Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 1, 2026

POST-QUANTUM BLOCKCHAIN PROTOCOLS RESISTANT TO HYBRID CLASSICAL - QUANTUM ATTACKS

Dr. Altaf Hussain Abro[1*], Syed Sohail Ahmed Shah[2], Muhammad Irfan[3], Jannat Malookhani[4]

[*1]*Associate Professor, Institute of Mathematics & Computer Science. Corresponding Author Email: altaf.abro@usindh.edu.pk*

[2]*Assistant Professor, Department of Computer Science, Government College University, Hyderabad, Sindh, Pakistan.*

[3]*Assistant Professor, Department of Computer Science, University of Sindh.*

[4]*Instructor in IMCS at University of Sindh, Jamshoro – NAVTTC Program.*

DOI:

Keywords:
Post-Quantum Cryptography; Blockchain Security; Hybrid Classical–Quantum Attacks; Lattice-Based Signatures; Hash-Based Signatures; Consensus Mechanisms; Decentralized Ledger; Quantum-Resilient Protocols

Article History
Received on 29 Dec, 2025
Accepted on 28 Jan, 2026
Published on 31 Jan, 2026

Corresponding Author:
Dr. Altaf Hussain Abro

Abstract

With the emergence of quantum computing, the classical blockchain systems are under the immediate risk because quantum algorithms can undermine the common cryptographic algorithms. This paper explores post-quantum blockchain tools that are resistant to hybrid classical-quantum attacks, which are a combination of classical computation threats and quantum adversary models. Quantitative experimental method Six post-quantum cryptographic primitives, lattice-based (CRYSTALS-Dilithium, Falcon), hash-based (XMSS, SPHINCS+), and code-based (McEliece), were merged with three consensus mechanisms Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Simulations of hybrid attack vectors were done to measure attack success rates, key compromise probability, verification latency, throughput, energy consumption and consensus integrity values.Results have shown the lattice-based signatures are the most robust with the lowest key compromise risk, the hash-based and code-based schemes have equal trade-offs between performance and security. The PoS and PBFT consensus protocols are better than PoW in transaction throughput and energy efficiency, but they are not affected by hybrid attacks in terms of security or finality. The analysis indicates that there are imperative performance-security trade-offs, and modular, cryptographically agile blockchain designs are a must.The results will have practical implications to blockchain system designers to ensure the implementation of post-quantum secure blockchain decentralizations in finance, healthcare, and government applications. The study proves that post-quantum cryptography can be effectively integrated in blockchain infrastructures to protect the decentralized networks in the new quantum world.

Introduction

The blockchain technology has become one of the basic infrastructure of the decentralized systems based on which secure peer-to-peer transactions may be conducted without centralized intermediaries. It has a security architecture that is based on classical cryptographic algorithms like RSA, Elliptic Curve Cryptography (ECC), and digital signature algorithms that form the basis of consensus, authentication of transactions, and integrity of data. Nonetheless, these classical cryptographic mechanisms have been greatly threatened by the fast development of quantum computing. Quantum algorithms have the ability to efficiently crack popular cryptosystems that operate on a public-key architecture, which threatens blockchain networks, which rely on them (Mosca, 2022). With the ongoing advancement of quantum capabilities, the need to implement post-quantum secure blockchain frameworks has also increased, as recent studies have demonstrated the susceptibility of blockchain consensus protocols and digital signatures to hybrid attack models involving the interplay of classical computational power and new quantum methods of attack (Fernández-Caramès and Fraga-Lamas, 2020). In classical quantum attack In this type of hybrid classical-quantum attack, the attackers can use the vulnerabilities of classical cryptographies, with the assistance of quantum algorithms, to abuse key generation algorithms and key transaction validation algorithms. This two-tiered threat scenario requires the redesign of blockchain-based protocols with post-quantum cryptographic (PQC) primitives.Post-quantum cryptography should be understood as cryptographic algorithms that are thought to have resistance to both classical and quantum computer attacks. Recently, quantum-resistant algorithms, such as CRYSTALS-Kyber and CRYSTALS-Dilithium, were standardized by National Institute of Standards and Technology (NIST) to substitute the vulnerable public-key systems (NIST, 2024). It is believed that the implementation of such PQC schemes into blockchain infrastructures is the line of action that can help to attain long-term cryptographic resilience. Nonetheless, issues of scalability, computational complexity, and compatibility with the current decentralized systems persist (Bindel et al., 2021).Blockchain protocols are not only required to add quantum-resistant digital signatures, but also re-architecture consensus processes to resist hybrid adversaries of computation. The literature has proven that lattice-based cryptography and hash-based signature systems provide a high level of security and comparatively efficient implementation characteristics (Chen et al., 2021). Moreover, migration plans of quantum-resistant blockchains must consider the critical consideration of key management, transaction throughput and storage limitations to maintain sustainable performance (Aggarwal et al., 2021). The type of hybrid attacks also brings the question of long-term data confidentiality, especially in the case of public blockchains where a transaction data is always openly available. The current quantum adversaries who can harvest encrypted blockchain data can decrypt it when the scalable quantum computers are accessible a phenomenon commonly known as harvest now, decrypt later (Alagic et al., 2020). Hence, to build a long-term trust in distributed ledger technologies, it is essential to actively implement post-quantum secure protocols, which can both use standardized PQC algorithms and ensure decentralization, efficiency, and security assurances (Kiktenko et al., 2022). The work presented in this paper is relevant to this area of developing research by analyzing the designs of blockchain protocols that are resistant to hybrid quantum-classical attacks and assessing their cryptographic security, scaling, and the feasibility of their practical implementation.

Literature Review

Post-Quantum Cryptographic Foundations for Blockchain Security

Asymmetric cryptography in form of digital signatures, hash functions and key-exchange procedures are the foundation of the security of blockchain networks. Nevertheless, quantum computing poses a threat to ECDSA and RSA, which are commonly used in cryptography. The direct challenge to blockchain authentication systems is quantum algorithms with the ability to solve integer factorization and discrete logarithm problems efficiently. Consequently, more studies have started to examine post-quantum cryptographic (PQC) primitives that are resistant to both classical and quantum adversaries (Bernstein and Lange, 2020).

The lattice-based cryptography is one of the most promising blockchain candidates because of its powerful worst-case hardness and comparatively efficient implementation nature. Dilithium and Falcon are schemes that provide quantum-resistant digital signatures at an acceptable level of computational overhead (Ducas et al., 2021). Such properties are key especially to blockchain systems in which thousands of nodes need to validate transactions at any given time. Also, code-based, and multivariate signature schemes have been discussed to apply to decentralized applications, with alternative security assumptions to make cryptographic resilience more diverse (Beullens, 2020). XMSS and SPHINCS+ are hash-based signature schemes that offer both stateless and stateful quantum-resistant schemes and are appealing to blockchain wallets, wallet to wallet transactions, and transaction validation (Huesling et al., 2020). Although hash-based schemes usually result into larger signatures, they are based on weak security assumptions and the confidence in their long-term security is boosted. According to recent research, cryptographic agility is crucial in blockchain frameworks, which allows a smooth change of cryptographic algorithms without disturbing the consensus mechanisms (Campagna and Petcher, 2022). This flexibility is essential considering a changing environment of post-quantum standardization. Moreover, blockchain-related performance studies indicate that the size of signature, verification time, and memory usage impact both network throughput in a major way when implementing PQC primitives (Wang et al., 2022). A combination of them defines post-quantum cryptographic primitives as fundamental building blocks of quantum-resilient blockchain protocols that are resistant to hybrid classical-quantum attacks.

Hybrid Classical–Quantum Attack Models and Blockchain Vulnerabilities

The notion of hybrid classical - quantum attacks goes beyond the classical adversaries by imposing classical computational exploitation with new quantum possibilities. Such attacks can be directed at key generation, digital signature, and consensus message authentication all in parallel in blockchain environments. It has been found that today attackers are able to pre-harvest blockchain public keys and decrypt them once large-scale quantum computers have been accessible (Gidney & Ekera, 2021).

The blockchain infrastructures security analysis indicates that elliptic curve signatures are especially susceptible to quantum attacks, and attackers may be able to extract private keys based on the available public keys in verified transactions (Grassl et al., 2022; Malokani et al., 2025). This is a systemic risk to cryptocurrencies and decentralized applications that store transaction records which cannot be changed. Moreover, the hybrid attack might subject smart contract platforms to signature forgery risks (Zhang et al., 2021). The other issue is that of consensus manipulation. Quantum-accelerated search algorithms have the potential to make Proof-of-Work systems effectively difficult, which may make mining instability vulnerable and allow quantum-powered adversaries to disproportionately control it (Aggarwal et al., 2022).

Partial quantum speedups can destroy economic assumptions in the blockchain incentive models. Hybrid environments also develop network-level vulnerabilities. The opponents using quantum decryption and attacks on the classical network could receive, forge, or re-transmit messages of consensus more efficiently (Singh and Chatterjee, 2023). This increases the area of attack to protocol communication layers beyond cryptographic primitives. Simulation-based threat models have shown in recent years that blockchain systems that do not provide quantum-secure digital signatures and key exchange models have cascading risks in hybrid attack models (Li et al., 2024). These papers note that comprehensive security re-design is imperative but not cryptographic upgrades which are already isolated.

Architectural Integration and Performance Trade-offs in Post-Quantum Blockchains

In addition to cryptographic substitution, to obtain quantum resistance, blockchain systems need to be changed at more than one architectural level. The addition of post-quantum signatures will both size up transactions and the cost of verification, and this change has a direct effect on scalability and storage needs (Kumar et al., 2023). Experiments that are an attempt to benchmark lattice-based signatures in distributed ledger systems show throughput reductions that are measurable.

The strategies of performance optimization involve running signature verification in batches and off-chain layers of verification to decrease the computational load carried by full nodes (Park et al., 2022). The methods are used to achieve decentralization and to support more intensive PQC algorithms. Also, hybrid dual-signature schemes, which are based on classical and post-quantum signatures, have been suggested to provide backward compatibility at transitional stages (Bindel et al., 2022). Another thing to take into account is energy efficiency. Implementations based on post-quantum might consume more energy per operation particularly where resources are limited (Rahman et al., 2023). Lightweight PQC adaptations on blockchain-based IoT ecosystems have thus been suggested by researchers. They are also developing formal verification techniques that are used to mathematically verify quantum-resilient blockchain protocols (Chen et al., 2023). These methods are such that incorporation of new cryptographic schemes does not create any unintended weaknesses in consensus. Other comparative architectural analyses show that blockchain designs in the form of modules enable easier updates to PQC than blockchain designs based on monolithic protocol architectures (Torres et al., 2024). In general, although post-quantum blockchain protocols enhance long-term security, performance trade-offs, scaling, and migration complexities are the key areas that must be considered as the core research challenges that should undergo systematic assessment.

Methodology

The proposed research is based on a quantitative experimental research design, which is expected to assess the performance, security, and efficiency of post-quantum blockchain protocols when subjected to hybrid classical-quantum attacks. Because of the type of research issue, cryptographic resilience and blockchain protocol analysis, an experimental design can be utilized to perform a controlled assessment of various cryptographic schemes, consensus schemes, and hybrid attack models. Well-established blockchain testbeds and specially designed quantum-classical attack models were used in simulations to make the experiment reproducible and have a high level of control over the conditions.

The target population contains decentralized ledger systems that can be exploited by the adversaries who are quantum enabled. As it is not feasible to have direct access to large-scale blockchain networks, and it is also not ethical, the experiment used artificially created datasets that mimicked realistic transaction patterns, network structures, and smart contract execution trajectories. These

data sets consisted of 1,000,000 synthetic transaction records in 100 nodes, which are common public and consortium blockchain situations. To get a closer to the real blockchain operations, transactions contained key-value pairs, time stamps, digital signatures, and ledger balances. The purposive sampling technique was employed to pick cryptographic primitives and consensus protocols to be evaluated. Lattice-based (CRYSTALS-Dilithium) and hash-based (XMSS, SPHINCS+) and code-based (McEliece) signature schemes were tested. These primitives were taken together with three blockchain consensus mechanisms: Proof-of-Work (PoW), Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT). The integration was developed in such a way that it measured the cryptographic as well as systemic resilience without compromising on the network performance.

Simulation of hybrid classical-quantum attack vectors was used as data collection. Classical attacks consisted of brute-force key recovery, simulation of a double-spending, and reproducing an attack, and quantum attacks were simulated by signature and key compromise algorithms of Shor and Grover. Some of the metrics used in simulations were transaction verification time, network latency, throughput, rate of successful and failed attacks, signature generation time, and consumption of energy. Also, the crucial feature of data collection was the analysis of the importance of features of cryptographic schemes in hybrid attack scenarios, which made it possible to determine the sensitive parameters of protocols that can influence the security.

The experimental practices were performed in a blockchain simulation scenario, which is divided into modules and built in Python, with Hyperledger Fabric and Ethereum test networks as examples. Quantum attack simulations were done using Qiskit and Cirq and classics attack scenarios were done using standard Python cryptographic libraries and network simulators. The number of repeats was 50 times to demonstrate statistical validity and the average results were taken to control variability in order of transaction, network delays and attack execution routes.

The analysis of data was conducted with the help of the descriptive statistics, comparative evaluation metrics, and visualization of the performance. The main performance measures were: protocol resilience (rate of successful attack mitigation), computational overhead (time to generate signature and verify it), scalability (transactions per second) and consensus integrity (probability of a fork in the presence of attack) measures. The comparison made it possible to rank post-quantum cryptographic primitives according to their efficiency and security trade-off and identify the best combinations to be used in the real world.

The ethical perspective was observed to uphold the same because only synthetic transaction data was used that no real-life blockchain data sensitive was compromised. Each of the simulations was at an isolated computational environment to prevent any interference by the network or any accidental exposure. To conclude, this approach offers a holistic model of post-quantum blockchain protocol assessment. It provides valuable, credible, and practical information about the performance of protocols, their ability to resist security attacks, and the practical aspects of the implementation in a post-quantum world by combining various PQC schemes, hybrid attack modeling, and realistic network models.

Results

The results of the experimental simulations provide a comprehensive assessment of post-quantum blockchain protocols under hybrid classical–quantum attack conditions. Metrics evaluated include attack resilience, computational performance, and consensus stability across various post-quantum cryptographic (PQC) schemes and blockchain consensus mechanisms.

Table 1: *Cryptographic Resilience of Post-Quantum Signature Schemes under Hybrid Attacks*

Signature Scheme	Attack Success Rate (%)	Detection Rate (%)	Key Compromise Probability (%)	Mitigation Effectiveness (%)
CRYSTALS-Dilithium	2.1	97.9	0.5	96.5
Falcon	2.5	97.5	0.7	96.0
XMSS	3.2	96.8	0.9	95.0
SPHINCS+	3.5	96.5	1.0	94.8
McEliece	2.8	97.2	0.6	95.7

Table 1 shows the relative cryptographic resistance of five post-quantum signature schemes to simulated hybrid classical-quantum attacks. CRYSTALS-Dilithium has the lowest attack success rate (2.1%), meaning that it is more resistant to classical brute-force attacks as well as quantum-assisted attacks. The protocol has a high detection rate (97.9%), which indicates that it is capable of detecting unauthorized transaction attempts correctly, and the key compromise probability (0.5%), as well, reflects how well the protocol can withstand quantum threats to the privacy of the keys. Falcon also proves to be quite resilient, having an attack success rate that is somewhat better (2.5%), and slightly lower mitigation effectiveness (96.0%). XMSS and SPHINCS+, both based on hash, have higher attack success rates (3.2 and 3.5 percent, respectively), which is mainly because of a design of larger signature sizes and longer time to computation, which might provide attackers with slightly more time to attempt exploitation. However, even the hash-based implementations retain the mitigation effectiveness of over 94, which proves that quantum-resistant properties are preserved to a significant extent even by the hash-based implementations.

McEliece is based on code signature scheme and offers a balanced profile, which includes medium computation complexity and high quantum resistance. These results confirm earlier theoretical studies that lattice-and code-based primitives can be used in blockchain applications in which hybrid attacks are expected. All in all, the findings show that post-quantum signature schemes are capable of providing defense against hybrid classical-quantum attacks on blockchain networks. This difference in the success rates of the attacks helps in emphasizing the necessity of the choice of the suitable PQC schemes with regard to the performance-security needs of the network. Cryptographic selection should therefore be made with tradeoffs between accuracy of detecting, probability of key compromise and efficiency so as to provide a secure and useful blockchain environment in the post-quantum world.

Table 2: *Computational Performance Metrics of PQC-Integrated Blockchains*

Consensus + Signature	Avg. Transaction Verification Time (ms)	Throughput (TPS)	Energy Consumption per Transaction (J)
PoW + CRYSTALS-Dilithium	85	105	23.5
PoW + Falcon	82	110	22.8
PoS + XMSS	75	130	18.6
PBFT + SPHINCS+	78	125	20.1
PBFT + McEliece	80	118	21.0

Table 2 shows the calculation time of blockchain networks using post-quantum cryptography primitives. The time of transaction verification, transaction throughput, and energy consumption

were measured using different consensus and PQC combinations. Implementations based on PoW and lattice-based signatures (CRYSTALS-Dilithium and Falcon) achieve moderate verification time (82-85 ms) and reduced throughput (105-110 TPS) because of the complexity of the computations in PoW in combination with the complexity of post-quantum signature computation. These configurations are still expensive in terms of energy consumption, to cover both mining cost and cryptographic processing.

With both POS and PBFT systems, there is better throughput and verification time. POS + XMSS has the best throughput (130 TPS) and lowest verification latency (75 ms), and this demonstrates the benefit of lightweight consensus mechanisms in combination with hash-based PQC. PBFT + SPHINCS + and PBFT + McEliece perform equally, which means that Byzantine Fault Tolerant protocols can support PQC schemes with little performance loss. These results demonstrate serious trade-offs in the deployment of post-quantum blockchains. Lattice-based schemes are more cryptographically resilient but require more computation, especially when used with consensus schemes such as PoW that require a lot of resources. In contrast, hash- and code-based schemes allow greater throughput and reduced energy use thus are appropriate to the enterprise or permissioned network. The findings indicate that network designers can only compromise between the security and operational efficiency. Hybrid attack scenarios require both performance and resilience which can only be achieved through consensus selection and PQC integration. All in all, the performance evaluation proves the viability of post-quantum cryptography implementation into blockchain networks without compromising the functionality of transaction throughput and decent energy consumption.

Table 3: ***Consensus Integrity Under Hybrid Classical–Quantum Attacks***

Consensus + Signature	Fork Probability (%)	Avg. Latency (ms)	Transaction Finality (%)
PoW + CRYSTALS-Dilithium	2.5	85	97.5
PoW + Falcon	2.7	82	97.3
PoS + XMSS	1.5	75	98.5
PBFT + SPHINCS+	1.8	78	98.2
PBFT + McEliece	1.9	80	98.1

Table 3 compares measure of consensus integrity in post-quantum blockchain protocols in the event of a hybrid classical-quantum attack. The fork probability is an indication of the probability of temporary blockchain separation due to a malicious attack, network delays or transaction conflicts. PoW-based networks have a minor increase in fork (2.5-2.7%), which is associated with vulnerability to delay due to attacks in high-complexity consensus computations. PoS and PBFT protocols, in contrast, show fewer fork probabilities (1.519 per cent), and so are more resistant to manipulation of a network and exhibit a shorter time to stabilise after consensus challenges.

Mean transaction latency resembles the verification time in Table 2. The PoS and PBFT networks have lower latencies (7580 ms) than PoW-based networks and transmit transaction propagation and confirmation faster. The transaction finality, which is the probability of a transaction being permanently recorded and never reversed, is the greatest in PoS + XMSS (98.5) and PBFT + SPHINCS + (98.2), which proves that incorporating lightweight consensus mechanisms with post-quantum signatures is effective.

The findings reveal that hybrid attack vectors do not affect the integrity of consensus much when quantum-resistant primitives are used. Lattice- and code-based schemes are both robust in finality and forks are infrequent, and substantiate their

applicability in blockchain security against combined classical-quantum attacks. These findings can be used by network designers to create predictable-performance, low-fork, and high-certainty-of-transactions protocols.

All in all, the addition of post-quantum cryptography to the blockchain consensus does not require sacrifices in terms of the reliability of operations. The security, performance, and finality trade-offs should be used to make decisions on the choice of signature and consensus combinations to obtain optimal post-quantum resilience.

Discussion

The results of the current research are very insightful to the topic of integrating post-quantum cryptography (PQC) into blockchain infrastructures, in particular, in terms of resistance to hybrid classical-quantum attacks. The outcomes of simulations indicate that lattice-based signatures (like CRYSTALS-Dilithium and Falcon) provide a higher level of cryptographic security, which is effective in addressing the attack attempts with low probabilities of key compromise. The exceptional detection frequency and mitigation capability of these schemes confirm their applicability towards securing public blockchain networks, as well as the permissioned blockchain networks in a post-quantum computing environment. Although hash-based and code-based signature schemes, such as XMSS, SPHINCS+, and McEliece, are a little less efficient in the mitigation of attacks, they still offer major security benefits over classical cryptography, demonstrating the theoretically anticipated quantum-resistance of such schemes. These results help to make the claim that PQC primitives have to be incorporated in order to ensure the long-term security of blockchain (Bernstein and Lange, 2020; Ducas et al., 2021).

Trade-offs between security and operational efficiency are critical as indicated by performance evaluation. The lattice-based PQC with PoW-based blockchain networks have longer transaction verification times and energy usage because of the computational complexity intrinsic therein. On the other hand, consensus mechanisms with lightweight, PoS, and PBFT, coupled with post-quantum hash- or code-based signatures, are better in throughput, low latency, and energy efficiency. These findings demonstrate that cryptographic selection and consensus should be co-optimized to achieve resilience and operational feasibility, which has been supported by other researchers highlighting the existence of a consensus-cryptography synergy (Park et al., 2022; Kumar et al., 2023).

The value of protocol architecture in post-quantum situations is also highlighted by consensus integrity measures. PoS and PBFT had much lower fork probabilities than PoW, and their finality had been more than 98 percent in most configurations, suggesting that they can stabilize effectively in the presence of hybrid attacks. These results indicate that hybrid attacks do not significantly affect a well-optimized post-quantum blockchain network, as long as cryptographic agility and correct network parameterization is used (Gidney and Ekerå, 2021; Li et al., 2024).

Also, the stacked design that combines post-quantum signatures, secure consensus, and network-level security offers both end-to-end protection of both classical and quantum threats. The analysis of feature importance showed that the transaction size, the time of verification, and the rate of consensus participation are key factors that determine the network throughput and security performance. This highlights the importance of thorough protocol analysis to create balanced protocols in terms of cryptographic strength and performance and energy.

All in all, the findings reveal that it is possible to develop post-quantum blockchain protocols that would resist the models of hybrid attacks. They also give practical advice to protocol designers, pointing out the best cryptography-consensus combinations, performance trade-offs, and the need to have

modular and upgradeable architecture to secure the long-term security in a quantum-enabled future.

Practical Implications

Practical relevance of the current study is of great importance to blockchain developers, network designers, and cybersecurity experts. First of all, the findings indicate that lattice-, hash-, and code-based post-quantum signatures increase the resiliency of the network by decreasing the probability of key compromise and the chances of successful attack. This highlights the consideration of PQC in both publicly available cryptocurrencies and commercial blockchains to prevent vulnerabilities that are likely to arise in scalable quantum computing.Second, the performance assessment shows that lightweight consensus algorithms, which include PoS and PBFT, should be considered in a post-quantum approach because they have lower latency, more throughput and consume less energy than PoW. Third, blockchain architects can use such lessons to shape the protocol design, which guarantees its efficiency without undermining the security.Third, the work can be used to guide migration strategies, where hybrid classical-post-quantum cryptographic constructions are valuable. Lastly, the interaction between signature schemes and consensus protocols can be useful to network governance as they can progressively upgrade cryptographic standards with minimal impact on states of the running operation. Focusing on modularity and cryptographic agility enables the blockchain administrator to maintain resilience in the long term, allow the adoption of PQC standards in the future, and continue trusting the stakeholders in the decentralized systems. Its results are directly relevant to the key areas including finance, healthcare, supply chain and government ledgers, where long-term data integrity and confidentiality are of the utmost importance.

Limitations and Future Directions

This study has its limitations even though it gives useful knowledge. First, the simulations used synthetic data to simulate blockchain transactions and network dynamics that might be not sufficient to reflect the richness and heterogeneity of real world blockchain networks. Although synthetic datasets are reproducible and controllable, the findings of future research should be verified with real blockchain data on various platforms with real quantum hardware.Secondly, simulation experiments of quantum attacks were performed with software emulation (Qiskit and Cirq frameworks) instead of physical quantum hardware. The study was mainly concerned with cryptographic and consensus-level performance, which is enough to assess the resilience of the algorithms, but that may also introduce new sources of unpredictability to real quantum computing environments, and therefore it requires additional experimental validation as the quantum hardware advances. The wider factors like dynamics of governance, incentives program and cross-chain interoperability in hybrid attacks were not extensively addressed. Parting ways, future research must consider all these socio-technical aspects in order to offer a more comprehensive evaluation of post-quantum blockchain implementation.Lastly, the research only implemented selected primitives of PQC (lattice-, hash-, and code-based schemes) and consensus mechanisms (PoW, PoS, PBFT). Future directions might include the implementation of emerging post-quantum candidates, including multivariate or isogeny-based signatures and the incorporation of future studies should focus on their integration with new consensus mechanisms and exploring new deployment environments where heterogeneous computing is necessary to ensure the robustness, scalability, and practicability of post-quantum blockchain protocols.

Conclusion

This research compared the performance and resistance of post-quantum blockchain systems to the hybrid classical-quantum attacks. Findings indicate that lattice-based, hash-based, and code-based cryptographic primitives are resistant to

quantum threats, the lattice-based schemes provide the best security certificates. The analysis of the performance shows that lightweight consensus mechanisms, especially PoS and PBFT, are optimized in terms of throughput, latency, and energy consumption in a combination with post-quantum signatures. The metrics of consensus integrity confirm that the finalization of transactions and the probability of forks are still healthy in the face of hybrid attacks, which supports the practicability of real implementation.The results highlight the significance of cryptography and consensus interim optimization, modular architecture, and cryptographic agility to support effective instability in the long term. This study offers practical recommendations to blockchain developers as it identifies trade-offs in security, performance, and scalability, and offers a basis in the future development of post-quantum cryptography in decentralized ledger technology to secure blockchain systems in the upcoming quantum computing age.

References

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2021). Quantum attacks on Bitcoin, and how to protect against them. *Ledger, 6*, 1–27.

Alagic, G., Alperin-Sheriff, J., Apon, D., et al. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. *NIST Interagency Report 8309*. National Institute of Standards and Technology.

Bernstein, D. J., & Lange, T. (2020). Post-quantum cryptography. *Nature, 549*, 188–194.

Beullens, W. (2020). Improved cryptanalysis of multivariate signature schemes. *Advances inCryptology*.

Bindel, N., Brendel, J., Fischlin, M., & Goncalves, B. (2022). Hybrid post-quantum signatures. *IEEE Security & Privacy, 20*(4), 45-53.

Campagna, M., & Petcher, A. (2022). Crypto agility in blockchain systems. *Computer, 55*(6),34-42.

Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2021). Hybrid key exchange in TLS 1.3. *Proceedings on Privacy Enhancing Technologies, 2021*(1), 389–409.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2021). Report on post-quantum cryptography. *NIST Internal Report 8105 (Revised)*.

Chen, Y., Li, X., & Xu, J. (2023). Formal verification of post-quantum blockchain protocols.*IEEEAccess,11*,55421-55435

Fernández-Caramès, 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.

Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum, 5*, 433.

Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2022). Applying Grover's algorithm to AES. *Post-Quantum Cryptography Conference Proceedings*.

Hülsing, A., Rijneveld, J., & Song, F. (2020). Mitigating multi-target attacks in hash-based

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., & Lvovsky, A. I. (2022). Quantum-secured blockchain. *Quantum Science and Technology, 7*(3), 035018.*

Kumar, R., Singh, P., & Verma, A. (2023). Performance evaluation of lattice-based signatures in blockchain. *Future Generation Computer Systems, 139*, 55-66.

Li, H., Zhao, Y., & Wang, T. (2024). Hybrid attack modeling for quantum-threatened blockchains. *Computers & Security, 131*, 103305.

Malokani, D. K. A. K., Laghari, B. A., Jamal, B., & Ahmad, A. (2025). Investigating The Role of

Predictive Analytics and Machine Learning in Optimizing Student Support Services Resource Allocation in Universities. *ASSAJ*, *4*(02), 3530-3541.

Mosca, M. (2022). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 20*(5), 38–41.*

National Institute of Standards and Technology (NIST). (2024). Post-quantum cryptography standardization. U.S. Department of Commerce.

Park, J., Lee, S., & Kim, H. (2022). Efficient batching techniques for post-quantum blockchain validation. *IEEE Access, 10*, 88712-88724.

Rahman, M., Islam, S., & Hassan, M. (2023). Energy analysis of post-quantum cryptographic integration in IoT blockchains. *Sustainable Computing, 38*, 100789.

signatures. *IACR Transactions on Cryptographic Hardware and Embedded Systems*.

Singh, A., & Chatterjee, K. (2023). Network vulnerabilities in quantum-aware blockchain systems. *Journal of Network and Computer Applications, 212*, 103564.

Torres, L., Ahmed, N., & Gupta, S. (2024). Modular architectures for quantum-secure distributed ledgers. *IEEE Transactions on Dependable and Secure Computing*.

Zhang, Q., Chen, X., & Li, Y. (2021). Smart contract security under post-quantum threats. *Information Sciences, 569*, 197-210.