Blockchain Frontier Technology (BFRONT)
Vol. 5, No. 2, 2026, pp. 207∼218
E-ISSN: 2808-0009 P-ISSN: 2808-0831, DOI:10.34306

Migration of Blockchain Systems to Quantum Resistant Security ECDSA vs NIST MLDSA

Santika Lya Diah Pramesti[1*], Yul Ifda Tanjung[2], Azwani Aulia[3], Muhammad Rafly Ramadhan[4], Ikyboy Van Versie[5]
[1]Faculty of Mathematics and Natural Science, Universitas Negeri Semarang, Indonesia
[2]Faculty of Mathematics and Natural Sciences, Medan State University, Indonesia
[3]Department of Accounting, Padjadjaran University, Indonesia
[3]Department of Accounting, Adiwangsa Jambi University, Indonesia
[4]Faculty of Science and Technology, University of Raharja, Indonesia
[5]Department of Business Digital, Eduaward Incorporation, United Kingdom
[1]santikalyadiahpramesti@students.unnes.ac.id, [2]yuly@unimed.ac.id, [3]azwaniaulia@gmail.com, [4]m.rafly@raharja.info
[5]vanrizkyid@eesp.io
***Corresponding Author**

Article Info

Article history:

Submission, 27-10-2025
Revised, 08-12-2025
Accepted, 08-01-2026

Keywords:

Post-Quantum
Blockchain
ML-DSA
Scalability
ECDSA

ABSTRACT

The advent of cryptographically relevant quantum computers poses an existential threat to the security foundations of contemporary blockchain networks, which predominantly rely on the ECDSA for transaction authorization and identity management. Shor's quantum algorithm can solve the underlying mathematical problems of ECDSA in polynomial time, rendering current ledgers vulnerable to catastrophic asset theft. **This study aims** to examine the implications of quantum computing on blockchain security by positioning ECDSA and ML-DSA as two generational digital signature standards within the evolving cryptographic landscape. **The analysis is conducted** through a standards-based comparative approach, focusing on the formal specifications and security objectives outlined in the U.S. NIST post-quantum cryptographic standard FIPS 204. **The findings** indicate that ECDSA and ML-DSA represent two critical generations of digital signature standards: ECDSA as the legacy cryptographic foundation for current blockchain ecosystems, and ML-DSA (formerly CRYSTALS-Dilithium) as the newly standardized, quantum-resistant successor mandated for future secure systems. **This transition** underscores the strategic importance of evaluating digital signature algorithms not only as cryptographic primitives but also as formal standards with far-reaching implications for public policy, regulatory compliance, and long-term protocol governance.

This is an open access article under the CC BY 4.0 license.

DOI: https://doi.org/10.34306/bfront.v5i2.944
This is an open-access article under the CC-BY license (https://creativecommons.org/licenses/by/4.0/
©Authors retain all copyrights

1. INTRODUCTION

Modern public blockchain protocols like Bitcoin and Ethereum rely on public-key cryptography, specifically the Elliptic Curve Digital Signature Algorithm (ECDSA), to secure asset ownership and authorize transactions [1, 2]. The integrity and immutability of these distributed ledgers are built on the computational difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which remains intractable for classical computers [3, 4]. This computational challenge serves as the foundation for their security.

However, the rise of quantum computing poses a significant existential threat [5]. A sufficiently powerful quantum computer running Shor's algorithm could efficiently solve the ECDLP, enabling an attacker to derive private keys from public keys and forge transactions [6]. This vulnerability is compounded by the Harvest Now Decrypt Later (HNDL) strategy, where adversaries can store public blockchain data today and decrypt it in the future when quantum computers become available [7, 8]. The retroactive nature of this threat makes it even more urgent for the digital asset ecosystem to transition to post-quantum cryptography [9, 10].

In response to this looming risk, the National Institute of Standards and Technology (NIST) has spearheaded a global initiative to standardize quantum-resistant cryptographic methods. This effort culminated in the selection of the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) as the primary digital signature standard for post-quantum cryptography [11, 12]. While essential for the future security of digital assets, this migration is not a simple algorithmic swap; it introduces significant changes to blockchain infrastructure. The shift from classical cryptographic methods to quantum-resistant ones results in dramatically larger keys and signatures, which in turn increases the storage and bandwidth requirements for blockchain networks [13]. This report aims to analyze these trade-offs, quantify their impact on blockchain scalability, and evaluate the architectural challenges and strategic solutions necessary to facilitate a secure and effective migration [14, 15].

Moreover, the transition to quantum-resistant cryptography aligns with broader global goals. It contributes to the United Nations' Sustainable Development Goal (SDGs) 9, which focuses on building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation. By enhancing the reliability and security of cryptographic systems, this transition helps ensure that the foundational technologies of modern digital services are prepared for the quantum era [16]. Additionally, the integration of quantum-resistant cryptography supports SDGs 16, which emphasizes the importance of peace, justice, and strong institutions. By bolstering the integrity, transparency, and long-term security of blockchain-based governance mechanisms, the adoption of post-quantum cryptography contributes to the strengthening of digital governance structures [17, 18]. From a national development perspective digital infrastructure readiness and economic resilience are essential for supporting large scale cryptographic transitions In Indonesia macroeconomic indicators published by Statistics Indonesia BPS 2023 provide an empirical basis for assessing the capacity of public and private sectors to absorb secure digital infrastructure transformation [19]

This study is particularly relevant to the IEEE community, as it examines the intersection of system-level engineering and managerial decision-making within blockchain networks [20, 21]. Through a comprehensive analysis of the post-quantum impacts on the Data, Network, and Consensus layers of blockchain, the study highlights how the adoption of ML-DSA will affect key blockchain parameters such as storage requirements, bandwidth consumption, hashing throughput, and decentralization risks [22, 23]. The managerial insights provided in this study further align with IEEE's emphasis on long-term technology governance and infrastructure resilience. The study offers structured guidance for organizations seeking to develop quantum-resilient migration strategies, thus contributing to the sustainable development of secure digital ecosystems. In addition, the governance frameworks proposed in this research support SDGs 17, which calls for partnerships to achieve the global goals. This underscores the importance of cross-sector collaboration in advancing secure and sustainable digital infrastructures that can withstand the challenges of the quantum era [24].

2. LITERATURE REVIEW

The impending threat of quantum computing has catalyzed a significant body of research focused on developing and integrating Post-Quantum Cryptography (PQC) into existing digital infrastructure [25]. The vulnerability of current blockchain systems stems from their reliance on classical cryptographic primitives like ECDSA,which are susceptible to attacks by quantum algorithms such as Shor's and Grover's [26, 27]. Shor's algorithm, in particular, can solve the discrete logarithm problem over elliptic curves in polynomial time, effectively breaking ECDSA's security foundation [28].

PQC has emerged as the primary defense, comprising a class of cryptographic algorithms believed to be secure against attacks from both classical and quantum computers [29]. These algorithms are typically categorized into families based on the underlying mathematical problems they leverage, including lattice-based, hash-based, code-based, and multivariate cryptography [30, 31]. To guide the global transition, the U.S. NIST initiated a multi-year standardization process in 2016. This effort culminated in the selection of several algorithms for standardization, with CRYSTALS-Dilithium (now ML-DSA) and CRYSTALS-Kyber (now ML-KEM) chosen as the primary standards for digital signatures and key encapsulation, respectively [32, 33].

Additionally, SPHINCS+ (now SLH-DSA) was selected as a hash-based signature alternative, and FALCON was identified for applications requiring smaller signatures [34].

The academic and research communities have begun to explore the practical implications of integrating these new standards into blockchain technology [35].Early studies and proof-of-concept implementations, such as PQFabric (a PQC-enabled version of Hyperledger Fabric), have provided initial insights into the performance and architectural challenges [36, 37]. A recurring theme in the literature is the significant trade-off between enhanced security and performance overhead. PQC algorithms, especially lattice-based schemes like ML-DSA, introduce substantially larger public keys and signatures compared to ECDSA [38]. This increase in data size has been identified as a major obstacle, leading to challenges such as a "hashing bottleneck" in consensus mechanisms and reduced transaction throughput due to larger block sizes [39, 40]. While PQC integration is recognized as a complex but necessary measure, much of the existing research has focused on theoretical aspects, with fewer studies addressing the practical, systemic impacts on public blockchain scalability and decentralization [41, 42]. Despite substantial progress in PQC research, no prior work systematically synthesizes cryptographic performance data into an architectural impact assessment spanning data growth, bandwidth demand, propagation latency, and decentralization risks [43]. This study fills that gap by providing the first integrated system-level model that links PQC signature size inflation to cross-layer blockchain performance and governance outcomes.

Despite the growing body of PQC research, a significant gap remains in the systematic evaluation of how post-quantum signatures affect blockchain architecture at scale specifically their implications on transaction size inflation, network propagation delays, state storage growth, hashing bottlenecks, and decentralization risks [44]. Existing studies often provide prototype-level experiments or cryptographic efficiency benchmarks but rarely examine how these impacts propagate across the Data, Network, and Consensus layers in real-world blockchain environments. This research directly addresses that gap by providing an integrated, system-level analysis of ML-DSA migration and quantifying its architectural consequences.

3. METHODOLOGY

This study employs a qualitative, comparative analysis methodology based on a systematic review of technical literature to evaluate the implications of migrating blockchain systems from ECDSA to the NIST-standardized ML-DSA. The research is designed to synthesize findings from authoritative sources to provide a comprehensive overview of the performance trade-offs and architectural challenges involved in this transition.

This study draws on official NIST PQC publications (FIPS 204), peer-reviewed works from IEEE Xplore and the ACM Digital Library, and selected 2023–2025 arXiv preprints providing benchmarks or comparisons of ECDSA and ML-DSA in blockchain settings. Only sources with transparent hardware details, aligned NIST security levels, and consistent algorithm versions were used [45]. All heterogeneous data was normalized into relative performance ratios. The study synthesizes external quantitative metrics key generation, signing/verification speed, and cryptographic sizes and contributes by integrating these benchmarks into a unified system-level evaluation rather than generating new measurements.

The analytical framework for this paper is centered on a direct comparison of the two algorithms across a set of key Performance Indicators (KPIs) critical to blockchain operation. These metrics include:

- Cryptographic Data Size: Public key size and signature size.
- Computational Efficiency: Time required for key generation, transaction signing, and signature verification.
- System-Level Impact: Resulting transaction size and the effect on total blockchain state storage (state bloat).

To formalize the analytical logic of this study, these KPIs are evaluated through a Cost Benefit Trade off Analysis Framework for Cryptographic Migration [46]. This framework conceptualizes ML-DSA adoption as a multidimensional trade-off model in which computational performance improvements represent measurable benefits, while the increases in signature size, public-key size, bandwidth load, and required storage constitute quantifiable costs. By structuring the evaluation as a systematic mapping between costs and benefits across the Data, Network, and Consensus layers, this study applies a formal decision-analytic model commonly

used in system-design and migration studies [47, 48]. This elevates the methodology beyond a KPI enumeration and positions it as a structured theoretical framework for assessing the architectural implications of PQC integration

To ensure methodological consistency, benchmark sources were filtered using strict criteria. Only studies using finalized NIST-standardized ML-DSA parameters (FIPS 204) and matching security levels (Level 3 or 5) were included. Benchmark papers were required to provide full hardware disclosure including CPU architecture, clock speed, and memory specifications with direct numerical comparisons limited to homogeneous architectures. Heterogeneous results were incorporated only as relative performance ratios [49, 50]. All raw metrics were normalized to highlight comparative behavior rather than absolute speed, ensuring that architectural conclusions such as effects on block validation latency or hashing load were not tied to a single hardware profile. These filtering and normalization steps enhance internal validity and maintain robustness across diverse benchmarking conditions.

The analysis extends beyond a simple comparison of metrics to a holistic and multidimensional evaluation of the systemic impact that these differences impose on the various layers of blockchain architecture including the data network consensus and application layers By synthesizing quantitative data derived from benchmarking studies with qualitative insights obtained from in depth architectural analyses this methodology seeks to construct a comprehensive clear and evidence based understanding of the technical challenges operational implications and strategic considerations associated with the post quantum transition

4. RESULT AND DISCUSSION

4.1. Quantitative Performance Benchmarking: Speed and Efficiency

Beyond raw execution speed, quantitative performance benchmarking also evaluates system efficiency in terms of resource utilization, including CPU load, memory consumption, and response time stability under varying workloads.

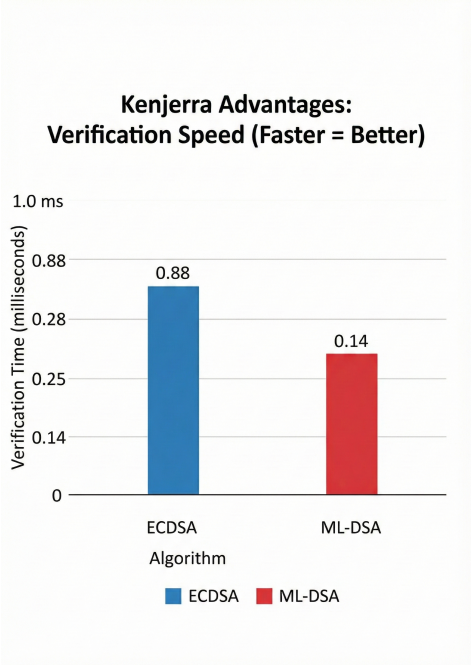


Figure 1. Verification speed comparison of ECDSA and ML-DSA

As shown in Figure 1, a foundational aspect of evaluating the feasibility of integrating ML-DSA into blockchain systems is the comparison of its computational profile against the incumbent ECDSA. The three critical cryptographic operations in a blockchain context are key generation (creating a new wallet), signing (authorizing a transaction), and verification (validating a transaction's authenticity). Benchmarking studies reveal a nuanced performance pattern in which ML-DSA is not only competitive but can, in certain crucial

aspects, outperform ECDSA. This relationship between computational efficiency and architectural implications forms the basis for interpreting the broader scalability challenges discussed in the subsequent analysis.

Several analyses have demonstrated that the efficiency of ML-DSA in key generation, signing, and verification can surpass that of ECDSA, particularly in signature verification. One study recorded a verification time of just 0.14 ms for ML-DSA at NIST Security Level 5, compared to 0.88 ms for ECDSA at a comparable security level, when tested on an ARM-based laptop. This advantage is highly significant for blockchain networks, where a single transaction is signed only once by the originator but must be verified independently by every validating node in the network. A faster verification time can therefore contribute to reduced block validation latency and improved overall network throughput.

It is important to clarify that the computational runtimes and cryptographic size values cited in this section including the 0.14 ms verification time and the 1,952-byte public key size are derived entirely from published benchmarking studies rather than original empirical measurements. Accordingly, the originality of this paper resides not in producing new performance data, but in synthesizing these heterogeneous empirical results into a unified architectural impact model that quantifies how PQC-induced data expansion affects transaction construction, network propagation, consensus hashing workload, state growth, and long-term decentralization. This multi-layered synthesis represents the novel contribution of the study.

This high performance can be attributed to ML-DSA's underlying design. It is based on the Fiat-Shamir with Aborts construction, a technique that enables compact and secure schemes based on lattice problems. Crucially, its design avoids the need for complex and computationally expensive Gaussian sampling, instead relying on uniform sampling and a centered binomial distribution. This not only contributes to its speed but also simplifies the process of creating secure, constant-time implementations a critical requirement for mitigating side-channel attacks where an attacker analyzes timing or power consumption to leak secret key information.

Previous benchmarking studies report that ML-DSA public keys typically reach 1,952 bytes and signatures approximately 3,309 bytes at NIST Security Level 3. These values form the basis of the comparative size entries in Table 1, ensuring that the quantitative analysis aligns with empirically established PQC parameters. To provide a clear and quantitative framing of the trade-offs involved, the following Table consolidates key metrics comparing ECDSA with ML-DSA. This data serves as the evidentiary foundation for the subsequent analysis of scalability and implementation challenges, illustrating the core conflict between computational efficiency and data footprint.

However, as summarized in Table 1, these computational advantages introduce a critical and unavoidable trade-off that shapes the rest of the analysis. While ML-DSA performs more efficiently at the cryptographic operation level, especially in signature verification, this performance gain comes at the cost of a dramatically larger public key and signature size. This size inflation represents the central scalability challenge of post-quantum migration and provides the analytical transition from micro-level efficiency to macro-level architectural impact.

The most immediate architectural consequence of this size inflation manifests at the transaction layer. Larger public keys and signatures directly increase the average transaction size, reducing the number of transactions that can be included within a fixed block size. In permissionless blockchains with strict block limits, such as Bitcoin or Ethereum, this effect translates into lower transaction throughput per block, potentially increasing confirmation times and transaction fees. Even in systems with adaptive block sizes, larger transactions impose higher bandwidth requirements on participating nodes, which may disadvantage nodes operating under limited network conditions.

Beyond transaction construction, increased cryptographic payloads exert significant pressure on network propagation mechanisms. Block dissemination latency is highly sensitive to block size, particularly in geographically distributed peer-to-peer networks. Larger blocks require more time to propagate across the network, increasing the probability of temporary chain forks and stale blocks. In proof-of-work systems, this can reduce effective mining efficiency, while in proof-of-stake systems it may impact validator synchronization and finality guarantees. Consequently, the adoption of ML-DSA necessitates careful consideration of gossip protocols, compression strategies, and relay optimizations.

The implications extend further into the consensus layer, where cryptographic data expansion influences hashing workloads and state transition costs. Although signature verification becomes faster with ML-DSA, the increased data volume must still be hashed, stored, and indexed as part of block validation and state updates. Over long operational horizons, this contributes to accelerated ledger growth, increasing storage

requirements for full nodes. As storage costs accumulate, the barrier to operating a fully validating node may rise, posing a subtle threat to decentralization by favoring resource rich participants.

From a systems engineering perspective, these pressures highlight the need for architectural mitigations rather than cryptographic optimization alone. Techniques such as signature aggregation, stateless client designs, and modular transaction formats become increasingly important in a post-quantum context. Layer-2 solutions, including rollups and off-chain execution frameworks, may also play a critical role in absorbing the data overhead introduced by PQC schemes, thereby preserving base-layer efficiency while maintaining post-quantum security guarantees.

Importantly, the trade-off between computational efficiency and data footprint reframes how performance should be evaluated in post-quantum blockchain systems. Traditional benchmarks that emphasize isolated cryptographic operations are insufficient to capture system-wide effects. Instead, performance must be assessed holistically, accounting for network latency, storage growth, synchronization overhead, and long-term sustainability. This shift in evaluation criteria underscores the necessity of architectural impact modeling as a complement to cryptographic benchmarking.

In this context, ML-DSA should not be viewed as a drop-in replacement for ECDSA, but as a catalyst for broader architectural evolution. Its adoption compels protocol designers to reconsider long-standing assumptions about block size, transaction structure, and node resource requirements. By framing post-quantum migration as a systems-level challenge rather than a purely cryptographic upgrade, this study provides a foundation for designing blockchain architectures that remain secure, scalable, and decentralized in a post-quantum era.

Table 1. Comparison of ECDSA and ML-DSA

Metric	**ECDSA (secp256k1)**	**ML-DSA (Level 3 / ML-DSA-65)**	**Impact Factor / Nuance**
Security Basis	Elliptic Curve Discrete Logarithm Problem (ECDLP)	Module Learning With Errors (MLWE)	Quantum-Resistant
Public Key Size	33 bytes	1,952 bytes	-59× Increase
Signature Size	-11 bytes (DER encoded)	3,309 bytes	-47× Increase
Typical Transaction Size	-250 bytes	-2.800 bytes	-11× Increase
Verification Speed	Slower at high security	Significantly faster	Performance Gain
Signing Speed	Generally fast	Competitive / slower	Context-dependent
Implementation Complexity	Mature, well-understood	Newer; requires careful constant-time coding	Higher Risk

As the Table 1 demonstrates, while ML-DSA offers a compelling performance advantage in verification, this comes at the cost of a dramatic increase in the size of its cryptographic outputs. This size discrepancy is not a minor detail; it is the central challenge of the post-quantum migration for blockchain systems and has profound implications for every layer of the network architecture.

4.2. On-Chain Footprint and Scalability Implications: The Challenge of ”State Bloat”

On-chain footprint growth has direct implications for long-term scalability, as every additional byte of persistent state must be stored, synchronized, and verified by all participating nodes. Unlike transient transaction data that can be pruned over time, on-chain state accumulates indefinitely, creating what is commonly referred to as state bloat. This condition increases the hardware requirements for full nodes, raising barriers to entry and potentially undermining decentralization as only well-resourced participants can afford to maintain complete replicas of the ledger.

From a performance perspective, state bloat exacerbates latency and throughput constraints. As the global state expands, read and write operations become more computationally expensive, affecting smart contract execution times and block validation speed. These overheads are particularly problematic for decentralized applications that rely on frequent state updates, such as DeFi protocols and on-chain governance systems, where scalability bottlenecks can translate directly into higher transaction fees and reduced user experience.

State bloat also introduces security and sustainability concerns. Larger state sizes increase the attack surface for denial-of-service vectors that exploit storage or execution inefficiencies. Moreover, the long-term energy and infrastructure costs associated with maintaining ever growing on-chain data challenge the environmental sustainability narratives of blockchain systems.

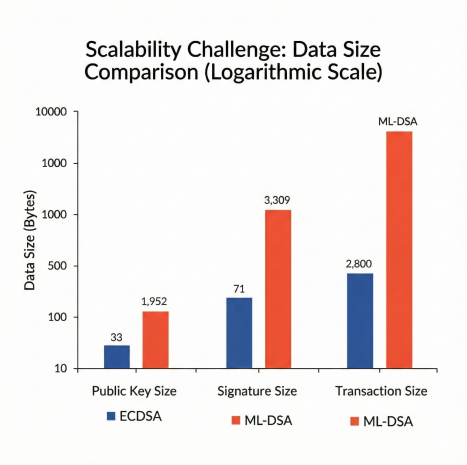


Figure 2. Comparative Data Size Analysis of ECDSA and ML-DSA

To illustrate the magnitude of the scalability impact, visualizes the comparative data sizes of ECDSA and ML-DSA across three core dimensions public keys, signatures, and transaction size using a logarithmic scale to highlight their exponential differences. The Figure 2 clearly shows the orders-of-magnitude increase in public key and signature sizes that occur when migrating from ECDSA to ML-DSA, a shift that introduces the critical challenge commonly referred to as "State Bloat". These substantial data expansions create cascading negative effects on network scalability, operational cost, and long-term decentralization. Consistent with the data summarized in Table 1, the visualization indicates that ML-DSA public keys grow by approximately a factor of 59, while signatures expand by roughly a factor of 47, underscoring the severity of the on-chain footprint problem.

The most immediate consequence is a drastic increase in the size of individual transactions. A typical ECDSA-based transaction might be around 250 bytes, but replacing the cryptographic components with their ML-DSA counterparts could inflate this to roughly 2,800 bytes an increase of more than 11 times. In blockchain systems with a fixed block size (like Bitcoin), this directly translates to a severe reduction in transaction throughput. Fewer transactions can fit into each block, meaning the network's capacity to process transactions per second is significantly diminished.

Beyond throughput, this data explosion leads to a rapid expansion of the blockchain's total size and active state. For account-based blockchains like Ethereum, the permanent storage required for each account's public key swells from 33 bytes to 1,952 bytes. This accelerates the growth of the ledger, which must be stored by every full node operator. The ever-increasing hardware requirements in terms of disk space, RAM for holding the active state, and network bandwidth raise the barrier to entry for individuals and smaller organizations to run their own nodes. A critical, if unintended, consequence of the PQC migration is that it may act as a powerful centralizing force. As the cost and technical difficulty of running a node increase, the network may become dominated by a smaller number of large, well-resourced entities, which could undermine the core value proposition of decentralization and censorship resistance.

Furthermore, the network propagation of larger blocks and transactions is inherently slower. Increased latency in block propagation across the global peer-to-peer network can lead to a higher rate of orphaned blocks and temporary network forks, which can in turn impact consensus stability and the finality of transactions.

Finally, the economic impact on users is direct and significant. As transaction fees are typically calculated based on data size, the larger footprint of PQC transactions is projected to lead to a 2-3x increase in average fees. This could render certain use cases, particularly microtransactions, economically unviable on the base layer and push more activity towards Layer-2 solutions.

4.3. Architectural and Security Implementation Challenges

The transition to ML-DSA introduces challenges that extend beyond performance metrics and data size, touching on the core architecture of the system and the nuances of secure implementation. While ML-DSA is designed to be secure against quantum cryptanalysis, its practical implementation must be hardened against a range of classical physical attacks. Lattice-based cryptography can be particularly susceptible to side-channel attacks, where an adversary analyzes non-functional characteristics like power consumption or precise execution timing to extract secret key information. It is therefore imperative that implementations are written in constant-time meaning their execution time is independent of secret values and are robust against fault injection attacks, where an attacker induces errors to glean information. The relative novelty of these primitives means that the developer community has less collective experience in avoiding these implementation pitfalls compared to the decades of work hardening ECDSA libraries.

This migration highlights the critical need for protocols to be designed with ”crypto-agility”. This architectural principle involves abstracting cryptographic functions so that algorithms can be updated or replaced without requiring a fundamental overhaul of the entire system. A crypto-agile design allows a network to gracefully transition from an old algorithm to a new one, and provides an essential defense against the possibility that a vulnerability might be discovered in ML-DSA or any other PQC standard in the future. Projects like PQFabric, a version of Hyperledger Fabric that allows for the live migration and selection of different signature schemes, serve as an important proof-of-concept for this approach.

The impact of this transition is felt across the entire blockchain technology stack, creating a complex, multi-layered engineering problem:

- Network Layer: Must be capable of handling significantly higher bandwidth requirements to propagate larger transactions and blocks without compromising performance.
- Data Layer: Faces immense pressure from increased storage demands, directly impacting the cost and feasibility of running a full node and archiving the chain history.
- Consensus Layer: While individual signature verification is fast, the cumulative effect of processing and hashing larger data chunks within a block can introduce new performance bottlenecks. Some implementations have reported a “hashing bottleneck,” where the overhead of processing larger data structures becomes a limiting factor.
- Application Layer: Smart contracts that perform on-chain cryptographic operations, such as verifying signatures within their logic, will experience dramatically increased gas costs due to the larger data sizes involved, potentially making such applications prohibitively expensive.

4.4. Strategic Pathways for a Quantum-Resistant Transition

Addressing the multifaceted challenges of PQC integration requires a strategic approach that combines cryptographic techniques with architectural innovation. A purely ”drop-in” replacement of ECDSA with ML-DSA is widely considered to be infeasible due to the severe scalability impacts. Instead, several pathways are being explored to facilitate a more manageable transition.

One of the most commonly discussed strategies is the use of hybrid cryptographic models In this approach a transaction is signed with both the legacy algorithm ECDSA and the new quantum resistant algorithm ML DSA This provides two key benefits

- Backward compatibility Ensures compatibility with existing wallets and infrastructure that have not yet been upgraded
- Hedge against vulnerabilities Acts as a safeguard against the possibility of an unforeseen vulnerability being discovered in the new PQC standard

If ML DSA were to be broken the ECDSA signature would still provide protection against classical attackers However this approach also introduces several drawbacks

- Data size problem Temporarily increases transaction size due to the inclusion of two signatures
- Complexity Adds additional complexity to protocol logic and key management

To directly combat the problem of on-chain data bloat, a promising architectural solution is the use of off-chain data storage. In this model, large cryptographic elements like full public keys and signatures are stored on a separate, decentralized storage network such as the InterPlanetary File System (IPFS). The blockchain itself would only store a compact cryptographic hash of this data.This could reduce the on-chain footprint of a transaction by orders of magnitude, preserving block space and keeping fees low. However, this approach introduces a new dependency on an external data availability layer, which must provide its own guarantees of persistence, retrievability, and security.

Perhaps the most formidable obstacle, however, is not technical but social and political. In a decentralized ecosystem, major protocol changes require broad community consensus. The PQC transition represents a unique challenge in this regard, as it can be framed as a ”defensive downgrade” a change that imposes immediate, tangible costs (higher fees, lower throughput) in exchange for protection against a future, abstract threat. Historical precedent in blockchain governance shows that even highly beneficial and non-controversial upgrades can take years of debate and coordination to implement. The timeline for achieving social consensus on a disruptive change like PQC migration may be dangerously misaligned with the accelerating progress in quantum computing. This ”governance lag” could become the most critical vulnerability of all, as the network may find itself unable to deploy a known solution before the threat becomes a reality.

5. MANAGERIAL IMPLICATIONS

The transition to post-quantum cryptography is not merely a technical upgrade but a profound strategic challenge that requires executive-level attention and proactive planning. With the rise of the HNDL threat model, organizations must recognize that sensitive data protected by current cryptographic systems is already at risk, making a passive “wait and see” stance untenable. Business leaders therefore need to initiate immediate strategic action, beginning with the development of a comprehensive PQC migration roadmap supported by a complete cryptographic inventory and risk-based prioritization framework.

A structured migration strategy must include identifying all public-key cryptographic components, evaluating their exposure to quantum threats, and categorizing systems based on data sensitivity and long-term asset value. This enables organizations to adopt a phased and risk-informed transition, focusing first on the most mission-critical systems. Managerially, this risk-based classification supports informed decision-making, efficient resource allocation, and accountability at the executive level. At the architectural level, building crypto-agility is essential. Designing systems with modular, easily replaceable cryptographic components ensures that organizations can transition smoothly to PQC while remaining adaptable to future cryptographic innovations or emerging vulnerabilities.

Furthermore, achieving quantum readiness requires substantial investments in R&D, infrastructure modernization, and workforce training. Executive leadership plays a crucial role in securing the budget, driving organizational commitment, and communicating strategic priorities to stakeholders, including boards, regulators, and customers. These managerial insights also point to broader implications for future research and policy development, such as the need for standardized quantum-readiness assessment frameworks, cross-sector coordination in PQC migration, and clear regulatory guidance on long-term cryptographic governance highlighting the relevance of this issue not only for individual organizations but for the overall digital ecosystem.

6. CONCLUSION

The analysis confirms that the quantum threat to ECDSA-based blockchains represents an existential risk requiring an urgent transition to quantum-resistant cryptography. By progressing from the identification of quantum vulnerabilities to the evaluation of standardized PQC solutions and their architectural consequences, this study provides a coherent foundation for future research in quantum-resilient blockchain governance. With NIST’s finalization of ML-DSA as the primary post-quantum signature algorithm, the path forward is technically clear: ML-DSA offers strong security and highly efficient verification performance, but at the cost of significantly larger public keys and signatures. This shift transforms blockchain systems from computation-bound to storage- and bandwidth-bound architectures.

The resulting data expansion has profound implications that go far beyond cryptographic replacement. Larger signatures create "State Bloat", reduce network scalability, and increase transaction fees, raising concerns about economic sustainability. Hardware demands for full nodes escalate, intensifying risks of network centralization and threatening the core decentralization ethos of blockchain ecosystems. Thus, the PQC transition is not a purely technical upgrade but a multifaceted architectural, economic, and political challenge. It forces a rethinking of scalability strategies and exposes the dangers of governance lag in decentralized systems, where collective decision-making may be slower than the pace of emerging threats.

Looking ahead, navigating this transition requires multi-dimensional research and policy coordination. High-priority efforts include developing more compact PQC signature schemes, improving aggregation or compression techniques for lattice-based cryptography, and designing Layer-2 architectures capable of absorbing PQC-induced data overhead. Economic analyses must determine the cost–benefit equilibrium of PQC adoption, assessing when increased storage, blockspace, and bandwidth costs outweigh gains in verification efficiency. By synthesizing benchmark results into a unified architectural model, this study contributes to an original system-level understanding of how PQC affects decentralization, consensus performance, network propagation, and node sustainability from an integrative perspective not previously addressed in the literature.

7. DECLARATIONS

7.1. About Authors

Santika Lya Diah Pramesti (SL) https://orcid.org/0000-0003-0042-9176

Yul Ifda Tanjung (YF) https://orcid.org/0000-0003-2324-5994

Azwani Aulia (AA) https://orcid.org/0000-0003-1333-9057

Muhammad Rafly Ramadhan (MR) https://orcid.org/0009-0000-9257-261X

Ikyboy Van Versie (IV) https://orcid.org/0009-0004-0232-6044

7.2. Author Contributions

Conceptualization: SL, YF, and AA; Methodology: MR; Software: IV; Validation: YF and AA; Formal Analysis: SL and MR; Investigation: IV; Resources: MR; Data Curation: SL; Original Draft Preparation: YF and AA; Writing Review and Editing: AA; Visualization: MR; All authors, SL, YF, AA, MR and IV, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] G. Wu, J. Zhou, and X. Fu, "Improved blockchain-based ecdsa batch verification scheme," *Frontiers in Blockchain*, vol. 8, p. 1495984, 2025.

[2] K. Balasubramanian, "Security of the secp256k1 ellptic curve used in the bitcoin blockchain," *Indian Journal of Cryptography and Network Security (IJCNS) Volume-4 Issue-1*, 2024.

[3] J. Ha, J. Lee, and J. Heo, "Resource analysis and modifications of quantum computing with noisy qubits for elliptic curve discrete logarithms," *Scientific reports*, vol. 14, no. 1, p. 3927, 2024.

[4] M. A. D. Yuda and S. Watini, "Implementation of blockchain technology as the latest solution to improve data security and integrity," *International Transactions on Education Technology*, vol. 2, no. 1, pp. 71–82, 2023.

[5] A. Wicaksana, "A survey on quantum-safe blockchain security infrastructure," *Computer Science Review*, vol. 57, p. 100752, 2025.
[6] M. Garn and A. Kan, "Quantum resource estimates for computing binary elliptic curve discrete logarithms," *arXiv preprint arXiv:2503.02984*, 2025.
[7] B. Rawat, N. Mehra, A. S. Bist, M. Yusup, and Y. P. A. Sanjaya, "Quantum computing and ai: Impacts & possibilities," *ADI Journal on Recent Innovation*, vol. 3, no. 2, pp. 202–207, 2022.
[8] R. Campbell, "Post-quantum security for bitcoin and ethereum: A comprehensive migration framework," *Preprints.org.Posted: August*, vol. 22, 2025.
[9] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: security dependency analysis and case studies," *IEEE Access*, vol. 12, pp. 23 427–23 450, 2024.
[10] F. Yusuf, R. Widayanti, S. R. Putri, and A. Wellington, "A comprehensive framework for enhancing blockchain security and privacy," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 171–182, 2025.
[11] K. A. Jackson, C. A. Miller, and D. Wang, "Evaluating the security of crystals-dilithium in the quantum random oracle model," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2024, pp. 418–446.
[12] D. Dziechciarz and M. Niemiec, "Efficiency analysis of nist-standardized post-quantum cryptographic algorithms for digital signatures in various environments," *Electronics*, vol. 14, no. 1, p. 70, 2024.
[13] R. Azhari and A. N. Salsabila, "Analyzing the impact of quantum computing on current encryption techniques," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 148–157, 2024.
[14] S. Holmes, "Impact of post-quantum signatures on blockchain and dlt system." in *DLT*, 2023.
[15] C. Monga, K. S. Raju, P. Arunkumar, A. S. Bist, G. K. Sharma, H. O. Alsaab, and B. Malakhil, "Secure techniques for channel encryption in wireless body area network without the certificate," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 2598465, 2022.
[16] R. Bhatia, "Finance as critical infrastructure: Embedding post-quantum cryptography in digital finance architectures," *Journal of Computer Science and Technology Studies*, vol. 7, no. 8, pp. 1184–1194, 2025.
[17] D. Commey and G. V. Crosby, "Pqs-bfl: A post-quantum secure blockchain-based federated learning framework," *arXiv preprint arXiv:2505.01866*, 2025.
[18] A. Bienstock, L. de Castro, D. Escudero, A. Polychroniadou, and A. Takahashi, "Efficient, scalable threshold ml-dsa signatures: An mpc approach," *Cryptology ePrint Archive*, 2025.
[19] BPS - Statistics Indonesia, "Indonesian economic report, 2023," Badan Pusat Statistik (Statistics Indonesia), Tech. Rep., 2023. [Online]. Available: https://www.bps.go.id/en/publication/2023/09/21/a62efbad86d18bc35581c33a/indonesian-economic-report--2023.html
[20] L. Schädler, M. Lustenberger, and F. Spychiger, "Analyzing decision-making in blockchain governance," *Frontiers in Blockchain*, vol. 6, p. 1256651, 2023.
[21] A. Sutarman, D. Juliastuti, I. Yati, L. P. Pasha *et al.*, "Enhancing security and privacy in blockchain systems for tax administration," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 145–155, 2025.
[22] Y.-Y. Fan, C.-J. Chew, and J.-S. Lee, "Asynchronous quantum-resistant blockchain for secure intelligence sharing," *Applied Sciences*, vol. 15, no. 11, p. 5921, 2025.
[23] U. Rahardja, Q. Aini, N. Lutfiani, F. P. Oganda, and A. Ramadan, "Blockchain application in education data security storage verification system," in *2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA)*. IEEE, 2022, pp. 1–4.
[24] M. Thanasi-Boçe and J. Hoxha, "Blockchain for sustainable development: A systematic review," *Sustainability*, vol. 17, no. 11, p. 4848, 2025.
[25] M. Zhang, J. Wang, J. Lai, M. Dong, Z. Zhu, R. Ma, and J. Yang, "Research on development progress and test evaluation of post-quantum cryptography," *Entropy*, vol. 27, no. 2, p. 212, 2025.
[26] M. Ullah, A. Ali, and A. Jadoon, "Quantum computing and blockchain security: A critical assessment of cryptographic vulnerabilities and post-quantum migration strategies," *Policy Research Journal*, vol. 3, no. 7, pp. 159–172, 2025.
[27] H. Khodaiemehr, K. Bagheri, and C. Feng, "Navigating the quantum computing threat landscape for blockchains: A comprehensive survey," *Authorea Preprints*, 2023.
[28] R. Supriati, S. A. Anjani, R. W. Anugrah, R. McCarthy *et al.*, "Enhancing network security with quantum cryptography: A study on future-proofing computer networks againstquantum attacks," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 24–35, 2025.

[29] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, 2023.
[30] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, "Post-quantum cryptography and quantum-safe security: A comprehensive survey," *arXiv preprint arXiv:2510.10436*, 2025.
[31] S. M. Hosseini and H. Pilaram, "A comprehensive review of post-quantum cryptography: Challenges and advances," *Cryptology ePrint Archive*, 2024.
[32] H. Oh and H. Jung, "Designing a scalable and area-efficient hardware accelerator supporting multiple pqc schemes," 2024.
[33] F. Zidan and D. E. Febriyanti, "Optimizing agricultural yields with artificial intelligence-based climate adaptation strategies," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 136–147, 2024.
[34] F. Opiłka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, "Performance analysis of post-quantum cryptography algorithms for digital signature," *Applied Sciences*, vol. 14, no. 12, p. 4994, 2024.
[35] D. Marchsreiter, "Towards quantum-safe blockchain: Exploration of pqc and public-key recovery on embedded systems," *IET Blockchain*, vol. 5, no. 1, p. e12094, 2025.
[36] S. Grebnev, Y. Melnichuk, I. Poltavskaya, O. Turchenko, A. Kurochkin, and A. Polubelov, "Analysis and challenges of implementing post-quantum cryptographic algorithms in ethereum and hyperledger fabric networks," *Journal of Computer Virology and Hacking Techniques*, vol. 22, no. 1, p. 3, 2026.
[37] T. Zhukabayeva, A. Ur Rehman, N. Tariq, and E. Benkhelifa, "Hyperledger fabric based post quantum cryptography healthcare application using discrete event simulation," *IEEE Access*, 2024.
[38] M. Vidaković and K. Miličević, "Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments," *Algorithms*, vol. 16, no. 11, p. 518, 2023.
[39] D. de Haro Moraes, J. P. A. Pereira, B. E. Grossi, G. Mirapalheta, G. M. M. A. Smetana, W. Rodrigues, C. N. Guimarães Jr, B. Domingues, F. Saito, and M. Simplício, "Applying post-quantum cryptography algorithms to a dlt-based cbdc infrastructure: Comparative and feasibility analysis," *Cryptology ePrint Archive*, 2024.
[40] M. B. Karo, B. P. Miller, and O. A. Al-Kamari, "Leveraging data utilization and predictive analytics: Driving innovation and enhancing decision making through ethical governance," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 152–162, 2024.
[41] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. Di Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 967–1002, 2023.
[42] S. Al-Janabi, "Post-quantum blockchain: Challenges and opportunities," *arXiv preprint arXiv:2508.17071*, 2025.
[43] A.-T. Ciulei, M.-C. Crețu, and E. Simion, "Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective," *Cryptology ePrint Archive*, 2022.
[44] D. A. Yusuf, R. W. Anugrah, M. A. Komara, D. Julianingsih, and E. Garcia, "Leveraging blockchain technology to strengthen cybersecurity in financial transactions: A comprehensive analysis," *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 119–125, 2024.
[45] P. Kolok, M. Hodon, M. Kubascik, and J. Kapitulik, "Design and comparison of hardware architectures for fips 140-certified cryptographic applications," *Electronics*, vol. 15, no. 1, p. 44, 2025.
[46] D. Loebenberger, S.-L. Gazdag, D. Herzinger, E. Hirsch, C. Näther, and J.-P. Steghöfer, "On the formalization of cryptographic migration," *arXiv preprint arXiv:2408.05997*, 2024.
[47] G. S. Parnell, C. R. Kenley, D. Clark, J. Smith, F. Salvatore, C. Nwobodo, and S. Davis, "Decision analysis data model for digital engineering decision management," *Systems*, vol. 13, no. 7, p. 596, 2025.
[48] K.-H. Nguyen, T. Comans, T. T. Nguyen, D. Simpson, L. Woods, C. Wright, D. Green, K. McNeil, and C. Sullivan, "Cashing in: cost-benefit analysis framework for digital hospitals," *BMC Health Services Research*, vol. 24, no. 1, p. 694, 2024.
[49] N. Lux, C. Mandal, J. Decker, J. Luboeinski, J. Drewljau, T. Meisel, C. Tetzlaff, C. Boehme, and J. Kunkel, "Hpc-ai benchmarks-a comparative overview of high-performance computing hardware and ai benchmarks across domains," *J. Artif. Intell. Robot.*, vol. 1, p. 2, 2024.
[50] I. Zablah, L. Sosa-Díaz, and A. Garcia-Loureiro, "Relevance and evolution of benchmarking in computer systems: A comprehensive historical and conceptual review," *Computers*, vol. 14, no. 12, p. 516, 2025.