockchains. Contemporary protocols span Proof-of-Work (PoW), chain-based Proof-of-Stake (PoS) with finality gadgets, committee-based Byzantine Fault Tolerant (BFT), and Directed Acyclic Graph (DAG)-oriented designs [9]–[11]. Feasible quantum adversaries invalidate discrete-log–based signatures(Sig.) used on the consensus path and reduce hash security margins, thereby changing concrete requirements for proposing, attesting, finalizing, and verifying blocks. Prior surveys are largely pre-quantum or lack a standardized basis for comparing post-quantum (PQ) choices across families [7], [9]–[14]. This survey revisits mainstream consensus families through a PQ lens using only the provided corpus and confines attention to *consensus-critical* cryptographic components: digital signatures for validator authentication, proposals, votes, and QC; hashing for block linking and Merkle and accumulator proofs; and verifiable randomness for leader and committee selection.

We ask how PQ substitutions (signatures, randomness, hashes) alter consensus guarantees and operations, and how concrete PQ parameters (key/signature sizes, verification costs) translate into throughput and time-to-finality across PoW, chain-PoS, BFT, and DAG. We compile stan-

TABLE I
Impact of Standardized PQ Primitives on Consensus–Critical Components

Component	PQC Primitive	Security Level	Artifacts Size	Impact on Consensus
Authentication (QC_SIG) [1]	ML-DSA (Dilithium)	Category 3	1,952B PK / 3,309B Sig.	High impact: ∼50× larger than ECDSA; fast verification, but thresholding bottleneck (∼1 s) [2], [3].
Authentication (QC_SIG) [4]	SLH-DSA (SPHINCS+)	Category 3	48B PK / 16,224B Sig.	Very high impact: tiny key, massive signatures; slower signing/verification [5]. Best for low-frequency, high-assurance uses.
State Integrity (Hashing) [6]	SHA-3 / SHA-2-512	Not Applicable	512-bit Digest	Low impact: structure unchanged; mitigate Grover by increasing digest length (e.g., 512-bit). [7]
Randomness (Leader Selection) [8]	PQC-VRF (e.g., X-VRF)	Not Applicable	Not Applicable	High risk / immature: uniqueness issues [8]; prefer commit–reveal or beacon or VDF for now.

dardized signature parameters (NIST Federal Information Processing Standards(FIPS) 204 ML-DSA/Dilithium; FIPS 205 SLH-DSA/SPHINCS+) and empirical performance data [1], [2], [4], [5]; for hashing we record the effect of quantum search and the mitigation by increasing digest length without changing proof structures [6], [7], [13], [15]; for randomness we summarize the state of Post-quantum Verifiable Random Function (PQ-VRFs) and documented vulnerabilities (e.g., uniqueness breaks) [6], [8], [13], [16].

The analysis explains why requirements differ by family: PoW keeps signatures off the block-generation fast path; chain-PoS typically collects few attestations per block; committee/BFT aggregates many signatures per decision (making signature size and verification cost dominant); and DAG designs rely on frequent attestations [2], [3], [5], [17]. All findings are synthesized strictly from the cited sources and remain limited to consensus-critical components.

II. Quantum Impact on Consensus–Critical Components

Classical ECDSA and EdDSA *break* against quantum adversaries, so validator authentication, proposals, votes, and quorum certificates (QCs) must migrate to standardized post-quantum signatures—ML–DSA (Dilithium) and SLH–DSA (SPHINCS+) [1], [4], [6], [13]. Hashing *weakens* in a quantifiable way: Grover reduces n-bit preimage security to $\approx n/2$, yet block linking and Merkle/accumulator proofs remain sound with longer digests (e.g., 512-bit) and no structural change [6], [7], [13], [15]. Randomness for leader and committee selection is *contested*: proposed PQ-VRFs are immature and have documented uniqueness/bias issues (e.g., X-VRF), motivating conservative commit–reveal or public randomness beacons/VDFs until robust PQ-VRFs are standardized [6], [8], [13], [16]. Sensitivity differs by family due to signatures-per-decision and attestation rates: committee/BFT protocols aggregate many signatures per round (high sensitivity), DAG designs issue frequent attestations (high sensitivity), chain-based PoS collects fewer attestations per block (moderate), and PoW keeps signatures off the block-generation fast path (low) [2], [3], [5], [9], [17].

In BFT protocols, QC *formation* dominates verification and bandwidth at PQ sizes, and immature aggregate/threshold support makes QC assembly the critical path [1], [3], [4]. In DAG variants, high attestation rates amplify verification and propagation costs [2], [17]. In chain-based PoS, overheads are smaller because fewer signatures are verified per block, but unbiased leader selection remains sensitive given PQ-VRF limitations [6], [8], [9], [13]. In PoW, only hash parameters need to be increased; transaction authentication still migrates to PQ signatures but lies off the block-creation fast path [7], [13], [15].

A. Signatures and Quorum Certificates

Validator authentication, proposals, votes, and QCs require signatures; classical ECDSA and EdDSA are unsafe under quantum attacks [6], [13]. FIPS 204 ML–DSA(Dilithium) specifies deterministic signing with kilobyte-scale public keys(PK) and signatures (Sig.); FIPS 205 SLH–DSA(SPHINCS+) provides a stateless hash-based option with minimal assumptions but much larger signatures [1], [4]. Empirical comparisons show lattice schemes (e.g., ML–DSA, Falcon family) verify faster than hash-based options, while SPHINCS+ trades extreme signature size for conservative security assumptions [2], [5]. In committee/BFT and DAG systems, verification and bandwidth dominate at PQ sizes, and the absence of mature aggregate/threshold signatures for standardized schemes makes QC formation the main bottleneck [3].

Many signatures per decision increase propagation and verification, raising time-to-finality or forcing smaller committee; these effects are reported across the cited analyses [2], [3], [5]. Where deployments rely on checkpoints, the lattice vs. hash-based signature choice intersects with operational cadence and artifact size [4], [16], [18]. Table II compares representative PQ signature families by key/signature sizes, verification cost, and aggregation readiness.

B. Hashing and Proof Structures

Hashes bind blocks and support Merkle/accumulator proofs. Grover weakens n-bit digests to $\approx n/2$ effective security, but

TABLE II
COMPARATIVE ANALYSIS OF POST-QUANTUM SIGNATURE SCHEMES

Scheme	Type	Security Level	PK / Sig. Size	Performance & Key Takeaway
ECDSA (secp256k1)	Elliptic Curve	Not Applicable	33B / ∼64B	Baseline (Fast); broken by Shor's algorithm [2], [5].
ML-DSA-65	Lattice-based	Category 3	1,952B / 3,09B	Fast; ∼50× larger than ECDSA; widely profiled [1], [2].
Falcon-512	Lattice-based	Category 1	897B / 666B	Very Fast; smaller artifacts but complex implementations [2].
SLH-DSA-192s	Hash-based	Category 3	48B / 16,224B	Slowest Sign; very large signatures; conservative assumptions [4].

structures remain sound; longer digests (e.g., SHA-2-512 or SHA-3) restore margin without redesign [6], [7], [13], [15]. In PoW, parameter adjustments preserve intended hardness under quantum search while leaving ledger correctness unchanged [13], [15].

C. Randomness and Validator Selection

PoS and BFT protocols often rely on verifiable randomness. PQ-VRFs remain immature; the X-VRF uniqueness break demonstrates bias risk [8]. Until robust PQ-VRFs exist, commit–reveal schemes or public randomness beacons and verifiable delay functions (VDFs) are conservative choices, with coordination and latency trade-offs [6], [9], [13], [17].

Across families, the dominant PQ overheads arise from signature size/verification and the immaturity of aggregate/threshold schemes for QC formation [1]–[4]. Hashing changes are parametric [7]. Randomness remains an open risk where PQ–VRFs are assumed [8].

III. CONSENSUS FAMILIES: IMPACT MAP

Post-quantum effects do not impact all consensus families uniformly. The specific mechanisms for Sybil resistance, block proposal, attestation, and finality determine which PQ components are critical. Using the taxonomy in Table III, we map which components each family depends on and identify where PQ substitutions induce the highest stress. Table IV consolidates the family-level view.

A. Proof-of-Work (PoW) Families

In PoW, consensus hinges on a hash-based computational puzzle [18]. Grover's algorithm weakens preimage security but the design remains functional by increasing digest size (e.g., 512-bit) and, if needed, retuning puzzle difficulty to preserve security margins without altering proof structures [7], [15]. Transaction authentication still uses signatures, yet signatures are not on the block-generation fast path and thus have limited effect on puzzle throughput [15].

B. Proof-of-Stake (PoS) Families

PoS protocols depend on signatures for proposals and attestations, making them sensitive to PQ signature size/verification costs (Section II-A).

1) Chain-based PoS: In chain-based PoS, a leader proposes a block and other validators attest. Classical signatures for proposals and attestations are replaced with post-quantum alternatives (e.g., ML–DSA), and some prototypes investigate WOTS variants for this path [15]. Secure, bias-resistant leader selection remains central; current PQ–VRFs are immature (see Section II-C), motivating caution in their use [8], [16].

TABLE III
CONSENSUS–CRITICAL COMPONENTS UNDER PQC

Component	Consensus Role	Quantum Impact	PQ Candidate(s) & Notes
Signatures & QCs [1]–[6], [13]	Proposals, votes, validator auth; quorum certificates (committee/BFT)	Shor breaks classical ECDSA and EdDSA ⇒ replace	ML–DSA (Dilithium); SLH–DSA (SPHINCS+). Lattice schemes verify faster; SPHINCS+ has larger sigs; PQ threshold/aggregate support is immature.
Hashing & Proofs [6], [13], [15]	Block linking; Merkle and accumulator proofs; PoW puzzles	Grover weakens n-bit security to $\approx n/2$	Prefer longer digests (e.g., 512-bit); proof logic unchanged; PoW parameters may need tuning.
Randomness/Selection [6], [8], [13]	Leader & committee eligibility (PoS/BFT)	PQ–VRFs are immature; uniqueness/bias issues	Prefer commit–reveal or beacon or VDF until robust PQ–VRFs exist.

TABLE IV
POST-QUANTUM IMPACT ACROSS CONSENSUS FAMILIES.

Family	Signatures / QCs (Impact)	Hashing / Proofs (Impact)	Randomness / Selection (Impact)
PoW	Low: signatures not on the fast path; tx auth can swap to ML–DSA/SLH–DSA [1], [4]	Medium: raise digest size; puzzle parameters may need tuning under Grover [6], [13], [15]	Low: typically no VRF at the consensus core [9], [17]
Chain-PoS	Medium: few sigs per block; feasible swap to ML–DSA/SLH–DSA; verification manageable [1], [2], [4], [5]	Low: longer digests; proof structure unchanged [6], [13]	Medium/High: avoid immature PQ–VRFs; prefer commit-reveal/beacon until robust PQ–VRFs exist [6], [8], [13]
Committee/ BFT	High: many sigs per round; QC aggregation stressed; PQ threshold/aggregate support immature [1], [3]	Low: longer digests only [6], [13]	Medium: VRF/beacon often used; be conservative given PQ–VRF limits [8], [13]
DAG-based	High: frequent attestations; verification or bandwidth dominate at PQ sizes [2], [17]	Low: longer digests only [6], [13]	Medium: where sampling exists, use conservative randomness [8], [13]

2) Committee-based PoS (BFT): BFT-style protocols (e.g., PBFT, HotStuff) finalize by collecting a super-majority (e.g., $2/3 + 1$) of committee signatures into a QC [9], [17]. Post-quantum pressure is strongest here: large signature artifacts inflate QC sizes (approximately 16 KB for SLH–DSA and 3.3 KB for ML–DSA) [1], [4], and threshold/aggregate mechanisms remain immature, with generic Multi-party computation (MPC) based thresholds reported to be on the order of seconds [3]. Mitigations under study include custom lattice-based aggregation prototypes [19] and the use of hash-based signatures in restricted roles [13].

C. DAG-based Families

DAG protocols produce frequent attestations and confirmations rather than a single linear chain. The high attestation rate amplifies signature verification and bandwidth costs at post-quantum sizes, making propagation a primary limiter [2], [17]. Where leader sampling or committee-like selection is employed, the immaturity of PQ–VRFs supports conservative randomness choices—such as commit–reveal schemes or public randomness beacons or VDFs—until robust PQ–VRFs are standardized [8], [13].

IV. COMPARISON & FINDINGS

Across surveyed designs, the dominant post-quantum effect on consensus stems from signature artifacts rather than hashing. Standardized ML–DSA signatures are multi-kilobyte (e.g., ML–DSA-65: 3,309 B) while SLH-DSA-SHA2-192s are $\sim$16,224 B [1], [4]. These sizes directly inflate QC payloads and verification: in a BFT protocol with $N = 3f + 1 = 100$ validators and $2f + 1 = 67$ votes per QC, classical ECDSA (≈ 64 B) yields about 4.3 kB of signatures per QC, whereas ML–DSA-65 yields $\approx$ 222 kB, over $50\times$ larger. As a result, cost is concentrated in committee/BFT protocols and frequent-attestation DAG designs; chain-based PoS aggregates fewer attestations per block (smaller relative penalty), and PoW keeps signatures off the fast path [2], [3], [5], [9], [15], [17]. Given immature aggregate/threshold support, QC formation remains the principal bottleneck in large-committee or high-attestation-rate protocols [3].

Hash-based components admit parametric mitigation rather than redesign: Grover's algorithm reduces n-bit preimage security to $n/2$, but block linking, Merkle trees, and accumulators still work; longer digests (e.g., 512-bit) and similar parameter tuning preserve PoW hardness [6], [7], [13], [15]. Randomness for leader/committee selection remains sensitive in PoS with BFT finality: proposed PQ-VRFs have unresolved issues (e.g., the X-VRF uniqueness break), so commit–reveal, public randomness beacons, or VDFs are conservative near-term choices [6], [8], [13]. In practice: increase digest length for hash-based components; budget explicitly for signature-driven QC size and verification; and avoid reliance on immature PQ-VRFs when specifying leader or committee selection.

Our synthesis identifies several critical open questions: (i) the viability of PQ aggregation and threshold at current costs; (ii) verifiable randomness under PQ and the maturity of PQ-VRFs; (iii) validator key management and rotation with larger

artifacts; and (iv) the role of hash-based signatures for low-frequency checkpointing versus per-block use.

V. Conclusion

A consensus-centric reading of the corpus indicates that post-quantum transition pressures concentrate on authentication and certificate formation: larger signature artifacts and the lack of mature aggregation and threshold schemes dominate bandwidth and verification on paths with many attestations, especially in committee-based BFT and high-rate DAG settings. Hash-based components retain structure with digest-size increases, while randomness for leader or committee selection remains fragile given immature PQ-VRFs. The comparative tables organize these effects across PoW, chain-PoS, BFT, and DAG under standardized parameters, enabling like-for-like interpretation of security and performance without proposing mechanisms. The open questions follow directly: practical PQ aggregation, robust verifiable randomness, and protocol configurations that accommodate artifact size without eroding safety or decentralization.

References

[1] *Module-lattice-based digital signature standard*, Aug. 2024. [Online]. Available: http://dx.doi.org/10.6028/NIST.FIPS.204

[2] L. Gan and B. Yokubov, "A performance comparison of post-quantum algorithms in blockchain," *The Journal of The British Blockchain Association*, vol. 6, pp. 1–10, 5 2023.

[3] K. Sedghighadikolaei and A. A. Yavuz, "A survey of threshold signatures: Nist standards, post-quantum cryptography, exotic techniques, and real-world applications," *ACM Computing Surveys*, Oct. 2025. [Online]. Available: http://dx.doi.org/10.1145/3772274

[4] *Stateless hash-based digital signature standard*, Aug. 2024. [Online]. Available: http://dx.doi.org/10.6028/NIST.FIPS.205

[5] P. Thanalakshmi, A. Rishikhesh, J. M. Marceline, G. P. Joshi, and W. Cho, "A quantum-resistant blockchain system: A comparative analysis," 9 2023.

[6] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys and Tutorials*, vol. 26, pp. 967–1002, 2024.

[7] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020.

[8] O. Bodaghi and R. Safavi-Naini, "Short paper: Breaking x-vrf, a post-quantum verifiable random function," in *Financial Cryptography and Data Security*, J. Clark and E. Shi, Eds. Cham: Springer Nature Switzerland, 2025, pp. 90–100.

[9] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, and R. Thomas, "A survey and taxonomy of consensus protocols for blockchains," *Journal of Systems Architecture*, vol. 127, p. 102503, 6 2022.

[10] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," 2 2022.

[11] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm," *Computer Networks*, vol. 214, p. 109118, 9 2022.

[12] F. Mogavero, I. Visconti, A. Vitaletti, and M. Zecchini, "The blockchain quadrilemma: When also computational effectiveness matters," *Proceedings - IEEE Symposium on Computers and Communications*, vol. 2021-September, 2021.

[13] J. M. Jose and P. V, "A survey on consensus algorithms in blockchain based on post quantum cryptosystems," in *2022 5th International Conference on Computational Intelligence and Networks (CINE)*, 2022, pp. 1–6.

[14] M. Edwards, A. Mashatan, and S. Ghose, "A review of quantum and hybrid quantum/classical blockchain protocols," *Quantum Information Processing*, vol. 19, no. 6, p. 184, 2020.

[15] A. Umar and D. Kumar, "Quantum-resistant security analysis of blockchain networks with pos consensus," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2024*. Institute of Electrical and Electronics Engineers Inc., 2024.

[16] J. Brown-Cohen, A. Narayanan, A. Psomas, and S. M. Weinberg, "Formal barriers to longest-chain proof-of-stake protocols?" in *ACM EC 2019 - Proceedings of the 2019 ACM Conference on Economics and Computation*. Association for Computing Machinery, Inc, 6 2019, pp. 459–473.

[17] X. Deng, K. Li, Z. Wang, J. Li, and Z. Luo, "A survey of blockchain consensus algorithms," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, Huaihua City, China, 2022, pp. 188–192.

[18] I. A. Álvarez, V. Gramlich, and J. Sedlmeir, "Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake," in *Proceedings of the ACM Symposium on Applied Computing*. Association for Computing Machinery, 4 2024, pp. 278–287.

[19] R. Saha, G. Kumar, T. Devgun, W. J. Buchanan, R. Thomas, M. Alazab, T. Hoon-Kim, and J. J. Rodrigues, "A blockchain framework in post-quantum decentralization," *IEEE Transactions on Services Computing*, vol. 16, pp. 1–12, 1 2023.