Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Quantum Resilient Blockchain Protocols for Securing U.S. Financial Systems

Md Rasheduzzaman Labu
Department of Information Assurance and Cybersecurity, Gannon University, Erie, PA, USA

Md Fahim Ahammed
Department of Information Assurance and Cybersecurity, Gannon University, Erie, PA USA

Corresponding Author: Md Rasheduzzaman Labu**, E-mail**: sourcerweb@gmail.com

| ABSTRACT

Blockchain technology has been in recent years among the most adopted technologies in the U.S. It has disrupted whole industries, ranging from finance and health to supply chain management and verification of digital identities. Nevertheless, such a tendency does not imply that the Blockchain systems are by any means fully protected against threats emanating from other emergent technologies, like quantum computing. State-of-the-art algorithms like Secp256k1 and Schnorr afford high levels of security in Blockchains; notwithstanding, they are vulnerable to quantum attacks. To solve this problem, a series of quantum-resistance algorithms has been proposed. Performance analysis of Quantum-resistant algorithms on a Blockchain in this respect, therefore, originates from getting effective insights into the efficiency of quantum-resistant algorithms in real-world scenarios. In light of the above need, we prototyped and analyzed the Falcon algorithm for a quantum-resistant Blockchain. Falcon is preferred because it provides a smaller signature and key size compared to Crystals-Dilithium and Sphincs++. This paper proposes a systematic quantum-resistant Blockchain and suggests different approaches to select quantum-resistant algorithms based on different Blockchain scenarios. These results from our approach and benchmark have implications for the future development and adoption of quantum-resistant Blockchains.

| KEYWORDS

Quantum-Resilient Blockchain; Quantum Computing; Falcon algorithm; Blockchain Security; Post-quantum signatures; Cryptography

| ARTICLE INFORMATION

ACCEPTED: 01 November 2025 **PUBLISHED:** 26 November 2025 **DOI:** 10.32996/fcsai.2025.4.2.4

Introduction

According to Kim et al. (2024), there has been massive development in recent years in the application of Blockchain technology in various industries, including finance, healthcare, supply chain management, and verification of digital identities. It also embodies several potential threats emanating from technologies at their inception today, such as quantum computing. Quantum computers can perform complex calculations-such as recreating private keys from public keys- much faster than even today's fastest supercomputers. Walter & Bardeen (2022), argued that while current quantum computers cannot break traditional encryption methods, Shor's algorithm provides a theoretical way in which vulnerabilities would be exploited in systems that are based on elliptic curve cryptography, such as Bitcoin and Ethereum. Shor's algorithm allows quantum computers to efficiently factorize integers, thereby compromising the secret keys used in Blockchain systems. This certainly poses a high risk to the popular digital signature schemes such as Secp256K1 and Schnorr, which rely on the hardness of integer factorization for their security. Considering the fast development of quantum computing, the need for developing quantum-resistant algorithms is necessary to safeguard the existing Blockchain systems against future quantum threats.

Copyright: © 2025 the Author(s). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) 4.0 license (https://creativecommons.org/licenses/by/4.0/). Published by Al-Kindi Centre for Research and Development, London, United Kingdom.

To address these challenges, a set of new algorithms has been developed that are not based on prime factorization but on mathematical problems considered hard to solve for both classical and quantum computers. Among the so-far-proposed quantum-resistant algorithms, Falcon, Crystals-Dilithium, and Sphincs+ emerged as the most secure and technologically advanced quantum-resistant digital signature schemes (Bishwas & Sen, 2024). However, several questions remain about their scalability and computational efficiency in real-world Blockchain applications. Theoretical studies, while performing extensive analyses and studying the relative strengths and weaknesses of these algorithms, have mostly shown their performance in off-chain scenarios. A notable lack of practical metrics for real-world performance and thorough performance evaluations about Blockchains using such state-of-the-art quantum digital signatures also exists (Larziko, 2023).

Background and Motivation

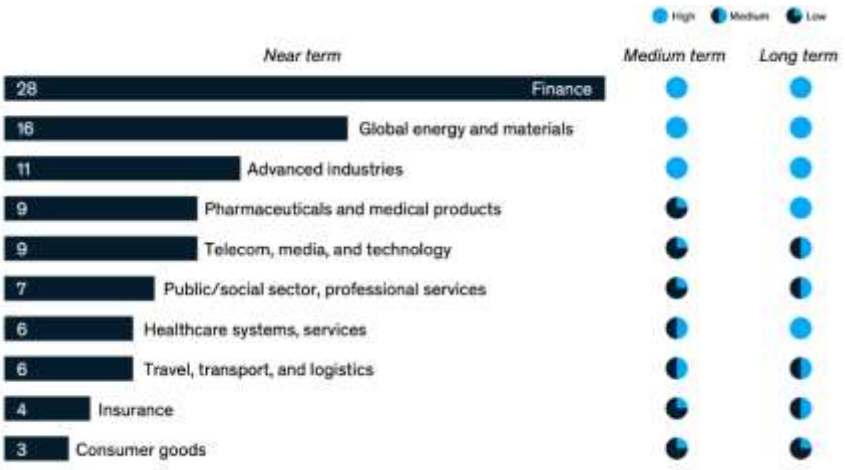
As per Casino et al. (2024), blockchain is one of the most talked-about technologies and fastest-growing innovations to date. At this juncture, it has gained recognition as an innovative solution not only in general but also in many industries. Since the time Blockchain was introduced back in 2008, this technology has emerged as a leading innovation with the potent potential to change the way we interact and automate payments or track and trace transactions. Kim et al. (2024), reported that this invention will give substantial cost benefits since the central authority has to monitor and validate the interactions/transactions among the multitude of participants. Each transaction in the Blockchain system is cryptographically signed and mined via nodes running a replica of the overall ledger that maintains within itself a chain of timestamped blocks of all transactions.

In this context, performing a comparative assessment of quantum-resistant Blockchain systems can provide valuable insights into the scalability and robustness of emerging quantum-resistant algorithms in real-world scenarios. This research Project aims at carrying out such an analysis for evaluating a quantum-resistant Blockchain using one of the latest quantum-resistant algorithms known as Falcon. The reason behind choosing Falcon is that, out of many such algorithms, it offers the best security against quantum attacks, and it also requires fewer computational resources compared to Sphincs+ and Crystals-Dilithium (Fauziyah et al., 2024). In this regard, our work proposed Quantum Blockchain prototype integration of Falcon for providing digital signatures and proof-of-stake combined with Byzantine fault tolerance as consensus mechanisms. Key metrics investigated in the decentralized setting concern key size, generation time, signature size, generation time, transaction size, and verification time. Finally, we provided the step-by-step framework to implement a quantum-resistant Blockchain.

Research Objective

This research is interested aims at designing, curating, evaluating, and propositioning quantum-resistant Blockchain protocols to secure U.S. financial systems against a wide range of emerging threats by quantum computing. The study intends to utilize post-quantum cryptography algorithms in coming up with robust Blockchain solutions to ensure data integrity, transactional security, and system reliability in the post-quantum world, based on the identified susceptibility in the current cryptographic frameworks. Besides, this paper intends to contribute by assessing the scalability, efficiency, and practical applicability of those protocols, therefore providing a strategic framework for protecting critical financial infrastructure and confidence against advancing quantum technologies.

Problem Statement



The graph above represents some of the expected impacts of emerging technologies specifically quantum computing, on various industries in the near, medium, and long term. The finance sector is seen to have the highest impact in the near term,

which would remain high going into the medium and longer term. Other noticeable near-term impacts can be seen in industries like Global Energy and Materials, Advanced Industries, Pharmaceuticals, Telecom, and Healthcare (Milnor & Kummer, 2024); in due course of time, the impact level of some of the industries decreases to medium or low influence in the long-term. Industries like consumer goods, insurance, and logistics show relatively low near-term impacts, and similarly cannot show much influence in the medium- and long-term period (Sanzeri, 2024). This means that those industries that handle very sensitive data or complex computation, such as finance, are at critical risk due to disruptive innovation the theme of early adoption of secure technologies, including quantum-resistant cryptography, is to be well-prepared.

Blockchain Overview

As per Casino et al. (2019), blockchain refers to a set of existing technologies put together in such a way that they produce a secure, trusted, and immutable database known as a Digital Ledger. Blockchain can also be defined as a trusted, decentralized, and secure database and network combined into one. A Blockchain comprises blocks that are interlinked in a secured manner; further, each block contains information such as transactions, Merkle tree, block hash, block number, and difficulty, among others. The data on the blockchain is immutable, and secured by a series of computers called miners/validators.

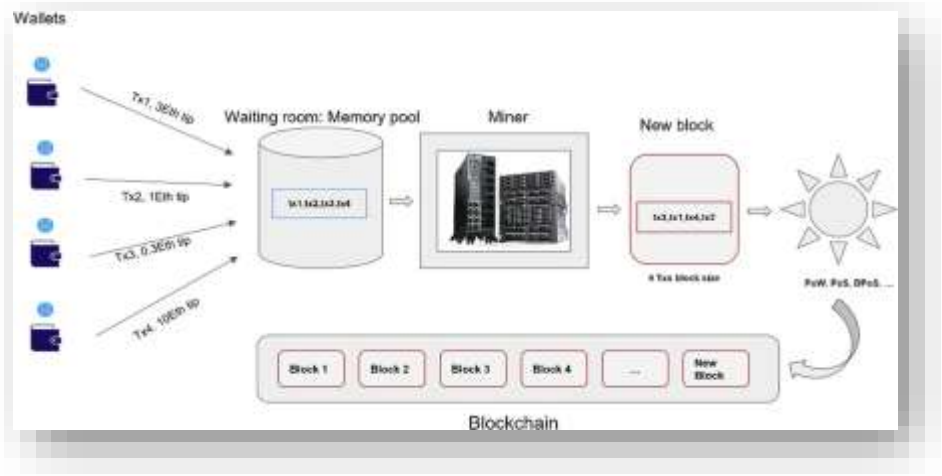


Figure 1: Portrays Transaction Life cycles

Each block in a Blockchain contains several transactions, and these transactions go through different stages before they are confirmed and added to a new block as shown in Fig. 1. The lifecycle of a transaction starts when a user signs the transaction with his private key. The details on key pair generation are discussed in the Blockchain security section. The Signed transaction is forwarded to the nearest node for verification. The valid transaction is then sent to the P2P network of the Blockchain, where every node stores this transaction in its memory pool locally holding area for transactions that have not yet been confirmed (Casino et al., 2024). The next step will be that the transactions from the memory pool are gathered together and included in a block, and mining or the validation process is started through a predefined consensus protocol. As soon as a particular node verifies the block, it is supposed to be verified by all nodes in the network for adding it to their locally copied Blockchain (Bansod & Ragha, 2022). So, the consensus algorithm of each Blockchain regulates this newly issued block validation process as depicted in Figs. 2 and 3,

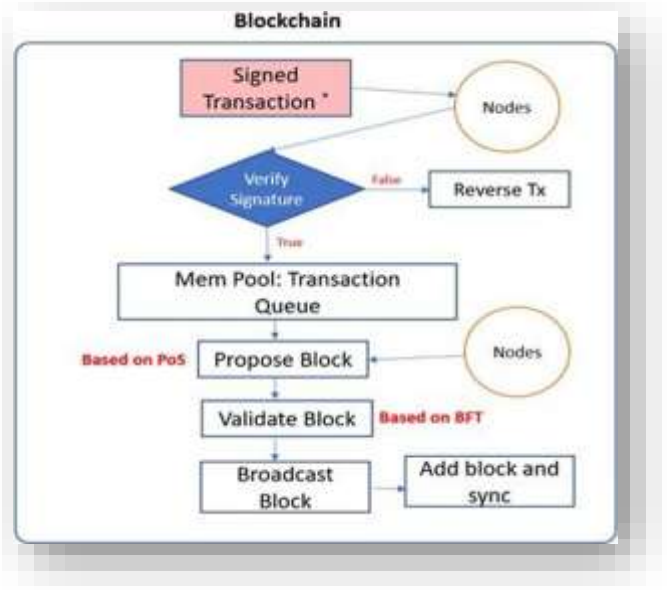


Figure 2: Visualizes the Transaction Verification Process

The flow diagram above depicts the transaction life cycle running on a blockchain network, highlighting all the steps in transaction validation and block propagation. Early steps involve a Signed Transaction, where a user or Node creates the transaction. It also embeds within it a cryptographic signature to introduce the authenticity and integrity attributes to it. The message is then forwarded to any one node in the Web3 Nodes, which refers to the decentralized participants within the node network (Sinai & Peter, 2024). The Verify Signature step is a critical security measure wherein, should the signature verification fail clear evidence of tampering or forgery-the transaction is rolled back and hence effectively discarded. This way, only the legitimate transactions move further on in the system.

According to Sinai & Peter (2024), after the signature is verified, the transaction enters a state called Mem Pool, short for Memory Pool, a sort of cache or queue for pending transactions. Group the transactions from the Mem Pool into blocks. In the Propose Block step, normally based on some sort of consensus-one at a time, such as Proof of Stake-normally, one or several nodes, in their role of validators, create a new block of batches of transactions. With a proposed block, this action confirms that the newly proposed block meets the predetermined rules and consensus of the blockchain. This mostly involves Byzantine Fault Tolerance mechanisms of validation for ensuring consensus among nodes even in the presence of potentially malicious or faulty participants.

Bansod & Ragha (2022), postulated that behind every blockchain implementation, there is a consensus layer. The most important layer is the consensus layer since it deals with validating the blocks and making sure there is not any altered block or transaction. Mostly, the consensus algorithms are categorized into two groups: the consensus-based voting mechanism Byzantine Fault Tolerance and Sybil control consensus-based Proof of Work and Proof of Stake. Several consensus algorithms and. Culei et al. (2022), reported that one of the salient features of Blockchain is security. Blockchain security depends on some cryptographic algorithms, such as elliptic curve cryptography for digital signature, and other cryptographic algorithms and hash functions that are used intensively during key pair generation, transaction signature and verification, consensus verification, Merkletree generation, block hashing, and so on. In this section, we are going to focus on Ethereum security as our case study.

Quantum Computing: Post-quantum cryptography

Li et al. (2021), posited that quantum computing is a branch of computer science that incorporates the capabilities of quantum mechanics to solve problems way beyond the realm of classical computers. A quantum computer is a bigger machine that solves a problem, which somehow or completely cannot be solved by a classical computer. This component implies that some cryptographic algorithms, such as elliptic curve digital signature algorithm support, will be insecure when a quantum computer of sufficient power is built due to Shor's algorithm. In fact, in preparation for this looming threat, many organizations are currently working on the needed solution to safeguard against quantum attacks. Among the most promising approaches, lattice-based cryptography has emerged as a pioneering candidate in providing secure post-quantum protection mechanisms (Lazirko, 2023).

Lattice-Based Cryptography

According to Fan-Fang Chua et al. (2024), Lattice-based cryptography is an area of cryptography based on mathematical problems that are mentioned among the most promising candidates to assure security in post-quantum cryptography. Quantum resistance is based on the fact that quantum computers are unable to easily solve this type of problem. The best-known problems involve Learning with Errors (LWE), its variant Ring Learning with Errors (RLWE), and the Shortest Vector Problem (SVP). SVP lies in the finding of the shortest vector in some high-dimension lattices. It is supposed to be one of the hardest problems a quantum computer can handle because of the nature of the computations involved. Rahman (2024), contended that a quantum computer relies on superposition principles; therefore, it requires the states of the quantum bits or qubits to be perfectly aligned. If these states are not aligned perfectly, then full exploitation of the superposition is not possible, and the quantum computer has to fall back to some conventional modes of computation. This limitation raises the possibility of errors while trying to solve the SVP and makes it resistant to quantum attacks. Because of this, lattice-based cryptography is considered a robust quantum-resistant solution. A more verbose account of the mathematical underpinning of the lattice problems and how they interface with quantum algorithms can be found in the lattice-based cryptography-related references.

Proposed 5-Phase Approach for Safe-guarding Blockchain Against Quantum Attacks

In this section, we outline all the critical steps that are necessary to transition to quantum-safe technology, which includes the identification of quantum threats to the selection of quantum-resistant algorithms, among other considerations.

- **Step 1: Identify the threat:** Quantum computers threaten traditional cryptographic methods since they could break many cryptographic algorithms currently in use for the purpose of securing communication and data storage. Their ability to execute certain computations much faster than classical computers allows them to solve mathematical problems that form the basis of many cryptographic systems (Sinai & Peter, 2024).
  Quantum computers can solve the "discrete logarithm problem" underlying many cryptographic algorithms used to keep Internet communications, including protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), secure(Sinai & Peter, 2024). Many symmetric key encryption algorithms in everyday use today, including the Advanced Encryption Standard (AES), can also be broken by them. By comparison, Figure 5 represents quantum-resistant versus non-resistant algorithms.

As an example, quantum computers can solve efficiently the "discrete logarithm problem," which is one of the bases underlying the cryptographic algorithms in protocols like Secure Sockets Layer SSL and Transport Layer Security TLS, securing Internet communication. They could break many symmetric key algorithms in common usage, for instance, the Advanced Encryption Standard AES. Figure 5 underlines a comparison of quantum-resistant versus nonresistant algorithms (Sinai & Peter, 2024).

$N=p*q$

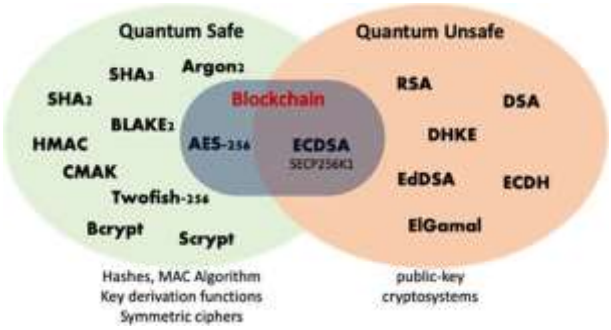


Figure 3: Displays Quantum-unsafe and Quantum-Resistant Algorithms

- **Step 2. Risk assessment:** All cryptographic algorithms whose security relies on the integer factorization problem are quantum-broken. The algorithm deals with finding the prime factors of a large composite number. It is believed to be infeasible for classical computers to solve the problem when numbers contain more than a few hundred digits, but quantum computers can solve it much faster (Sinai & Peter, 2024). The integer factorization problem could be expressed mathematically in the following manner: given a composite integer N, find its prime factors p and q.

According to Michelagnoli (2023), Most cryptographic algorithms, for example, the RSA and ECDSA algorithms rely on this problem to be difficult. Quantum computers, however, use algorithms such as Shor's algorithm to solve the integer factorization problem way more efficiently than any classical computer can so far, hence enabling them to break the encryption obtained

through the aforementioned algorithms (Sinai & Peter, 2024). Besides the integer factorization problem, it is also able to solve the discrete logarithm problem used widely in Blockchain. It is the problem of finding the value of x in the following equation:

$$g^x = h \pmod{p}$$

Here, g and h are pre-set values, and p is a prime. Many such cryptographic algorithms, including the Diffie-Hellman key exchange, are based on the security assumption of this problem no efficient algorithm for mining can be found. Quantum computers take advantage of algorithms such as the quantum discrete logarithm algorithm, which solves the discrete logarithm problem much more rapidly than a classical computer. As a result, they can effectively break the encryption offered by these cryptographic methods (Michelagnoli, 2023).

- **Step 3: Selecting Quantum-Resistant Algorithm:** Variety ranges in different post-quantum algorithms that can be developed to securely replace the existing quantum-vulnerable cryptographic methods. These submitted algorithms to NIST undergo evaluation, and in early July 2022, NIST announced four post-quantum algorithms that have been proven secure against quantum and classical computers (Raheman, 2023). The categories of algorithms are divided into two divisions

- General Encryption: ** CRYSTALS-Kyber

-Digital Signatures: CRYSTALS-Dilithium, Falcon, and Sphincs+

Above are the algorithms that were chosen for the postquantum cryptographic standard currently under development at NIST and are due to be completed in 2024.

- **Step 4: Crafting Quantum-Resistant protocols:** The description of a quantum-resistant blockchain covers all the aspects of quantum-resistant protocol design: quantum-resistant routing protocols, node-discovery protocols, peer-to-peer protocols of communication, and quantum-resistant consensus mechanisms (Raheman, 2023).
    - **Quantum-Resistant Routing:** Quantum-resistant routing protocols should be in place to ensure that, even against the occurrence of quantum attacks, data is efficiently and securely routed across the network. This may be ensured by the implementation of quantum-attack-resistant routing algorithms, such as quantum-resistant link-state or distance-vector routing protocols (Raheman, 2023).
    - **Quantum-Resistant Node Discovery:** Quantum-resistant node discovery protocols ensure nodes can always discover and reconnect to other nodes in the network securely and efficiently, even against active quantum attacks. This would involve the implementation of quantum-resistant algorithms for node discovery, like quantum-resistant flooding and gossip-based protocols (Sanzeri, 2023).
    - **Quantum-resistant peer-to-peer communications:** It is a quantum-resistant peer-to-peer communication protocol that will assure nodes are able to communicate securely and efficiently with each other, even against potential quantum attacks. This may include the implementation of quantum-resistant communication algorithms, including quantum-resistant key exchange protocols or quantum-resistant message authentication codes (Sanzeri, 2023).
    - **Quantum-Resistant Consensus:** The Blockchain will be able to finally reach a secure and decentralized consensus among nodes, even in the presence of possible quantum attacks, by implementing quantum-resistant consensus algorithms. This may include the implementation of quantum-resistant proof-of-work or proof-of-stake consensus algorithms or the implementation of a quantum-resistant variant of the existing consensus algorithms. All these protocols shall be designed to be protected against any potential quantum-based attack and to withstand such attacks. The protocols should undergo regular tests and evaluations to enforce their robustness (Sinai & Peter, 2023).
- **Step 5. Quantum-resistant hardware** -The blockchain itself is also divided into five layers as depicted in Fig. 6, namely: Application, Consensus, network, Data, and hardware layers. All these layers have to provide a quantum-resistant mechanism to make the Blockchain fully quantum-resistant. Therefore, hardware/infrastructure must be secure against quantum attacks (Sinai & Peter, 2023).

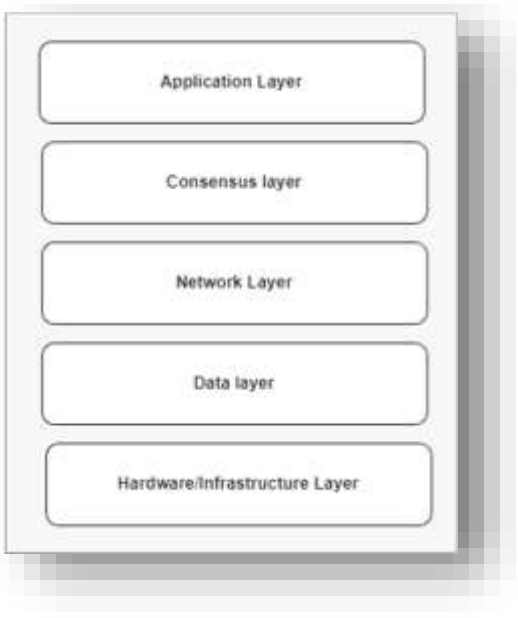


Figure 4: Illustrates the Block-Chain Layers

The flowchart in Figure 4 above shows that blockchain architecture is a layered structure that, starting from the roots, includes hardware to application. Hardware/Infrastructure Layer: This is the base layer that requires physical hardware, including servers and storage devices with relevant network infrastructure to host and use the blockchain (Sinai & Peter, 2024). It provides the necessary computing power and connectivity for operating blockchain nodes-computers, processing transactions, and maintaining the decentralized network. The robustness and scalability of this layer directly influence the overall performance of the blockchain network.

Above the hardware layer lies the Data Layer, which entails the instrumental data structures and storage mechanisms of the blockchain. The responsibility it has to ensure that actual storage is implemented, meaning in real instances of such an application blockchain ledger will hold blocks and transactions with links to hold the integrity through the cryptographic hash (Sanzeri, 2023). Accordingly, the data layer incorporates facilities such as Merkle trees so that verification and retrieval are highly efficient. Besides this, the said layer has already managed all those facets of immutability and redundancy such that every participant remains left with identical, interference-free copies of blockchain data (Raheman, 2023).

The Network Layer provides for the peer-to-peer communication of the blockchain nodes. Guaranteed under decentralized propagation of information in the form of broadcasting transactions or block synchronization. Above this is the Consensus Layer, which is the layer that coordinates the nods in such a way as to agree on the verification and addition of new blocks in the blockchain. It has a consensus mechanism like PoW, PoS, and BFT that keeps the record of all transactions consistent and tamper-proof (Raheman, 2023). The Application Layer interacts with end users and developers through user interfaces for Apps and smart contracts. The functionality of blockchain in practice-e.g., cryptocurrency transactions, supply chain management, and safe data sharing becomes achievable this way. This set of layers provides the entire framework for ensuring that the functionality of blockchains is reliable and adaptive across various use cases.

Quantum-resistant Blockchain

As per Sinai & Peter (2024), to provide quantum security, the quantum-resistant should be implemented into the user's wallet and Blockchain nodes as shown in Fig. 7, which begins when a user joins the network. Then a quantum wallet is generated using the Falcon algorithm where this private and public key is kept inside that wallet. The next one is emitting transactions to the Blockchain.

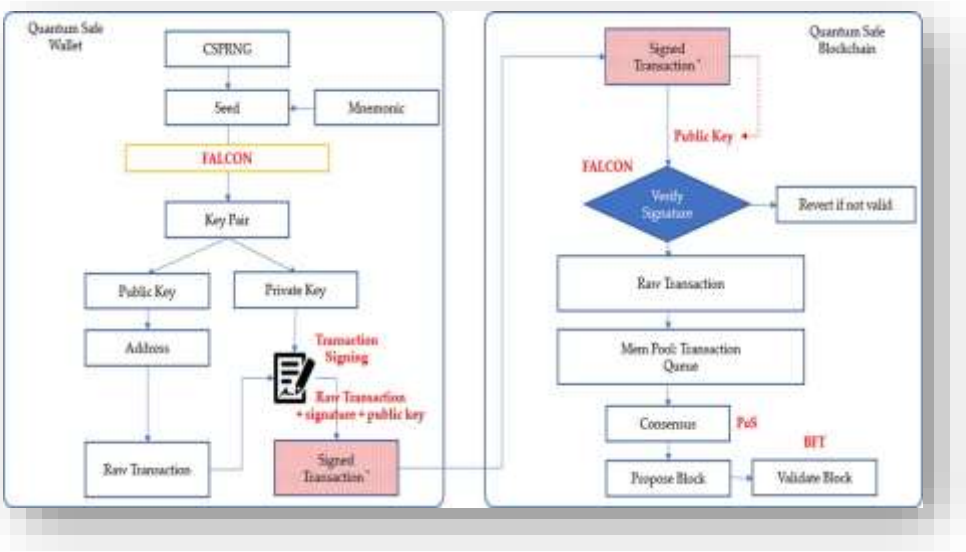


Figure 5: Exhibits the Quantum-Resistant Block Chain and Wallet Flow-chart

Figure 4 enumerates a process designed for a quantum-safe blockchain ecosystem, underscoring safe and secure cryptographic techniques to counteract potential threats from quantum computing. It is subdivided into Quantum Safe Wallet and Quantum-Safe Blockchain sections to show interactions between Wallet Generation, Transaction Signing, and Blockchain Procession. As per Sinai and Peter (2024), The Quantum-Safe Wallet begins the process by making use of a CSPRNG, or Cryptographically Secure Pseudo-Random Number Generator, securely generating a random seed. This is a seed from which a mnemonic phrase for easy backup and restoration is derived. Using the quantum-safe cryptographic algorithm of FALCON, this produces a key pair, which consists of a public key and a private key. The public key generates an address that will serve as the identity on this blockchain, while the private key is used for signing transactions.

As regards the Quantum-Safe Blockchain Section, the signed transaction goes to the blockchain system. Here, the blockchain checks the signature of the transaction using a public key and FALCON. In case the verification of the transaction fails, it is rejected; otherwise, the transaction continues. Once validated, it moves into the Mem Pool, a pool for pending transactions that are waiting in a queue(Sinai & Peter, 2024). Afterward, the blockchain uses a proof of stake-type consensus for selecting a proposer node that aggregates some number of transactions into a block. This is further followed by Byzantine Fault Tolerance for the validation of blocks to make sure that nodes agree that a block is valid, even when some are malicious or faulty.

According to Andreou et al. (2024), this protocol focuses on blockchain security with quantum resistance and performs cryptographic operations with FALCON against potential quantum computational powers. This represents how quantum-safe methods may be integrated into traditional blockchain processes: creating a wallet, signing of transactions, and verification of blocks among other activities. It has a forward-looking design to future-proof blockchain systems against emergent quantum threats while retaining their underlying principles of decentralization, security, and efficiency in performance. Signing the raw transaction with the private key results in a signed transaction containing the raw transaction data, the digital signature, and the public key. This will ensure the authenticity of the transaction and its verifiability without exposure to the private key.

To make the development easier, the transaction only contains the signature and a "hello" message. The signed transaction is emitted to the nearest Blockchain node which will verify the eligibility of the signature. Immediately after the transaction is valid, the validator will broadcast it to other modes. According to the Proof of Stake mechanism, the block proposal is elected, and the proposed block has been broadcast on the network (Sinai & Peter, 2023). All nodes verify it using Byzantine Fault Tolerance and once verified, the latest block containing that transaction is added to the node's local ledger, and this goes on and on.

Conclusion

This research project presented an implementation and performance evaluation of the quantum-resistant Blockchain, which is based on the Falcon algorithm with Proof of Stake and Byzantine Fault Tolerance mechanisms according to a proposed framework. Its performance was compared to commonly used Blockchains that are based on Secp256k1 and Schnorr digital signatures, respectively, vulnerable to quantum attacks. This study demonstrated that a quantum-resistant Blockchain by deploying the Falcon algorithm is theoretically and mathematically secure against quantum threats but compared to quantum-

vulnerable variants due to the inherent complexity in the mathematical operations of the algorithm. Besides, the signature and key size remain fairly constant across all key strengths, which shows the efficiency of the algorithm. Moreover, a digital signature scheme's security is closely related to the key involved: the longer and more complex the key, the better the security.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Andreou, A., Mavromoustakis, C. X., Markakis, E. K., Mastorakis, G., Pallis, E., & Bourdena, A. (2024). Exploring Quantum-Resistant Cryptography Solutions for Health Data Exchange. In *Intelligent Technologies for Healthcare Business Applications* (pp. 19-47). Cham: Springer Nature Switzerland.
[2] Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024, October). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In 2024 15th International Conference on Network of the Future (NoF) (pp. 195-203). IEEE.
[3] Bansod, S., & Ragha, L. (2022). Challenges in making blockchain privacy compliant for the digital world: some measures. *Sādhanā*, *47*(3), 168.
[4] Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure. *arXiv preprint arXiv:2404.10659*.
[5] Bishwas, A. K., & Sen, M. (2024). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. *arXiv preprint arXiv:2411.09995*.
[6] Brattain, Walter, and John Bardeen. "Quantum and the Cybersecurity Imperative." *Dig tal Debates* (2022): 15.
[7] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and informatics*, *36*, 55-81.
[8] Ciulei, A. T., Crețu, M. C., & Simion, E. (2022). Preparation for the post-quantum era: a survey about blockchain schemes from a post-quantum perspective. Cryptology ePrint Archive.
[9] Fang-Fang Chua, Junaidi Abdullah, Mehdi Yadollahi, Mona Moradi, and Sima Ahmadpour. "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data." *Heliyon* 10, no. 10 (2024).
[10] Fauziyah, Z. W., & Tabassum, M. Quantum-Enhanced Cyber Security. *Innovative Computing and Communications: Proceedings of ICICC 2024, Volume 3*, 87.
[11] Kim, B. G., Wong, D., & Yang, Y. S. (2024). Quantum-Secure Hybrid Blockchain System for DID-based Verifiable Random Function with NTRU Linkable Ring Signature. *arXiv preprint arXiv:2401.16906*.
[12] Lazirko, M. (2023). Quantum computing standards & accounting information systems. *arXiv preprint arXiv:2311.11925*.
[13] Li, Z., Tan, T. G., Szalachowski, P., Sharma, V., & Zhou, J. (2021). Post-Quantum VRF and its Applications in Future-Proof Blockchain System. *arXiv preprint arXiv:2109.02012*.
[14] Michelagnoli, C. (2023). *Quantum-resistant Blockchain* (Doctoral dissertation, Politecnico di Torino).
[15] MILNOR, J., & KUMMER, N. (2024). QUANTUM-RESILIENT CRYPTOGRAPHIC PROTOCOLS FOR SECURING 5G NETWORKS: A MULTIDISCIPLINARY APPROACH.
[16] Raheman, F. (2024). Futureproofing Blockchain & Cryptocurrencies against Growing Vulnerabilities & Q-Day Threat with Quantum-Safe Ledger Technology (QLT). *Journal of Computer and Communications*, *12*(7), 59-77.
[17] Sanzeri, S. (2024). The Quantum Computing Threat. In *Counterterrorism and Cybersecurity: Total Information Awareness* (pp. 547-567). Cham: Springer International Publishing.
[18] Sinai, N. K., & In, Peter, H.,. (2024). Performance evaluation of a quantum-resistant Blockchain: a comparative study with Secp256k1 and Schnorr. *Quantum Information Processing*, *23*(3). https://doi.org/10.1007/s11128-024-04272-6