A Systematic Review of Quantum-Resilient Indexing Strategies in Blockchain-Based Data Storage

Asad Ali

Department of Computer Science, Virtual University of Pakistan, Email: MS230400088aal@vu.edu.pk

Received on 28 Oct 2025: Revised on 20, Oct 2025 Accepted: 2025

Abstract - Blockchain based databases are widely used in various applications including health records, supply chains and finance due to its tamper proof ledgers and decentralization. Data on blockchains is protected using cryptographic algorithms such as RSA and elliptic curve cryptography (ECC). As quantum computing growths, key cryptographic assumptions deserve evaluation. Public-key signature schemes are vulnerable to Shor's algorithm, whereas Grover's algorithm primarily reduces the effective security level of hash-based primitives without directly compromising them. As a result, researchers proposed number of post-quantum indexing mechanisms in blockchain based databases. A systematic literature review (SLR) on the application of post-quantum cryptography (PQC) to data indexing in blockchain databases has been provided in this article. Detailed examinations and analysis have been done on 24 papers out of the corpus of 158 identified papers. The various classical indexing structures like Merkle trees, Patricia trees, and AVL-Merkle trees have been studied. As well as post-quantum cryptographic methods such as hash-based (XMSS, SPHINCS+) and lattice-based (CRYSTALS-Dilithium, Kyber) schemes are identified in this literature. Extracted information tells that PQC schemes are quantum resistant but increase storage and verification costs. However, these challenges can be reduced through methods like aggregation, off-chain indexing, and hybrid encryption. The review highlights and discusses the need for better performance benchmarks and migration strategies toward post-quantum blockchain systems.

Index Terms: post-quantum cryptography, blockchain databases, Merkle tree, XMSS, SPHINCS+, lattice cryptography, authenticated indexing

1 INTRODUCTION

Blockchain databases provide decentralized, tamper-evident storage that is attractive for applications requiring high auditability; finance, supply chains, and health records among them. The authenticated data structures such as Merkle trees, Patricia tries, and Merkleized prefix tries and the public-key signatures used to authorize and verify state changes are fundamental to these systems trust model (Chan et al., 2024; H. Liu et al., 2021; Zhaofeng et al., 2020). However, developments in quantum computation threaten classical assumptions. Shor's algorithm targets integer and discrete-log-based schemes used for signatures and key exchange and Grover's algorithm reduces the effective security of hash functions by providing a square-root speedup to generic search attacks(Ahmadjee et al., 2022; Gidney & Ekerå, 2021; Grover, 1996). As a response, designers must consider the long-term security benefits of post-quantum cryptography (PQC) against the storage, computation, and protocol complexities that arise in real blockchain systems (Fernandez-Carames & Fraga-Lamas, 2020; Gao et al., 2024).

This article reviews existing research on quantum-resistant data indexing techniques, seeking to answer how classical and post-quantum approaches differ in terms of query efficiency, storage overhead, implementation complexity, and resilience to quantum attacks within blockchain-based databases. Particular attention is given to practical, case-based implementations such as Electronic Health Record (EHR) ledgers. The subsequent sections methodology, results & discussion, challenges, and conclusion synthesize observed techniques, empirical results, and open gaps to inform the case-based evaluation described in this thesis.

VOLUME 1, NO. 1, Issue 1 2025

2 RELATED WORKS

This section places our review in the context of existing research and explains the main technical concepts that form its foundation.

2.1 Authenticated Indexing in Blockchains

Verified data structures keep blockchains quick and reliable. For instance, merkle trees, Patricia Merkle tries used in Ethereum to quickly store and access data, and AVL-Merkle trees handling range based searches (Ahmadjee et al., 2022; H. Liu et al., 2021). These structures are used for convenient proofs of data correctness, and reasonable validation, though relying on hash functions and digital signatures for the final level of verification. As a result, their overall long-term protection could be put at risk (Fathalla & Azab, 2024).

2.2 Post-Quantum Cryptographic Primitives

There are variety of post-quantum methods, each with unique features that affect how data is indexed:

- Hash-based schemes (XMSS, SPHINCS+): These provide conservative security grounded purely in hash assumptions. XMSS is stateful and efficient per signature, while SPHINCS+ is stateless at the cost of larger signatures and higher computation. Hash-based schemes naturally pair with Merkleized constructions but present signature-size and state management challenges in multi-validator systems (Kathrine et al., 2023; Lopez-Valdivieso & Cumplido, 2024).
- Lattice-based schemes (Dilithium, Falcon, Kyber as KEMs): Lattice schemes provide relatively compact signatures and moderate verification cost and are widely considered practical PQC candidates for ledgers (Bagchi et al., 2025; Han et al., 2025). They become attractive when signature size and stateless operation are priorities, but their arithmetic may require optimization on constrained nodes (Chen, 2024; Gao et al., 2024).
- Others (code-based, multivariate): These are less frequently used in blockchain indexing due to very large keys or verification costs in many proposed parameterizations (Shen et al., 2019).

2.3 Hybrid & Architectural Strategies

Because direct, naive replacement of classical primitives can inflate block sizes and verification costs, researchers propose hybrid or architectural mitigations, including:

- Hybrid Signatures (Classical + PQC in Parallel): Hybrid digital signature schemes combine traditional cryptographic algorithms such as ECDSA or RSA with post-quantum cryptographic (PQC) algorithms like CRYSTALS-Dilithium or Falcon. By applying both signatures to the same transaction or block, these hybrid methods ensure forward security during the migration period between classical and quantum-safe systems (Bagchi et al., 2025). In essence, even if classical cryptography is later broken by quantum attacks, the PQC component still guarantees authenticity and integrity.
- Aggregation and Batching of Signatures or Inclusion Proofs: Post-quantum signatures such as lattice-based or hash-based schemes tend to produce longer keys and proofs. As a result, researchers have proposed aggregation and batching methods to lessen on-chain storage and computational costs. Signature aggregation combines many individual signatures into one smaller signature, making verification faster and more efficient. Likewise, batching processes several inclusion proofs at the same time instead of checking each separately. Both techniques reduce the extra computation and communication costs caused by post-quantum cryptography. By spreading these costs across multiple transactions, they improve system speed while keeping security intact (Goyal & Vaikuntanathan, 2022; Zhao, 2019). In blockchain contexts this can substantially mitigate the scalability drawback associated with PQC adoption.
- Off-chain Authenticated Indexes Anchored On-chain: In this approach the performance impact of PQC in blockchain systems is achieved by shifting large cryptographic objects and indexing data off the main chain. Off-chain authenticated indexes such as sparse Merkle trees, AVL-Merkle hybrids, or hash-based accumulators are periodically summarized and anchored on-chain through cryptographic commitments or Merkle roots. Keeping the full PQC data structures remain off-chain, the integrity and verifiability of the data are preserved through periodic commitments recorded on-chain (Fernandez-Carames & Fraga-Lamas, 2020). This design ensures that quantum-safe verification does not burden the consensus layer, allows scalability and

efficiency. Moreover, transparent auditability is still maintained.

Such type of information is persistent in recent literature and are the principal focus of the case-based evaluation within this thesis (Mu et al., 2024; Peng et al., 2022; Zhao, 2019).

3 RESEARCH METHODOLOGY

This SLR follows established guidelines adapted from evidence-based software engineering literature. The approach was implemented with reproducibility and transparency in mind.

3.1 Research Questions

The SLR addresses these research questions:

RQ1: Which PQC primitives and indexing structures have been proposed or evaluated in blockchain contexts with respect to indexing and proof structures?

RQ2: What are the measured or estimated impacts of PQC on query efficiency, storage overhead, and verification latency in blockchain indexes?

RQ3: What architectural strategies mitigate PQC overhead for indexing (e.g., aggregation, off-chain indexing, selective application)?

RQ4: Where are the empirical gaps and benchmarking needs to support deployment decisions?

3.2 Search Strategy and Sources

Searches were carried out across multiple academic databases and augmented by backward/forward snowballing:

- Databases: IEEE Xplore, ACM Digital Library, Scopus, Google Scholar (as primary sources), plus targeted searches of security and cryptography venues and recent preprints.
- Search terms**:** combinations of ("blockchain" OR "distributed ledger") AND ("post-quantum" OR "quantum-resistant" OR "quantum safe") AND ("index" OR "indexing" OR "Merkle" OR "commit*" OR "searchable" OR "query") AND ("lattice" OR "hash-based" OR "XMSS" OR "SPHINCS" OR "Dilithium" OR "Kyber").
- Date range**:** 2012–2025 to capture early blockchain indexing work and the full span of recent PQC developments.

The initial broad search and snowballing returned several hundred candidate records. Bibliographic metadata for identified records was maintained and saved in excel file. After removing duplicates and title/abstract screening, 169 unique records were retained for potential inclusion. Subsequently, full-text assessment produced a final set of 24 studies selected for in-depth analysis. These numbers reflect the staged screening described above and the corpus used for the Results & Discussion in Section IV.

3.3 Inclusion and Exclusion Criteria

Inclusion criteria:

- Peer-reviewed conference/journal papers, and significant technical preprints that address PQC in blockchain contexts or explicitly evaluate indexing/commitment structures under PQC assumptions.
- Works that report empirical measurements (benchmarks or simulations) or provide concrete algorithmic/design proposals for index/proof structures.
- English language publications (2012–2025).

Exclusion criteria:

- Papers that discuss PQC primitives purely from a theoretical cryptography perspective without application or implication for ledger indexing or proofs.
- Non-technical editorial pieces lacking experimental or design detail.
- Works limited to general blockchain performance improvements such as consensus algorithm adjustments lacking connections to indexing structures or cryptographic design, were omitted from the review.

3.4 Data Extraction and Synthesis

From each included paper we extracted: bibliographic details (authors, year, venue); cryptographic primitives discussed; indexing/data structure(s) considered; metrics reported (signature size, proof size, storage overhead, transaction per second, verification latency); experimental platform (simulator, testbed, mainnet traces); and proposed architectural mitigations. The extracted fields were tabulated, enabling thematic coding and quantitative summaries of reported metrics.

A standard PRISMA-style flow (records identified → screened → included) was maintained in the internal review documentation and is included as Figure 1.

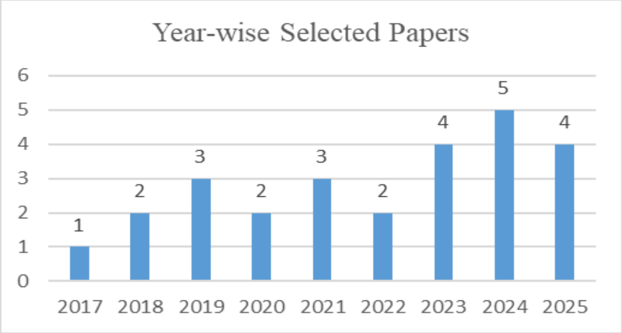

Figure 2. Year Wise data of selected papers

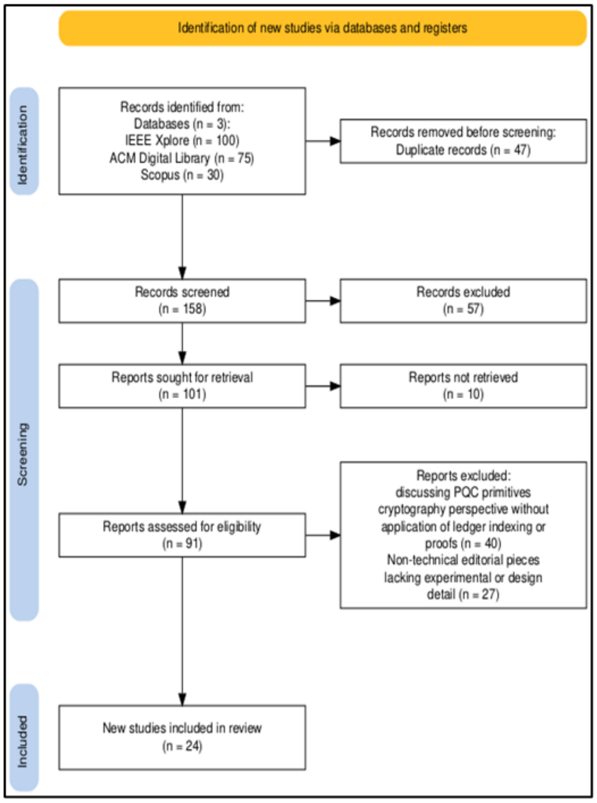
Identification of new studies via databases and registers
Identification
Records identified from:
Databases (n = 3):
IEEE Xplore (n = 100)
ACM Digital Library (n = 75)
Scopus (n = 30)
Records removed before screening:
Duplicate records (n = 47)
Screening
Records screened
(n = 158)
Records excluded
(n = 57)
Reports sought for retrieval
(n = 101)
Reports not retrieved
(n = 10)
Reports assessed for eligibility
(n = 91)
Reports excluded:
discussing PQC primitives
cryptography perspective without
application of ledger indexing or
proofs (n = 40)
Non-technical editorial pieces
lacking experimental or design
detail (n = 27)
Included
New studies included in review
(n = 24)

Figure 1. PRISMA flow diagram summarizing the article selection process for the systematic literature review.

The selected papers revealed that most of the work is done in last five years. The graph pertaining to year wise data of selected studies is shown as figure 2.

4 RESULTS AND DISCUSSION

This is the heart of the review. Findings are presented by theme: (A) classical indexing structures, discussing context and limitations under quantum threats, (B) hash-based PQC and Merkle-centric adaptations, (C) lattice-based and other PQC alternatives and their indexing implications, and (D) architectural mitigations and empirical evidence. Each subsection summarizes the relevant studies and points out specific performance measures and design insights where possible.

4.1 Classical Indexing Structures: properties and quantum limitations

4.1.1 Merkle trees and Merkleized tries

Binary Merkle trees and Merkle-based prefix tries are the basic data structures used in blockchain ledgers. They are popular because they make it easy to prove that a piece of data exists in the ledger using very small proofs. These structures also allow quick and simple updates as new data is added (Ahmadjee et al., 2022; H. Liu et al., 2021; M. Liu et al., 2021). Patricia Merkle tries used in state storage offer compact key-value representation and efficient path compression (Dhiman et al., 2022)). Balanced tree variants such as AVL-Merkle blends provide better worst-case bounds for range queries (Kushwah et al., 2022).

Quantum implications: The principal quantum concern is not the tree structure itself, but the cryptographic building blocks underpinning verification (hash functions and signature schemes). Grover's algorithm reduces the effective security of a hash function by roughly one bit of security per doubling of core operations (i.e., roughly a square-root speedup), which suggests that hash outputs and security parameters must be scaled conservatively (Grover, 1996). Therefore, while Merkle trees remain conceptually valid, their parameterization (hash size, domain separation) and integration with PQC signatures must be rethought for long-term resilience (Chen, 2024).

Practical trade-offs: Papers evaluating direct substitution of larger or quantum-hardened hashes find modest storage increases at the digest level but larger systemic impacts when signature sizes also grow: the per-node proof remains small, but the cost of storing and transmitting signatures, public keys, and proofs that reference large keys can dominate block sizes in practice (Alagic et al., 2024).

4.2 Patricia/Trie structures and state proofs

Patricia tries optimize key-value retrieval and are widely used in stateful chains (Dhiman et al., 2022). Their design is favorable for authenticated lookup, but their proof-size advantages can be counterbalanced if PQC increases the per-object signing metadata. Work in the literature shows that deploying PQC in systems with many small state updates (e.g., high-volume EHR writes) may disproportionately increase chain growth unless mitigations are applied (Alagic et al., 2024).

4.3 Hash-based PQC (XMSS, SPHINCS+) and Merkle-style integrations

4.3.1 XMSS and the stateful signature model

XMSS is a Merkle-tree-based signature scheme that aggregates many one-time signatures under a single root. Its major advantage is conservative security based solely on secure hashes; its major operational challenge is statefulness, signers must track leaf usage to prevent signature reuse (Kathrine et al., 2023; Ma et al., 2024). For single-authority append-only logs (audit trails), XMSS aligns naturally with Merkleized ledgers: the root can serve as a public verification anchor, and one-time keys correspond to per-transaction signatures.

Indexing implications. In systems where index nodes or validators are thin clients or where multiple nodes sign concurrently, XMSS state management introduces complexity: key synchronization becomes necessary, or signing must be centralized (which undermines decentralization). Storage impact is moderate (signature sizes are larger than ECDSA but vary by parameter set), and authors suggest that XMSS is best suited for append-only, controlled signing environments (Ma et al., 2024).

4.4 SPHINCS+ and stateless hash-based designs

SPHINCS+ eliminates the stateful requirement by building a stateless hypertree over hash-based one-time schemes. This makes it operationally attractive for distributed validator sets, but signature sizes are larger and signing/verification computation heavier than for most lattices (Fernandez-Carames & Fraga-Lamas, 2020; Lopez-Valdivieso & Cumplido, 2024).

Indexing implications. SPHINCS+ simplifies deployment in multi-party networks but raises per-transaction bandwidth and storage needs. Studies indicate that without aggregation or careful anchoring, SPHINCS+ signatures can substantially increase block size and propagation time in high-throughput systems (Alagic et al., 2024; Fernandez-Carames & Fraga-Lamas, 2020; M. Liu et al., 2021).

4.5 Aggregation and amortization for hash-based schemes

Several works propose aggregating many small proofs/signatures into batch commitments (Goyal & Vaikuntanathan, 2022). Aggregation amortizes signature overhead across many transactions, reducing per-transaction on-chain cost at the expense of latency and finality characteristics. Aggregation is particularly effective when workloads are tolerant to small batching delays (Chan et al., 2024). In the planned EHR case study, batching trade-offs must be evaluated carefully because healthcare access can be latency sensitive.

4.6 Lattice-based & other PQC families

4.6.1 Lattice schemes (Dilithium, Falcon, Kyber)

Lattice-based signatures and KEMs have found strong traction in PQC evaluations and proposals for blockchain use: they offer competitive signature sizes and verification speed relative to many hash-based stateless schemes (Bagchi et al., 2025; Gao et al., 2024; Han et al., 2025). Papers implementing lattice signatures in prototype ledgers report storage increases smaller than naive hash-based stateless replacements, and verification times that are acceptable when optimized or parallelized (Fernandez-Carames & Fraga-Lamas, 2020).

Indexing implications. Because lattice signatures are comparatively compact, they reduce the per-transaction bandwidth/registry inflation that would otherwise stress block propagation and index growth. Conversely, lattice arithmetic such as polynomial operations, modular reductions is heavier and may require optimized libraries or hardware support on resource-constrained nodes (Alagic et al., 2024; Bagchi et al., 2025).

4.6.2 Hybrid designs using lattices + DAG/parallel topologies

There are some studies which proposed coupling lattice based PQC with DAGs or parallel chains to merge high throughput with quantum resilience(Zhang et al., 2021) . These designs distribute indexing tasks to ease the load on the main chain and lower verification costs through parallel processing.

The literature here is more experimental than field-tested: prototypes show promise moderate storage cost and improved Transaction per second (TPS), but complexity of implementation remains high and the consensus/index interplay requires further study (Sedghighadikolaei & Yavuz, n.d.).

4.7 Architectural mitigations (off-chain indices, anchoring, and selective PQC)

4.7.1 Off-chain authenticated indexes anchored on-chain

A common design pattern is to store large PQC artifacts or full indexes off-chain in verifiable data stores, while committing compact digests or roots to the chain periodically (Mu et al., 2024). Off-chain indexes can provide low-latency query performance without inflating the on-chain index; the on-chain anchor preserves immutable verifiability for audits.

Trade-offs & risks. Off-chain approaches rely on availability and trustworthy retrieval or verifiable retrieval protocols. Papers recommend combining off-chain storage with content addressing and erasure coding to manage availability and support verifiability (Miyachi & Mackey, 2021). In healthcare settings, off-chain storage can preserve patient privacy and permit richer indexing such as full-text search, but it also creates additional operational responsibilities.

4.7.2 Selective PQC application and hybrid signatures

Applying PQC selectively to long-term artifacts such as block headers, checkpoints while allowing short-term transactions to use hybrid classical+PQC signatures during migration windows has been proposed as a pragmatic transition strategy (Bagchi et al., 2025). Hybrid signatures, both classical and PQC provide immediate post-quantum auditability while preserving existing client compatibility. The downside is increased storage and verification cost while both signature types are maintained.

4.7.3 Compression, deduplication, and delta encoding

Because a nontrivial portion of on-chain growth comes from repeated key and metadata patterns such as signatures from a small set of frequent signers, deduplication and compression techniques can mitigate PQC inflations. Literature shows that effective deduplication reduces on-chain index growth in practice, but its benefit depends heavily on workload patterns.

4.8 Empirical evidence (measured impacts and open gaps)

4.8.1 Storage overhead and block/transaction size

Multiple experimental and simulation studies report that replacing small classical signatures (e.g., 64–72 bytes for ECDSA/Ed25519) with PQC signatures can multiply per-transaction metadata by 3×–30×, depending on scheme and parameterization (Alagic et al., 2024; Chen, 2024; Ma et al., 2024; Sedghighadikolaei & Yavuz, n.d.). Aggregation and off-chain anchoring reduce effective per-transaction on-chain costs dramatically (often by 50–90%), but require new protocols to preserve per-transaction accountability.

4.8.2 Verification latency and throughput

Verification cost increases are observed in many implementations (Ma et al., 2024; Sedghighadikolaei & Yavuz, n.d.). However, careful software optimization, parallel verification across cores, and use of optimized PQC libraries reduce end-user impact to tolerable levels for many use cases. As for as latency is concern, lattice techniques are attractive because they typically show reduced verification overhead than stateless hash-based systems of comparable security (Sedghighadikolaei & Yavuz, n.d.).

4.8.3 Benchmarking inconsistency & reproducibility

Many studies use different test settings, batching methods, and workload models, making it hard to compare their results fairly. Researchers emphasize the need for standardized datasets and shared evaluation benchmarks to make future studies more consistent and comparable.

5 FUTURE DIRECTIONS

In the literature several open challenges are identified for evolution of quantum safe indexing in blockchain bases databases. The main difficulty is maintaining strong security without compromising efficiency and building cost effective systems. For instance, hash-based methods such as SPHINCS+ and XMSS offer durable security against quantum threats, but they also demand significant storage space and bandwidth. This makes them difficult to use efficiently in large-scale or high-speed databases unless improved through techniques like signature aggregation or off-chain storage (Lopez-Valdivieso & Cumplido, 2024; Ma et al., 2024; Zhao, 2019). Lattice-based algorithms like Dilithium and Falcon also emerge as a key priority; they present a more balanced alternative. Combining post-quantum resilience with smaller signatures and faster verification provides secured and efficient indexing operations (Han et al., 2025). Architectural optimization is another alternative to mitigate stated issues. Methods such as off-chain authenticated indexes and selective application of quantum-safe cryptography can reduce on-chain data growth as well as maintaining transparency and verifiability (Fernandez-Carames & Fraga-Lamas, 2020). Moreover, workload features play an important role in determining suitable strategies. Immutable audit records are better secured through stronger PQC signatures at the archival stage whereas, latency-sensitive applications can benefit from off-chain indexing for quicker access. Lastly, non-technical concerns such as key management, migration planning, and validator software upgrades remain critical for maintainable adoption. Proper management of XMSS key states, clear policies for hybrid system evolution, and well-defined governance procedures are all crucial to maintaining both technical reliability and operational readiness.

6 CONCLUSION

This review discusses the evolution of post quantum cryptographic indexing from database perspective in last 10 years. It closely examined 24 selected studies from a total of 158 identified papers. Quantum-safe cryptography (QSC) has shifted from being a theoretical concept to a crucial element of blockchain security. With the rapid development of quantum computing, traditional cryptographic foundations are being challenged. Shor's algorithm endangers public key signatures, while Grover's algorithm weakens hash-based mechanisms which highlights the need for stronger and more resilient cryptographic designs. Most of the researchers agree that post-quantum cryptography (PQC) will be needed for maintaining data integrity in the coming years. Lattice-based algorithms like CRYSTALS-Dilithium, Falcon, and Kyber provide a reasonable trade-off between efficiency and protection. Hash-based methods such as XMSS and SPHINCS+ provide stronger long-term security but at the cost of higher storage and bandwidth use.

The database indexing and query operations are affected by integration of PQC. Larger keys and longer signatures cause slow transaction processing and increased proof sizes. This can be a major issue in high-volume systems such as electronic health records and digital identity platforms. These systems demand both quick access and strong protection along with balance between performance and security. To overcome these performance costs, several architectural approaches have been proposed. Common approaches include batching and aggregation, which help reduce repetitive cryptographic operations. Another solution is to use off chain authenticated indexes that keep verification data locally while only storing small proofs on the blockchain. In addition, quantum-safe algorithm can be applied selectively, using them only where strong security is essential to balance safety and performance. Techniques like data compression and pruning are also used to prevent excessive blockchain growth. Together, these strategies indicate that well-planned designs can achieve both robustness and efficiency.

A number of challenges still remain. Research still lacks a cohesive framework for benchmarking PQC performance. Very few studies test classical indexing such as Merkle, Patricia, or AVL-Merkle trees and post-quantum indexing such as XMSS, lattice-based schemes under the same conditions. Real-world implementations are rare. Practical concerns such as key management, migration planning, and validator software upgrades are often ignored. Future work should therefore move toward applied, case-based evaluations that link cryptographic methods with database performance. The next chapters of this thesis build on this direction by introducing a framework that measures how post-quantum techniques influence indexing speed, scalability, and cost in real blockchain systems.

References

[1]. Ahmadjee, S., Mera-Gómez, C., Bahsoon, R., & Kazman, R. (2022). A Study on Blockchain Architecture Design Decisions and Their Security Attacks and Threats. *ACM* Transactions *on Software Engineering* and *Methodology*, *31*(2), 1–45. https://doi.org/10.1145/3502740

[2]. Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2024). *Status report on the first round of the additional* digital *signature schemes for the NIST post-quantum cryptography standardization process* (No. NIST IR 8528; p. NIST IR 8528). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8528

[3]. Bagchi, P., Bera, B., Das, A. K., & Sikdar, B. (2025). Quantum Safe Lattice-Based Single Round Online Collaborative Multi-Signature Scheme for Blockchain-Enabled IoT Applications. *ACM Transactions on Sensor Networks*, *21*(2), 1–33. https://doi.org/10.1145/3715696

[4]. Chan, K. Y., Chen, L., Tian, Y., & Yuen, T. H. (2024). Reconstructing Chameleon Hash: Full Security and the Multi-Party Setting. In *Proceedings of the 19th ACM Asia Conference on* Computer *and*

Communications Security (pp. 1066–1081). https://doi.org/10.1145/3634737.3656291

[5]. Chen, A. C. H. (2024). *The Security Performance Analysis of Blockchain System Based on Post-Quantum Cryptography—A Case Study of* Cryptocurrency *Exchanges*. https://doi.org/10.1142/S2196888825500204

[6]. Dhiman, P., Henge, S. K., Singh, S., Kaur, A., Singh, P., & Hadabou, M. (2022). Blockchain Merkle-Tree Ethereum Approach in Enterprise Multitenant Cloud Environment. *Computers, Materials and Continua*, *74*, 3297–3313. https://doi.org/10.32604/cmc.2023.030558

[7]. Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10731676/

[8]. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, *8*, 21091–21116.

[9]. Gao, Y., Chen, X., & Shang, W. (2024). A Lattice-based Linkable Ring Signature Scheme for Blockchain Privacy Protection. *2024 IEEE/ACIS 27th International Conference on Software* Engineering*, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 76–80. https://doi.org/10.1109/SNPD61259.2024.10673921

[10]. Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

[11]. Goyal, R., & Vaikuntanathan, V. (2022). Locally Verifiable Signature and Key Aggregation. In Y. Dodis & T. Shrimpton (Eds.), *Advances in Cryptology – CRYPTO 2022* (pp. 761–791). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-15979-4_26

[12]. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the* Twenty-*Eighth Annual ACM Symposium on Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866

[13]. Han, L., Hu, G., Li, X., Xia, F., Wang, S., & You, L. (2025). A Novel Lattice-Based Blockchain Infrastructure and Its Application on Trusted Data Management. *IEEE Transactions on Network Science and Engineering*, *12*(4), 2524–2536. https://doi.org/10.1109/TNSE.2025.3550158

[14]. Kathrine, G. J. W., P, K., Johnraja, I., Kirubakaran, S., Salaja, S., & Arunkumar, K. (2023). Enhancing Smart Grid Security with XMSS-Based Blockchain Technology. *2023* International *Conference on Emerging* Research *in Computational Science (ICERCS)*, 1–6. https://doi.org/10.1109/ICERCS57948.2023.10433959

[15]. Kushwah, J. S., Gupta, D., Shrivastava, A., Ambily Pramitha, P., Abraham, J. T., & Lunagaria, M. (2022). Analysis and visualization of proxy caching using LRU, AVL tree and BST with supervised machine learning. *Materials Today: Proceedings*, *51*, 750–755. https://doi.org/10.1016/j.matpr.2021.06.224

[16]. Liu, H., Luo, X., Liu, H., & Xia, X. (2021). Merkle Tree: A Fundamental Component of Blockchains. *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, 556–561. https://doi.org/10.1109/EIECS53707.2021.9588047

[17]. Liu, M., Wang, H., & Yang, F. (2021). An Efficient Data Query Method of Blockchain Based on Index. *2021* 7th International Conference *on Computer and Communications (ICCC)*, 1539–1544. https://doi.org/10.1109/ICCC54389.2021.9674708

[18]. Lopez-Valdivieso, J., & Cumplido, R. (2024). Design and Implementation of Hardware-Software Architecture Based on Hashes for SPHINCS+. *ACM Transactions* on *Reconfigurable Technology and* Systems, *17*(4), 1–22. https://doi.org/10.1145/3653459

[19]. Ma, M., Ji, X., & Cai, J. (2024). A Configurable XMSS Post-Quantum Hardware Implementation with SM3 and SHA-256. *2024 4th International Conference on Communication Technology and* Information *Technology (ICCTIT)*, 220–225. https://doi.org/10.1109/ICCTIT64404.2024.10928459

[20]. Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for

healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, *58*(3), 102535. https://doi.org/10.1016/j.ipm.2021.102535

[21]. Mu, L., Lv, M., Wang, S., & Cao, H. (2024). A Hybrid Index-Based Block Construction and Retrieval Algorithm for Efficient Data Retrieval on Blockchain. *2024 4th International Conference on Computer Science and Blockchain (CCSB)*, 487–491. https://doi.org/10.1109/CCSB63463.2024.10735653

[22]. Peng, C., Xu, H., & Li, P. (2022). Redactable Blockchain Using Lattice-based Chameleon Hash Function. *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 94–98. https://doi.org/10.1109/ICBCTIS55569.2022.00032

[23]. Sedghighadikolaei, K., & Yavuz, A. A. (n.d.). A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications. *ACM* Computing *Surveys*, *0*(ja). https://doi.org/10.1145/3772274

[24]. Shen, R., Xiang, H., Zhang, X., Cai, B., & Xiang, T. (2019). Application and Implementation of Multivariate Public Key Cryptosystem in Blockchain (Short Paper). In X. Wang, H. Gao, M. Iqbal, & G. Min (Eds.), *Collaborative Computing: Networking,* Applications *and Worksharing* (pp. 419–428). Springer International Publishing. https://doi.org/10.1007/978-3-030-30146-0_29

[25]. Zhang, X., Li, R., Hou, W., & Zhao, H. (2021). V-Lattice: A Lightweight Blockchain Architecture Based on DAG-Lattice Structure for Vehicular Ad Hoc Networks. *Security and* Communication *Networks*, *2021*, 1–17. https://doi.org/10.1155/2021/9942632

[26]. Zhao, Y. (2019). Practical Aggregate Signature from General Elliptic Curves, and Applications to Blockchain. *Proceedings of the 2019 ACM Asia Conference on Computer and Communications* Security, 529–538. https://doi.org/10.1145/3321705.3329826

[27]. Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. (2020). Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet of Things Journal*, *7*(5), 4000–4015. https://doi.org/10.1109/JIOT.2019.2960526