A DAG-Based Post-Quantum Ledger

Allan Edgard Silva Freitas[1]

[1]Instituto Federal da Bahia (IFBA), Salvador, Bahia, Brasil

allan@ifba.edu.br

Abstract. *Quantum computing threatens foundational cryptographic assumptions in today's distributed ledgers, while application demands outgrow the throughput and latency ceilings of single-chain blockchains. Directed acyclic graph (DAG) ledgers unlock parallelism but raise new questions about ordering, security, and light-client viability. This position paper argues for a* post-quantum (PQ) DAG ledger *that matches DAG concurrency with PQ-secure consensus and transactions, plus a privacy-preserving identity/reputation layer. We sketch the architecture, situate it against the literature, and enumerate some open challenges to be addressed for deployment at scale. A carefully engineered PQ DAG can provide credible security and performance in a quantum-enabled adversarial landscape .*

1. Introduction and Motivation

Quantum advances (e.g., Shor's and Grover's algorithms) imperil widely deployed public-key signatures and reduce the adequate security margin of hash-based search problems underpinning several consensus designs, motivating a transition to PQ cryptography (PQC) throughout ledger stacks [Gomes et al. 2023, Chen et al. 2021]. In parallel, classical linear blockchains face intrinsic bottlenecks from single-leader, single-chain ordering that hamper high-rate workloads and micro-transactions. DAG-structured ledgers relax these constraints, enabling concurrent writes and faster confirmation under the proper ordering and finality mechanisms—but they also introduce new analysis and engineering concerns [Wang et al. 2023, Pervez et al. 2018].

We claim that a *PQ-hardened DAG ledger*—with PQ-secure consensus randomness and transaction authentication, and a privacy-preserving identity/reputation substrate—offers the most promising path to sustain scalability, security, and accountability under quantum-capable adversaries [Wang et al. 2023, Pervez et al. 2018, Gomes et al. 2023, Chen et al. 2021, de Sousa et al. 2025].

2. Related Work

DAGs may decouple data dissemination from final ordering, choosing a proper design option between availability-first vs. consistency-first and dealing with the latency-throughput trade-offs alongside risks around reorgs, pruning, and light-client support [Wang et al. 2023]. Comparative analyses reinforce DAGs' suitability for high-throughput workloads[Pervez et al. 2018].

Systematic reviews of PQ blockchain consensus catalog how quantum algorithms impact PoW, VRFs, and signatures, and discuss countermeasures such as

PQ signatures, memory-hard or serial puzzles, and quantum-safe randomness beacons/VRFs [Gomes et al. 2023]. So, we may assemble an end-to-end PQ blockchain, including transaction layers with PQ signatures and consensus adjustments to blunt Grover-style advantages [Chen et al. 2021]. Also, we must deal with privacy: decentralized identifiers (DIDs) combined with zero-knowledge proofs (ZKPs) and privacy-enhancing computation can deliver verifiable yet private reputation, supporting Sybil resistance and accountability without revealing sensitive information [de Sousa et al. 2025].

3. Proposal Sketch: The Q-DAG Ledger

We propose a DAG-based block structure, where each block (or event) references multiple parents, thereby supporting parallel appends and high throughput. A partial order emerges from the DAG topology and timestamps [Wang et al. 2023, Pervez et al. 2018]. That allows to concile an availability-first DAG (rapid data inclusion) with a lightweight *finality gadget* (e.g., a PQ-secure committee vote or checkpoint rule) to resolve conflicts and bound reorg depth.

The consensus adopts puzzles that reduce the practical benefit of quadratic speedups, such as memory-aware/serializable puzzles with dynamic difficulty adjustment; calibrate parameters for equitable work distribution under heterogeneous hardware. Through compact proofs and batched quantum-safe verification, we limit the communication cost. Replacing ECDSA with PQ signatures, we allow for verification speed and compactness (e.g., appropriately tuned lattice- or hash-based schemes).

We propose to bind participants to DIDs, issuing verifiable credentials and proving eligibility (stake, service quality, or rate limits) in zero-knowledge, so consensus only learns the minimum necessary facts [de Sousa et al. 2025]. Also, maintaining reputation off-chain or in encrypted on-chain commitments and support ZK attestations (e.g., "reputation $\geq \theta$") helps to deter Sybils and collusion while limiting profiling, publish aggregate or blinded signals to guide admission and QoS.

Some threats arise in such that environment, our ZK reputation based approach in conjunction with PQ scheme strengthens the system. For instance, PQ signatures (with migration paths and possibly one-time/aggregate variants) harden transaction authenticity and committee votes; careful key-rotation and multi-scheme support enable staged upgrades [Gomes et al. 2023, Chen et al. 2021]. We assume a honest-majority assumption over PQ-secure identities/credentials to limit Sybils and short-range forks [Wang et al. 2023, de Sousa et al. 2025].

4. Final Remarks

DAGs supply the concurrency modern applications demand; PQC restores cryptographic resilience as quantum capabilities grow. The proposed *Q-DAG* blends an availability-first DAG with a PQ-secure consensus, a compact PQ transaction layer, and privacy-preserving identity/reputation. The literature suggests feasibility, but the path to production hinges on optimizing PQ overheads, standardizing DAG light-client proofs, and operationalizing PQ randomness and private reputation at scale [Wang et al. 2023, Pervez et al. 2018, Gomes et al. 2023, Chen et al. 2021, de Sousa et al. 2025]. We view Q-DAG as a pragmatic baseline for trustworthy, high-throughput ledgers in the quantum era.

References

Chen, J., Gan, W., Hu, M., and Chen, C.-M. (2021). On the construction of a post-quantum blockchain. In *2021 IEEE conference on dependable and secure computing (DSC)*, pages 1–8. IEEE.

de Sousa, A. M., Freitas, A. E. S., and Sampaio, L. N. (2025). Entre a confiança e o sigilo: Reputação descentralizada com garantia de privacidade por meio de identidades digitais auto-soberanas. [between trust and secrecy: Decentralized reputation with privacy assurance through self-sovereign digital identities]. In *Brazilian Symposium on Cybersecurity (SBSeg)*, pages 1066–1073. SBC.

Gomes, J., Khan, S., and Svetinovic, D. (2023). Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience. *IEEE Access*, 11:74088–74100.

Pervez, H., Muneeb, M., Irfan, M. U., and Haq, I. U. (2018). A comparative analysis of dag-based blockchain architectures. In *2018 12th International conference on open source systems and technologies (ICOSST)*, pages 27–34. IEEE.

Wang, Q., Yu, J., Chen, S., and Xiang, Y. (2023). Sok: Dag-based blockchain systems. *ACM Computing Surveys*, 55(12):1–38.