scientific reports

Check for updates

OPEN

Quantum secured blockchain framework for enhancing post quantum data security

Nalavala Ramanjaneya Reddy[1]✉, Supriya Suryadevara[2], K. Guru Raghavendra Reddy[3], Ramisetty Umamaheswari[4], Ramakrishna Guttula[5] & Rajitha Kotoju[6]

Quantum computing is an evolution of classical computing, capable of solving problems that are competitive enough to break the existing cryptographic primitives upon which current blockchain systems are based. Popular schemes like RSA, ECDSA, and SHA-256 can be compromised by quantum algorithms (Shor's and Grover's), raising questions about the security and trustworthiness of blockchain-based applications in finance, healthcare, and supply chains. Many current approaches focus on isolated aspects of the blockchain, such as cryptographic primitives or key exchange, without a comprehensive strategy that can guarantee end-to-end security in the face of a quantum threat. Finally, traditional consensus mechanisms such as Proof-of-Work and Proof-of-Stake are vulnerable to Sybil attacks, centralization, and leader-selection bias. When the adversary has access to a quantum computer, these issues become significantly worse. In this paper, we present QuantumShield-BC, a modular blockchain framework incorporating post-quantum cryptographic signatures, quantum key distribution (QKD), and a novel Quantum Byzantine Fault Tolerance (Q-BFT) consensus mechanism driven by quantum random number generation (QRNG) to address these challenges. QKD: The system supports tamper-proof key exchange, quantum-resilient consensus among validator nodes, and secure transaction signing. Experimental evaluation demonstrates that QuantumShield-BC achieves low consensus latency and high throughput, while providing perfect security against simulated attacks from Shor's and Grover's algorithms. The proposed framework eradicates the Sybil attack effectiveness up to 0%, eliminates replay and MITM vulnerabilities, and achieves an average throughput of over 7,000 transactions per second with 100 validators, orders of magnitude better than classical blockchain systems. The importance of each quantum part to the system's robustness is also demonstrated using an ablation study. With its unique ability to provide a post-quantum framework for high-assurance, general-purpose, scalable, and interoperable blockchain networks resistant to quantum-inspired attacks or quantum retrieval, QuantumShield-BC is practical for deployment in critical infrastructure and digital trust ecosystems where performance and a future-proof foundation are essential.

Keywords Post-quantum cryptography, Quantum key distribution, Quantum blockchain, Byzantine fault tolerance, Blockchain security

Quantum computers are advancing rapidly, posing one of the most significant threats to traditional cryptographic systems, which underpin the security of nearly all blockchains. Secure algorithms like RSA, ECDSA, and SHA-256 are at risk of quantum attacks using Shor's and Grover's algorithms in polynomial time. With the increasing adoption of blockchain in financial systems, healthcare, supply chains, and decentralized identity, researchers must also focus more on blockchain's inherent resilience to quantum-enabled attacks. Concerning quantum adversarial models, classical blockchains (even those augmented with modern cryptographic optimizations) cannot provide the same level of security.

Various researchers have explored some standard components of individual enhancement in post-quantum cryptography (PQC), quantum key distribution (QKD), and Blockchain technology enhancements. Carames and

[1]Department of CSE, RGM College of Engineering and Technology (Autonomous), Nandyal, A P, India. [2]DW Matrix Inc, 2440 Laura Mark Lane, Herndon, VA 20171, USA. [3]Department of CSE, Jayaprakash Narayan College of Engineering, Dharmapur, Mahabubnagar, Telangana, India. [4]Electronics and Communication Engineering, Vignan's Institute of Information Technology, Visakhapatnam, Andhra Pradesh 530049, India. [5]Department: Electronics and Communication Engineering, Aditya University, Surampalem, Andhra Pradesh 533437, India. [6]Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, (MGIT), Hyderabad 500075, India. ✉email: nalavala.ramanji@gmail.com

Lamas[1] studied PQC schemes for blockchain; Gao et al. Quantum blockchain models presented by[2] are based on the entanglement and DPoS mechanisms. Bhavin et al. Introduction of a hybrid model based on quantum blind signatures for security in healthcare[3]. Yet, these seem purely component-wise and fail to deliver insights into systematic, scalable, and modular quantum-safe solutions that span cryptographic, communication, and consensus-level quantum resilience.

This paper proposes a comprehensive blockchain framework, QuantumShield-BC, that fills these crucial blanks. This research aims to design, implement, and evaluate a post-quantum secure blockchain architecture comprising three critical components: post-quantum digital signatures for transaction signing and verification, QKD to provide secure peer-to-peer communication between all nodes of the network, and a new Q-BFT consensus mechanism based on QRNG to protect against malicious nodes. It is a scalable system that aims to counter key compromise, Sybil, replay, and man-in-the-middle attacks.

The main contributions of this work are that (i) it integrates PQC, QKD, and QRNG in an end-to-end manner in a single blockchain protocol, (ii) it minimizes trust in random numbers via QRNG-based consensus and leader election that achieves strong security for random numbers, and (iii) it fosters the gradual introduction of PQC by modular, layered architecture that allows any underlying blockchains to be converted to post-quantum blockchain systems incrementally. A comprehensive evaluation based on extensive simulation is also conducted, reinforcing the research contributions by quantifying the system's underpinning against quantum attacks, performance benchmarking, and ablation studies.

The remainder of the paper is structured as follows: Sect. 2 reviews the related literature on quantum-safe blockchain technologies, highlighting recent advancements and identifying research gaps. Section 3 presents the QuantumShield-BC framework, detailing its layered architecture, integrated quantum components, and proposed algorithms. Section 4 provides security benchmarking details. Section 5 presents experimental results, including the system setup, a comparative analysis with classical blockchains, security benchmarking against quantum attacks, a scalability assessment, and an ablation study of quantum components. Section 6 presents a detailed discussion of the findings and outlines the study's limitations. Section 7 concludes the paper and offers directions for future research.

Related work

The rise of quantum computing has intensified research into blockchain security, with a focus on quantum-resistant cryptography, secure key exchange, and consensus mechanisms. Existing works have individually explored post-quantum cryptosystems, QKD protocols, and blockchain enhancements. However, a gap remains in developing unified, scalable frameworks that integrate these components to address end-to-end security threats in the quantum era.

Quantum cryptography fundamentals

Quantum cryptography leverages quantum mechanical principles to ensure secure communication and data protection, forming the basis for quantum-secure blockchain systems. Studies have focused on the principles of quantum bits, quantum entanglement, and secure key generation for cryptographic resilience. Gnatyuk et al.[4] created a safe PRNG for Q-trit cryptography, pointed out evaluation technique shortcomings, and made recommendations for future tool development. Lone and Naaz[5]. examined studies on quantum cryptography, emphasizing post-quantum cryptography and key distribution, pointing out problems, and making recommendations for further advancements. Yang et al.[6] examined quantum computing, emphasizing its essential elements, difficulties, and potential avenues for further study in quantum networks, computers, and cryptography. Yang et al.[7] examined the problems and solutions of quantum cryptography, emphasizing the significance of QKD developments and future security requirements and constraints. Singamaneni et al.[8] examined quantum computing, its uses in key distribution and network security, and potential future paths in computational engineering. EI-latif et al.[9] proposed a quantum walk-based S-box technique for 5G-IoT security, highlighting the difficulties and potential applications of quantum cryptography in the future.

Post-quantum cryptographic techniques in blockchain

To counter the vulnerabilities of traditional cryptography against quantum attacks, researchers have proposed lattice-based and hash-based post-quantum cryptographic schemes tailored for blockchain applications. These include quantum blind signatures, secure hash functions, and digital signature algorithms that resist Shor's and Grover's algorithms. Lamas[1] examined post-quantum cryptosystems to secure blockchains. One of the limitations is the difficulty of implementation. Cryptosystem performance may be improved in future development. Dhar et al.[3] proposed a hospital blockchain architecture that utilizes quantum blind signatures to enhance data security. Future research might improve efficiency. Gao et al.[10] suggested an anti-quantum blind signature system for blockchain, emphasizing its effectiveness, safety, and potential advancements in cryptography. Yang et al.[11] evaluated Post-Quantum Cryptography (PQC), highlighting future efforts to improve security and highlighting gaps in existing research. Bansod and Ragha[12] examined blockchain privacy technologies, identified issues, and suggested further study to mitigate and enhance privacy. Zeydan et al.[13] presented a post-quantum signature technique with potential for future scaling that addresses quantum weaknesses in secure IoT blockchain networks. Radanliev[14]. examined IoT security, finds weaknesses, and suggests lattice-driven cryptography for post-quantum IoT security that is immune to quantum errors. Leng et al.[15] analysed post-quantum hash-based signatures for Internet of Things security, emphasizing issues, suggestions for further study, and implementation strategies. Tosh et al.[16] addressed the avoidance of misuse and effective integration with current technology by proposing quantum-resistant chameleon hash algorithms for redactable blockchain. Zhang et al.[17] examined SIKE's susceptibility to side-channel attacks, provided a defense, and recommended future security enhancements. Nejatollahi et al.[18] examined the energy-efficient polynomial multipliers of post-

quantum cryptography, highlighting speedups and providing ideas for future design improvements. Banupriya and Kottilingam[19] examined potential solutions to blockchain privacy concerns, such as deterministic keys and quantum-resistant algorithms, with a focus on Bitcoin.

Additionally, NTRU lattice-based identity proxy signatures have been investigated as quantum-resistant replacement methods for proxy signatures that secure identity delegation and privacy on blockchains[20]. Such schemes are significant for role-based access control in privacy-preserving decentralized systems.

Quantum key distribution (QKD) and hybrid protocols

QKD-based blockchain communication protocols provide tamper-proof key exchange using quantum channels. Some studies integrate QKD with classical post-quantum encryption to form hybrid cryptographic frameworks, enhancing blockchain security during transmission.

Dhar et al.[21] investigated how to improve IoT multimedia security using blockchain and quantum cryptography. Computational limitations are one type of limitation. Future research could improve security techniques. Gupta et al.[22] explained the blockchain's susceptibility to quantum computing, suggested a quantum-secure electronic voting mechanism, and outlined potential future research areas. Radanliev[23] examined how AI can improve quantum cryptography, discussed potential integration for digital security, and addressed related issues.

Chen et al.[24] addressed security issues, transaction capacity, and quantum threats by implementing a post-quantum PoW method for smart cities. Pedone et al.[25] addressed upcoming quantum difficulties by presenting a QKD software stack and simulator for safe incorporation into distributed infrastructures. Garcia et al.[26] proposed hybrid QKD-PQC systems that offer future-proof security improvements, albeit with performance trade-offs, for quantum-resistant TLS.

Quantum-secure blockchain architectures

Multiple architectures have been proposed to integrate quantum technologies into blockchain systems. These include quantum tokenization, quantum consensus protocols, and entanglement-based blockchain structures that resist quantum attacks while enhancing decentralization and immutability. Gao et al.[2] proposed using an quantum blockchain to improve efficiency and security while mitigating quantum attacks. Scalability may be enhanced via future research. Edwards et al.[27] examined the development of quantum blockchain, discussing sustainability, scalability, and efficiency, and discussing upcoming difficulties and unanswered concerns. Yang et al.[28] examined quantum blockchain for decentralized identity verification, highlighting issues and providing recommendations for creating future quantum-resistant infrastructure. Nilesh et al.[29] addressed the problems of quantum security, presented a paradigm for a quantum blockchain, and made recommendations for further research into the creation of quantum tokens.

Yang et al.[30] examined the differences between post-quantum and quantum blockchains, highlighting their challenges, security issues, and potential avenues for further blockchain development studies. Zohaib et al.[31] offered a Quantum-Blockchain-6G municipal management system that tackles scalability, integration, and cryptographic risks. Iovane[32] addressed the issues of randomness, democracy, and key distribution by introducing a quantum-based negotiating technique for blockchain validation. Abulkasim et al.[33] proposed a quantum-based blockchain sealed-bid auction protocol that offers extensive feature coverage and ensures security and anonymity.

Applications in iot, 5G/6G, and smart cities

Quantum-secure blockchain has significant applications in IoT networks, 5G/6G systems, and smart city infrastructures. Research highlights its use in ensuring secure data transmission, coordinating autonomous systems, and managing device authentication in complex environments. Chamola et al.[34] examined the security risks of quantum computing, its applications in 5G, and quantum-resistant cryptosystems for future networks. Bhatia and Sood[35] enhanced data accuracy, offered a quantum-inspired method for IoT optimization, and made recommendations for further study on algorithm improvement. Xu et al.[36] discussed the uses, challenges, and future research directions for quantum NFTs and security, while presenting a Web 3.0 platform powered by a quantum blockchain. Singamaneni et al.[37] addressed issues and demonstrated the efficacy of QHABE for future privacy security by proposing it for data integrity and access control in MEC.

Khan et al.[38] examined the security of UAVs, discussed the challenges of Post-Quantum Cryptography (PQC), and provided recommendations for future research on quantum-resistant algorithms. Tosh et al.[39] examined the use of quantum cryptography to protect cyber-physical systems, tackling the risks associated with quantum computing and potential advancements in security. Sicari et al.[40] examined 5G security and privacy options, discussing issues and potential avenues for research in IoT, blockchain, and fog computing. Chowdhury et al.[41] discussed the 6G concept, technology, challenges, and future research directions for enhanced capacity, security, and superior quality of service.

Lu and Li[42] proposed a lightweight authentication scheme for microgrids that is immune to quantum attacks and ensures both security and efficiency. Farouk et al.[43] examined the effects of blockchain and IoT on healthcare, emphasizing the enhancement of privacy, data security, and treatment efficiency. Pavithran et al.[44] examined blockchain for IoT, identified design issues, and found that device-to-device architecture increases throughput compared to solutions that rely on gateways. Tran et al.[45] identified design, motives, and ten archetypes for further study by doing a literature analysis to investigate BC-IoT integration.

Zhu et al.[46] suggested potential uses and highlighted lightweight protocols in their semi-quantum blockchain architecture for IoV security. Kumari et al.[47] examined the integration of blockchain and IoT in smart cities, highlighting obstacles and providing ideas for future research to ensure successful deployment. EL-Latif et al.[48] offered a quantum walk-based encryption method that addresses security issues and recommends enhancements

for safe Internet of Things connections. Gui et al.[49] examined the developments in 6G, offering an architecture, discussing obstacles, and making recommendations for future research areas.

Privacy, authentication, and identity management

Post-quantum authentication schemes, anonymous identity protocols, and privacy-preserving ledger structures have been developed to safeguard blockchain participant identities and prevent the tracking or misuse of sensitive data in a post-quantum world. Lone and Naaz[50] discussed blockchain cryptography, with particular attention on Bitcoin, Ethereum, and post-quantum cryptography requirements for next-generation blockchains. Awan et al.[51] highlighted the difficulties and recommended future transdisciplinary research, identifying and ranking the main obstacles to implementing quantum computing in software engineering. Trcek[52] proposed a blockchain-based approach to preserving digital cultural assets related to tourism, emphasizing energy efficiency and the potential for upcoming multidisciplinary advancements. Zeydan et al.[53] examined the use of PQC with blockchain networks for network service management, pointing out issues and recommending further study on safe orchestration.

Leng et al.[54] addressed technological, business, and operational issues, evaluated blockchain security, identified research gaps, and recommended future paths. Malina et al.[55] examined privacy techniques for II services, emphasizing post-quantum cryptography, issues, and upcoming PET development for the Internet of Things. Alkadri et al.[56] addressed blockchain problems by presenting a quantum-resistant deterministic wallet architecture; security analysis will be the primary focus of future research. Banupriya and Kottilingam[19] examined potential solutions to blockchain privacy concerns, such as deterministic keys and quantum-resistant algorithms, with a focus on Bitcoin.

Kumar et al.[57] offered IoF, a blockchain-based IoT forensic framework that is effective across various criteria for resolving cross-border concerns. Hassan et al.[58] examine the problems and potential applications of incorporating differential privacy into blockchain to address data privacy issues. Kumar and Bhalaji[59] proposed a peer-to-peer, blockchain-based architecture for ensuring data confidentiality and authentication in electronic government systems, with plans for future enhancements.

Current privacy-preserving data queries appear to be a suitable fit for integration into quantum-secure frameworks. Examples include efficient privacy-preserving spatial range queries over encrypted outsourced data to secure searchability in cloud systems[60] and privacy-aware spatial data queries in cloud computing environments. While such schemes primarily rely on classical cryptographic assumptions, incorporating these types of spatial data protection mechanisms into post-quantum blockchain environments is an important future research direction and highly beneficial for the goals of QuantumShield-BC at the same time.

Quantum threats and security challenges

Quantum computing introduces serious risks to blockchain confidentiality, integrity, and availability. Literature identifies specific attack vectors, including quantum-enabled Sybil attacks, transaction forgery, consensus manipulation, and countermeasures. Akter[5] examined studies on quantum cryptography, emphasizing post-quantum cryptography and key distribution, identified problems, and provided recommendations for further advancements. Yang et al.[30] examined the differences between post-quantum and quantum blockchains, highlighting their challenges, security issues, and potential avenues for further blockchain development studies. Shahwar et al.[7] examined the problems and solutions of quantum cryptography, emphasizing the significance of QKD developments and future security requirements and constraints. Sharma and Ramachandran[8] examined quantum computing, its uses in key distribution and network security, and potential future paths in computational engineering.

Kearney and Delgado[61] compared the risk exposure and efficacy of cryptographic protocols to examine the susceptibility of blockchain cryptocurrencies to quantum attacks. Sanka et al.[62] examined the uses, difficulties, cryptography, and potential research avenues of blockchain, with an emphasis on fields beyond cryptocurrency. Singh et al.[63] reviewed the security of blockchain-IoT systems, discussed mitigation strategies, and identified areas for further research. Zarrin et al.[64] examined how blockchain technology might help decentralize the Internet, emphasizing consensus algorithms and the challenges of integrating blockchain with the Internet.

Shrivas et al.[65] suggested a hybrid security framework for blockchain systems to mitigate security risks and enhance dependability. Shrivas et al.[66] examined blockchain security risks, identified adoption obstacles, and proposed a paradigm for enhanced security. Sharma and Lal[67] examined the security issues associated with IoT, discussed how blockchain technology may be improved, and provided recommendations for further study.

Integration with emerging technologies (AI, fog, edge)

The integration of quantum-secure blockchain with artificial intelligence, fog computing, and edge intelligence has been explored to enhance automation, trust, and performance in decentralized systems across both industrial and public sectors. Radanliev[23] examined how AI can improve quantum cryptography, discusses potential integration for digital security, and addresses related issues. Pandl et al.[68] examined the integration of AI and DLT, identified opportunities for further study, and suggested areas for convergent technologies in real-world systems. Honda and Otsuyama[69] experimented with DTTB signal delay for aircraft location, demonstrating the possibility of ISDB-T signal surveillance. Li et al.[70] investigated and suggested options for integrating blockchain technology for edge intelligence security and privacy in B5G networks. Bhushan et al.[71] examined blockchain technology, its security advantages, difficulties, and potential avenues for further study to enhance security and privacy.

Performance evaluation, tools, and optimization

Researchers have proposed simulation tools, benchmarked quantum-resilient algorithms, and introduced frameworks for evaluating blockchain scalability, latency, and energy efficiency in post-quantum environments. Xu et al.[36] discussed the uses, difficulties, and future research on quantum NFTs and security, while presenting a Web 3.0 platform powered by a quantum blockchain. Pedone et al.[25] addressed upcoming quantum challenges by presenting a QKD software stack and simulator for secure integration into distributed infrastructures. Wang et al.[72] proposed GSCS, a blockchain consensus method resistant to quantum errors, with a focus on security optimization in future research. Zhang et al.[17] examined SIKE's susceptibility to side-channel attacks, provided a defense, and recommended future security enhancements. Sinai and In[73] examined the Falcon algorithm for quantum-resistant blockchains, emphasizing its scalability and performance while recommending future algorithm selection strategies. Kumar et al.[74] created PRODCHAIN, a blockchain system that enhances the traceability of e-commerce products by utilizing lattice-based encryption and PoA consensus.

In addition, comparative analyses have recently demonstrated the effectiveness of quantum-secure blockchain architectures under various consensus protocols and employing different cryptographic primitives[75] in terms of trade-offs between transaction throughput, entropy quality, and attack resiliency.

Future trends, challenges, and open research directions

Future research in quantum-secure blockchain focuses on algorithmic efficiency, scalability, standardization, legal frameworks, and cross-domain integration to facilitate the global adoption of quantum-proof distributed systems. Zohaib et al.[31] offered a Quantum-Blockchain-6G municipal management system that tackles scalability, integration, and cryptographic risks. Ferdous et al.[76] identified gaps in blockchain consensus algorithms and proposed a decision tree for selecting the most suitable algorithms. Guo and Yu[77] examined security threats, solutions, and blockchain technology, emphasizing research trends and issues related to safe and scalable systems. Alfa et al.[78] examined blockchain integration, discussed IoT security issues, and offered low-tech cryptography fixes for next-generation decentralized systems.

Li et al.[79] examined the challenges and potential pathways for future growth in integrating blockchain technology with advanced civil aviation systems. Nasir et al.[80] examined the literature on cryptocurrencies and blockchain, found important study topics, and suggested future lines of inquiry. Wustmans et al.[81] evaluated blockchain innovation domains using trend and patent data, indicating ideas for further study and technological advancement. Raikwar et al.[82] examined the relationship between databases and blockchain, discussing the effects of each and offering ideas for additional research on integration.

Unlike previous quantum-secure blockchain designs that target isolated protocol improvements using post-quantum cryptography (PQC) for transaction signing or quantum key distribution (QKD) for key distribution, QuantumShield-BC enables an integrated, modular design integrating post-quantum cryptography, quantum key distribution, and quantum random number generation into a cohesive protocol stack, in contrast to[2,10,24], which study isolated components or limited hybrid models concerning secure classical communication, QuantumShield-BC proposes a fully integrated framework for quantum integrity in support of large-scale validators, providing seamless integration of tamper-proof QRNG and hybrid PQC-KEM key exchange protocols. The leveraging of QRNG for both leader selection and validator authentication (post-quantum) enables its consensus layer—Quantum Byzantine Fault Tolerance (Q-BFT)— to become inherently resistant to Sybil and predictability attacks. Compatibility with these strengths, along with performance benchmarking (such as 7000 + TPS while testing with 100 validators), demonstrates clear architectural and operational superiority over past quantum-aware systems.

Furthermore, employing post-quantum threshold cryptography has also been suggested to achieve stronger multi-party privacy in blockchain consensus settings[83], a direction that aligns with the quantum-secure multiparty computation used in our Q-BFT protocol.

Proposed framework

This paper proposes a QuantumShield-BC framework to provide end-to-end protection for blockchain systems in the quantum age. It incorporates post-quantum digital signatures at the protocol layer, quantum key distribution (QKD) at the network layer, and a Quantum Byzantine Fault Tolerance (Q-BFT) consensus mechanism based on quantum random number generation (QRNG) to provide end-to-end quantum attack resistance, scalability, fairness, and high transaction throughput.

Introduction to QuantumShield-BC

One of the challenges it poses for blockchain technology is that quantum computing has a disruptive capability concerning the cryptographic techniques we use, primarily traditional cryptographic methods such as RSA and ECC. However, the main disadvantage of all these classical methods is their vulnerability once large-scale quantum computers become available and can perform quantum attacks, such as Shor's algorithm, which efficiently breaks widely used public-key encryption schemes. It has led to the need for quantum-resistant blockchain architectures that ensure the security and safety of these decentralized methodologies against any future threats. Abstract: QuantumShield-BC is a quantum-secured blockchain framework that combines post-quantum cryptography (PQC) and quantum key distribution (QKD) to provide real-time security and resilience against quantum attacks over the long term.

The growing reliance on blockchain technologies for secure transactions, digital identity management, and decentralized applications (DApps) further underscores the necessity of quantum-resistant mechanisms as timelines for such attacks get shorter. However, this dependence on classical encryption introduces the risk of vulnerabilities in existing blockchain security models, as classical encryption can be solved in polynomial time with the aid of quantum computers. QuantumShield-BC addresses this issue by utilizing lattice-based post-

quantum digital signatures that can be seamlessly integrated into smart contracts, thereby significantly lowering the barrier to usage on existing protocols while ensuring signature security, even in a quantum adversarial setting. Moreover, Quantum Key Distribution (QKD) is implemented by creating a secure peer-to-peer communication channel to prevent eavesdropping and man-in-the-middle attacks.

Deterministic PRNGs pose a significant attack vector for classical blockchains, as they often lead to nonce prediction in digital signatures, which attackers can exploit. QuantumShield-BC further introduces quantum random number generation (QRNG), providing cryptographically secure random values for generating transaction hashes and executing smart contracts, as well as for the consensus mechanism, significantly augmenting entropy and security. This introduces random deviation, thereby strengthening the protection of classical cryptography against more predictable attacks.

In Fig. 1, in addition to securing each transaction, QuantumShield-BC replaces standard proof-of-stake (PoS) and proof-of-work (PoW) models with a Quantum-enhanced Byzantine Fault Tolerance (Q-BFT) consensus layer, bringing the same transactional protection to consensus mechanisms. By ensuring that validator nodes use post-quantum cryptographic authentication, adversaries cannot forge post-quantum authentication signatures or influence the consensus mechanism. The framework incorporates post-quantum secure multi-party computation (MPC) to preserve the resistance of node selection and block validation against classical and quantum-based cyber attacks.

By fusing classical cryptography robustness with quantum-safe innovations, QuantumShield-BC embodies a transformation in the landscape of blockchain security. The framework combines encryption with lattice-based digital signatures, QKD-secured communication, QRNG-enhanced randomness, and a quantum-resistant consensus protocol to create a next-generation, tamper-proof blockchain ecosystem. With the continued evolution of quantum technology, the fundamental need for a quantum-secured, decentralized system is heightened. In an era where quantum adversaries pose a potential risk, QuantumShield-BC provides the ideal future-proof solution, safeguarding the integrity of blockchain applications across multiple domains.

The workflow diagram of QuantumShield-BC, shown in Fig. 2, illustrates the complete lifecycle of a blockchain transaction secured against quantum threats. It begins with a user-initiated transaction digitally signed using post-quantum cryptography. The transaction is then securely transmitted across blockchain nodes using quantum key distribution (QKD). Validators authenticate the transaction using lattice-based signatures, followed by QRNG-based leader selection to ensure unbiased consensus initiation. The Quantum Byzantine Fault Tolerance (Q-BFT) protocol is executed for multi-party consensus, and upon reaching agreement, the block is finalized and appended to the blockchain. The user receives a confirmation, completing the secure and quantum-resilient transaction flow.

Table 1 presents the key notations used throughout the QuantumShield-BC framework, defining symbols related to transactions, cryptographic operations, consensus mechanisms, quantum processes, and validator interactions in blockchain.

Quantum-secure blockchain layer

The QuantumShield-BC builds a quantum-safe layer on top of the BC, protecting it from quantum adversaries across all three layers (transaction validation, block generation, and ledger) using PQ cryptographic methods. This layer provides the option to replace traditional cryptographic primitives with post-quantum digital

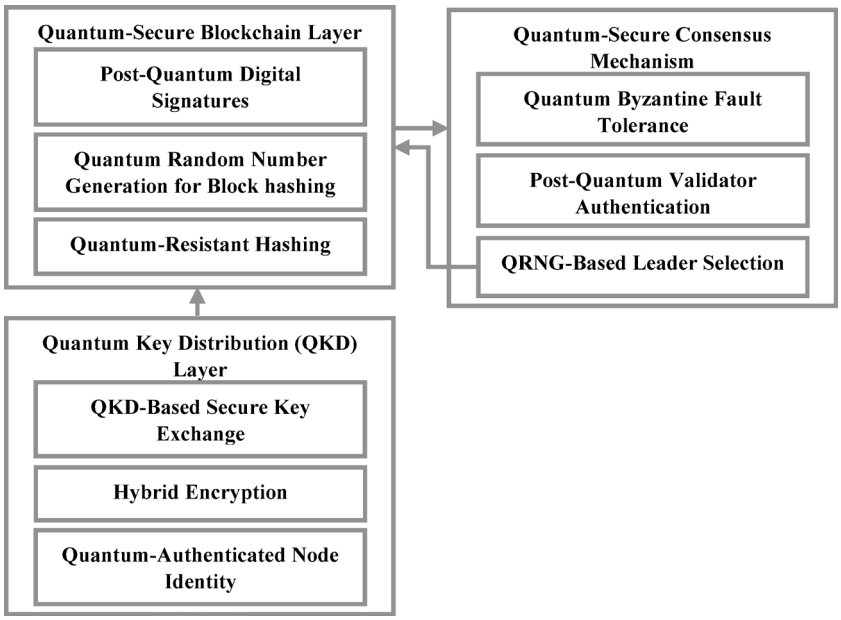

Fig. 1. System architecture of QuantumShield-BC with PQC, QKD, QRNG, and Q-BFT integration for secure blockchain operations.

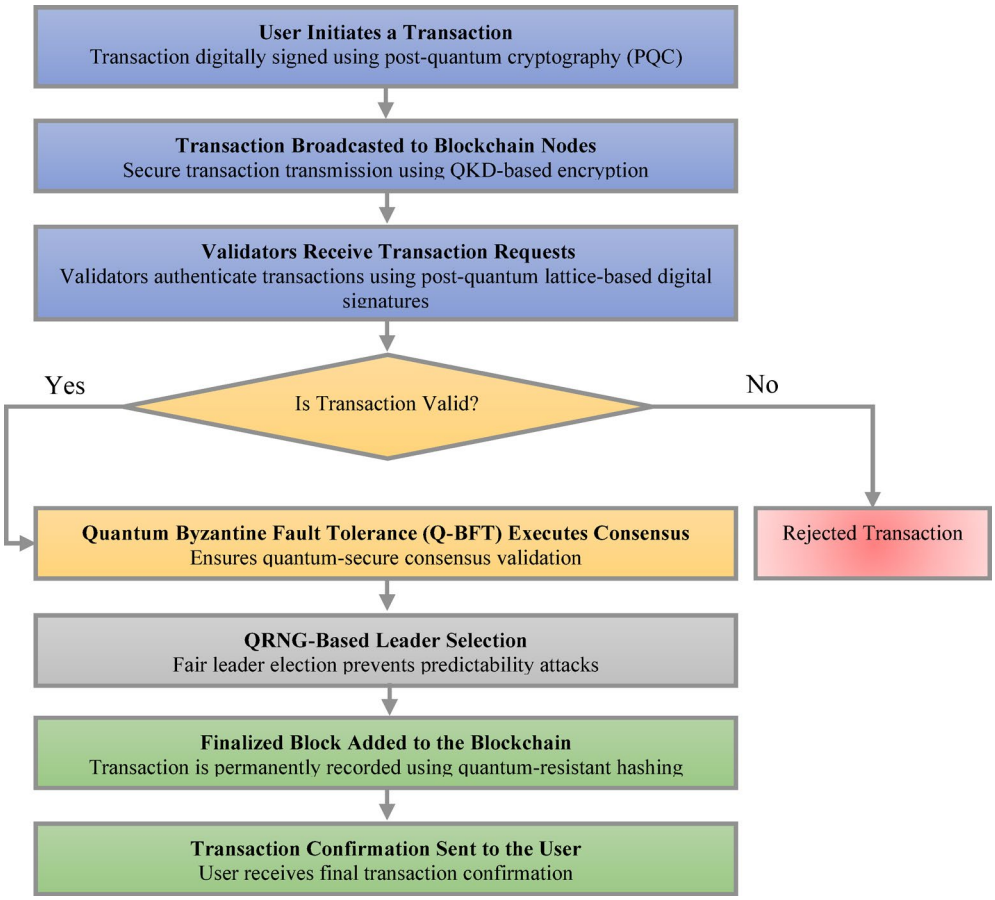

Fig. 2. Workflow diagram of QuantumShield-BC depicting end-to-end transaction processing with PQC-based signing, QKD communication, QRNG-driven leader selection, and Q-BFT consensus.

signatures and merge quantum-safe hash functions, aided by quantum random number generation (QRNG) to increase entropy in the blockchain. These changes further bolster the blockchain against key stealing, signature forgery, and entropy-based attacks that may become possible with the emergence of quantum CPUs.

Digital signatures are crucial in verifying the authenticity of a transaction and preventing third-party manipulation. Unlike classical cryptographic schemes like RSA or ECDSA, which rely on Shor's algorithm, QuantumShield-BC adopts a cryptographic stance when it comes to signing and verifying transactions, utilizing PQC algorithms such as CRYSTALS-Dilithium or Falcon post-quantum cryptographic (PQC) technology. The function for transaction verification is defined by

$$V\left(T\right) = Verify_{PQ}\left(S_k, H\left(T\right)\right) \tag{1}$$

Where $V\left(T\right)$ is the validity of the transaction, S_k is the post-quantum digital signature produced with the private key, and $H\left(T\right)$ is the cryptographic hash of the transaction. The function $Verify_{PQ}$ insures that the transaction is signed using a cryptosystem resistant to quantum computations before being included in the blockchain.

The security of the blockchain relies on more secure block generators, which allow data integrity to be secured while still maintaining immutability. QuantumShield-BC: Each block in QuantumShield-BC is tied to the previous one using a quantum-resistant hashing function. The hash of a block can be computed using a post-quantum secure hash function, such as SPHINCS + or Keccak, providing resistance to Grover's search algorithm. The computation of the block hash is given by

$$H\left(B_n\right) = Hash_{PQ}\left(B_{n-1} \parallel T_n \parallel S_n\right) \tag{2}$$

Where $H\left(B_n\right)$ is the hash of the block B_n, B_{n-1} is the hash of the previous block, T_n stands for the transactions that the block contains and S_n is a digital signature of the block. The function $Hash_{PQ}$ secures the hash process against quantum computing attacks.

One of the fundamental weaknesses of classical blockchains is the use of deterministic pseudo-random number generators (DPRNG), which can be vulnerable to entropy prediction attacks. To mitigate this, QuantumShield-BC leverages quantum random number generation (QRNG) to introduce high-entropy

Notation	Definition
T	Transaction initiated by the user in the blockchain network
S_k	A post-quantum digital signature is generated using a private key
$H\,(T)$	Cryptographic hash of the transaction
$V\,(T)$	Transaction validity function, verifying if the transaction is authentic using post-quantum cryptography
B_n	Newly created blockchain block containing validated transactions
$H\,(B_n)$	Cryptographic hash of the newly created block using quantum-resistant hashing
B_{n-1}	The previous block's hash is used to ensure blockchain immutability
P_i	Post-quantum public key of validator ii
T_i	Individual transactions in a block
V_{node}	Validator authentication status using post-quantum signatures
C_v	Consensus validation result ensures all transactions in a block are validated
K	The secret key is established using Quantum Key Distribution (QKD)
Q_S	The quantum state is transmitted from the sender node (Alice) in QKD
Q_R	Quantum state received by receiver node (Bob) in QKD
K_H	A hybrid encryption key is generated from QKD, and a post-quantum key encapsulation mechanism (PQC-KEM) is used
Q_C	Quantum consensus threshold, ensuring that a predefined fraction of validators reach agreement
V_{node_i}	An individual validator's vote contributes to the consensus process
τ	A minimum threshold is required to achieve consensus in Q-BFT
R_Q	Quantum entropy value generated by the Quantum Random Number Generator (QRNG)
QB	Sequence of quantum bits used for entropy generation in QRNG
P_i	Probability distribution of quantum states in QRNG
L	The leader node is selected for block finalization in the consensus process
T_B	Block confirmation time measures the total time to validate and finalize a block
T_{Shor}	Computational complexity of breaking a cryptographic key using Shor's Algorithm
T_{Grover}	Computational complexity of searching for a cryptographic hash using Grover's Algorithm
O_Q	Network overhead factor introduced by QKD encryption
B_Q	Bandwidth consumed during QKD-based encryption
B_C	Bandwidth consumed using classical encryption methods
M_C	Multi-party consensus verification function using quantum-secure cryptography

Table 1. Notations used in the QuantumShield-BC framework for quantum-secure blockchain operations.

randomness in cryptographic operations, such as block generation and nonce generation in smart contracts. We define the quantum entropy function by the following:

$$R_Q = H\,(QB) = -\sum p_i \log_2 p_i \tag{3}$$

Where R_Q is the quantum entropy, QB is the quantum bits, seqi is the probability for each quantum state. This feature guarantees that roll results are at random, free from the weak state seeds.

QuantumShield-BC also interfaces to a quantum-resistant Merkle tree for secure ledger storage. It is interesting to note that classic Merkle trees are based on hash-based proof of eligibility and could not be trusted alone in the presence of a quantum attack. The approach replaces traditional construction with a post-quantum Merkle tree where each node is signed through a lattice-based DS. The Merkle root calculation is given by

$$M_R = Hash_{PQ}\,(L_1 \parallel L_2 \ldots \parallel L_n) \tag{4}$$

Where M_R is the post-quantum Merkle root, and $L_1 \parallel L_2 \ldots \parallel L_n$ are the signed transaction leaves. By combining post-quantum signatures at every node layer, the transaction integrity is preserved against quantum adversaries.

QuantumHyperledger/QuantumShield-BC distinguishes itself as a tamper-resistant and robust decentralized ledger via the QRL by combining post-quantum digital signatures, hash hardening algorithms, and QRNG-based entropy. These improvements keep the blockchain operational and resilient to quantum-computing attack vectors as they emerge, meaning that QuantumShield-BC is the future of decentralized, secure applications.

Quantum key distribution (QKD) for secure peer-to-peer communication

QuantumShield-BC enhances blockchain security by utilizing Quantum Key Distribution (QKD) for secure peer-to-peer communication, thereby protecting the cryptographic keys exchanged between blockchain nodes against quantum attacks. Figure 3 illustrates that classic key-exchange mechanisms in cryptography, such as

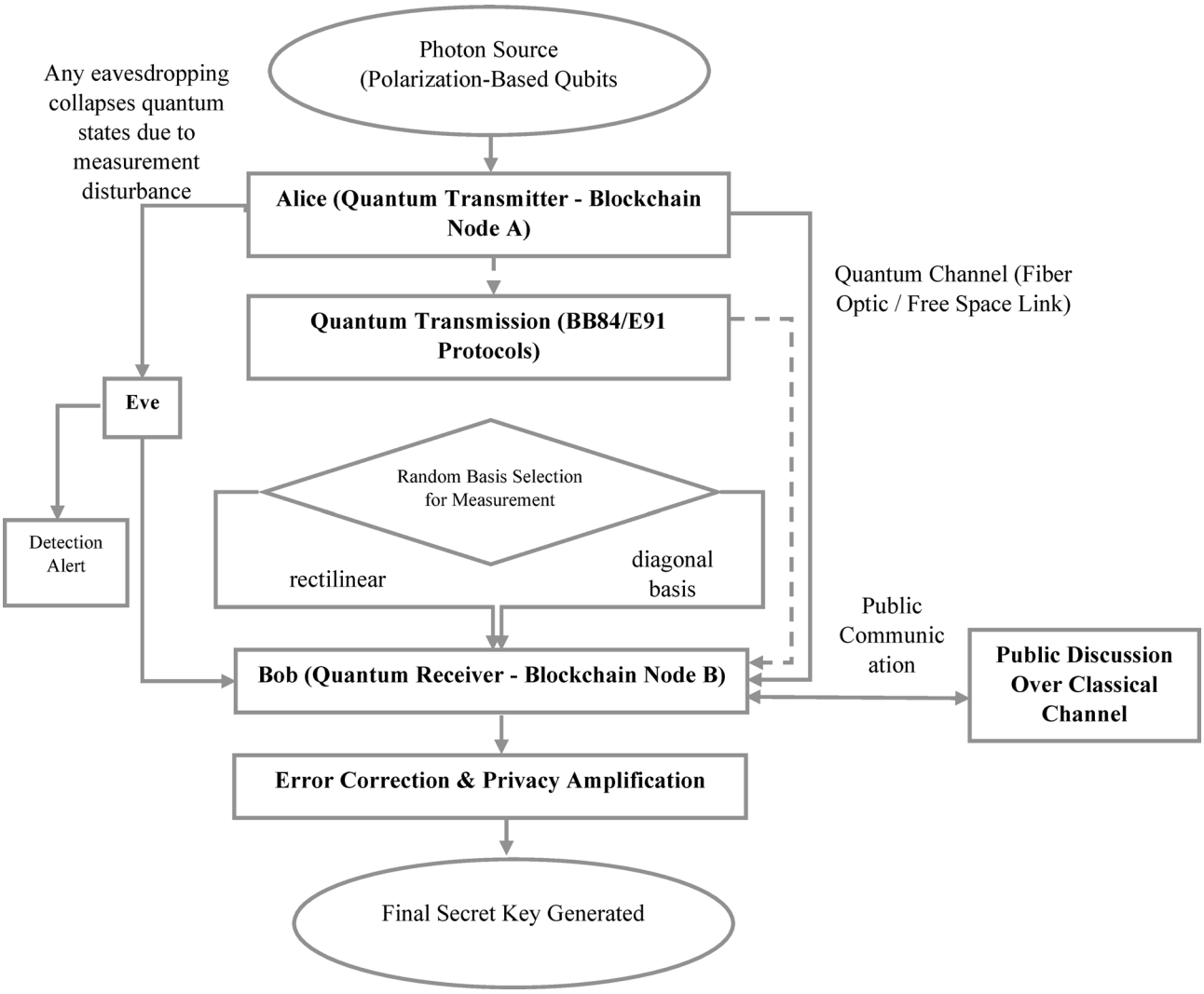

Fig. 3. Quantum key distribution (QKD) process flow illustrating secure key exchange between blockchain nodes using quantum states and classical reconciliation.

RSA and Diffie-Hellman, lack security against Shor's algorithm in traditional blockchain networks. QKD, on the other hand, can provide the generation and secure transmission of cryptographic keys based on quantum states, for which eavesdropping and key compromise are not feasible.

Protected by the no-cloning theorem and superposition in quantum mechanics, 7 QKD allows for an intercept-resilient exchange of cryptographic keys. QuantumShield-BC utilizes the BB84 protocol to exchange a key between the sender and receiver blockchain nodes via quantum state-encoded, polarized photons. The key exchange can then be mathematically described.

$$K = QKD_{BB84}\left(Q_S, Q_R\right) \tag{5}$$

Where K denotes the obtained secret key, Q_S is the quantum state transmitted by the sender node, and Q_R is the quantum state received by the recipient node. If the eavesdropper attempts to tap the quantum channel, the organization of the quantum state collapses, informing the communicating parties.

After the Quantum Key is exchanged successfully, it is applied to build a safe symmetric encryption channel between blockchain nodes. By encrypting, the transmitted blockchain data is kept private and secure. The encryption with the key generated by the QKD is defined as.

$$C = E_K\left(M\right) = M \oplus K \tag{6}$$

Where C is the encrypted message, $E_K\left(M\right)$ is encryption with the secret key K, and $\oplus$it is the XOR operation. The recipient decrypts the message with

$$M = D_K\left(C\right) = C \oplus K \tag{7}$$

Here $D_K(C)$ is the cryptographic decryption operation. Since the encryption key is securely exchanged by using the QKD, the communication is secure against quantum decoherence attacks.

QuantumShield-BC also included post-quantum cryptographic algorithms to supplement QKD in addition to secure key exchange. QKD provides the guarantee of key confidentiality, and post-quantum key encapsulation mechanisms (KEM), such as Kyber and FrodoKEM, are applied to achieve hybrid security for blockchain data exchange. The hybrid encryption, combining QKD and lattice-based encryption, aims to protect against vulnerabilities in one security layer by ensuring the other remains secure. Denote the hybrid key agreement function by

$$K_H = HybridKEM\left(K_{QKD}, K_{PQC}\right) \tag{8}$$

where K_H is the hybrid secret key for secure communication, K_{QKD} is the secret key generated from qa quantum source, and cap K sub cap P cap Q cap C is the key from a post-quantumkey encapsulation mechanism.

QKD-authentication based mechanisms also add a layer of security to blockchain communications. Validator nodes in the blockchain network are authenticated by quantum-secure key exchange method and can defend against Sybil and identity cues attacks. A key QKD-authenticated identity hash is generated in each validator node, as follows:

$$H_V = Hash_{PQ}\left(ID_V \parallel K\right) \tag{9}$$

Where H_V is the identity of the authenticated validator, ID_V is the unique identifier for the node, and K is the QKD-derived key. This allows consensus and block validation only by nodes that are quantum-authenticated.

By using QKD for secure key exchange, QuantumShield-BC Se mitigates the risks associated with classical key exchange protocols and adds layer of post-quantum encryption. QKD is integrated with hybrid encryption schemes and QKD-authenticated node validation to secure the blockchain against classical and quantum attack fronts. With this, QuantumShield-BC establishes a channel for communication that will remain for the decentralized networks of the blockchain's future.

Practical deployment considerations

Theoretically unbreakable, Quantum Key Distribution (QKD) provides secure key exchange; however, practical implementations raise several issues. The significant challenges include the high hardware costs of quantum photon sources, detectors, and synchronization systems, as well as channel loss over long distances, particularly when the channel is a fiber-optic or free-space link. In addition, the scalability of QKD is limited for blockchain networks because of the requirement of individual quantum channels among the nodes. QuantumShield-BC addresses these concerns, supporting a modular integration that allows hybrid PQC-KEM mechanisms to supplement QKD in situations where its deployment is not feasible. Future improvements will investigate satellite-based QKD or trusted node relays to eliminate losses caused by distance and increase the practical applicability of the system.

Quantum-secure consensus mechanism

Introducing a quantum-secure consensus, QuantumShield-BC enhances the security of the blockchain by utilizing post-quantum cryptographic algorithms with Byzantine Fault Tolerance (BFT), as illustrated in Fig. 4. Classic consensus schemes, such as PoW and PoS, are based on cryptographic algorithms that are susceptible to quantum attacks (e.g., Shor's algorithm, which can crack RSA and ECC). It is ensured that the proposed Q-BFT-based protocol is secure for block validation and transaction verification even in the quantum environment.

In QuantumShield-BC, each validator node is required to verify transactions with a post-quantum cryptographic signature before contributing to the consensus. The authentication is formed using lattice-based digital signatures, so malicious parties cannot forge the validator credentials. The function is the validator authentication function assigned by where quale lector.

$$V_{node} = Verify_{PQ}\left(S_v, H\left(B\right)\right) \tag{10}$$

where V_{node} denotes the validator at the position 1the validator's authenticating status at the position, S_v is the post-quantum digital signature produced by the validator at the 11 st position, and cap H of cap B is the cryptographic hashrecord of the candidate block. This prevents the Byzantine Army from joining the consensus by only accepting quantum-resistant signatures to verify a block.

This consensus decision function collects multiple signatures of validator nodes, and the block is appended to the blockchain only if a large enough set of quantum-authenticated validators accept it. This is mathematically modeled as:

$$C_V = \sum {}^{n}_{i-1} Sign_{PQ}\left(T_i, P_i\right) \tag{11}$$

Where C_V is the consensus declared voting result, T_i is any individual transaction of a block, and P_i is the post-quantum public key of the validator i. QiatumShield-BC can defend against attacks such as quantum Sybil attacks and signature forging by implementing this quantum-secure aggregation process.

QuantumShield-BC uses quantum-resistant threshold cryptography to guarantee that block finalization is not possible unless a sufficiently large number of validators participate. The block confirmation horizon can be derived as follows:

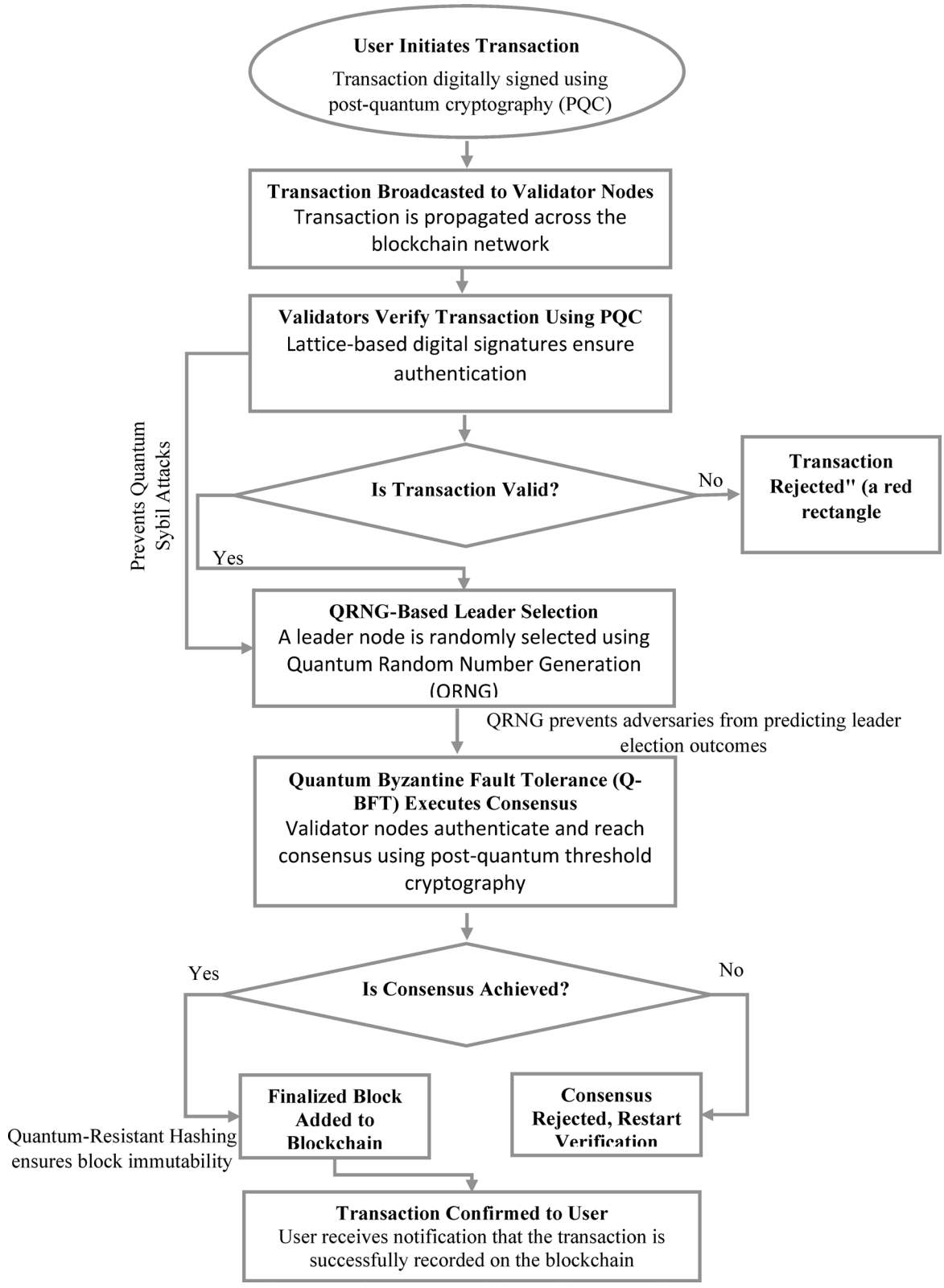

Fig. 4. Quantum byzantine fault tolerance (Q-BFT) consensus flowchart showing validator authentication, QRNG-based leader selection, and multi-party consensus execution.

$$Q_C = \frac{1}{n} \sum {}^{n}_{i-1} V_{node_i} \geq \tau \tag{12}$$

Where Q_C is a quantum consensus threshold, V_{node_i} is the verification status of single validator nodes, and τ is a minimum threshold required for consensus. This maintains decentralization in the blockchain and thwart quantum bloc adversaries attempts to effect block finalization.

Leader election in consensus protocols is generally susceptible to predictability attacks. QuantumShield-BC addresses this challenge by using QRNG for unbiased leader election. The leader selection function that uses QRNGs has the form of

$$L = argmax\,(R_Q \bmod n) \tag{13}$$

Where L is the leader node, R_Q is the quantum-generated random number, and nn denotes the total number of the validators that participate in the procedure. Thanks to the use of QRNG, QuantumShield-BC makes sure leader election mysterious and non-manipulatable.

In QuantumShield-BC (QSB)-QRNGs are not augmentations of conventional PRNGs(2), but separated quantum entropy sources based on physical behavior of quantum systems. QRNGs, however, take their source of randomness from fundamentally unpredictable quantum processes (such as photon phase noise, radioactive decay, or vacuum fluctuations), in contrast to PRNGs, which rely on deterministic algorithms and seed value(s). Such sources are physically uncloneable and therefore they cannot be mimicked so that they not only quantum mechanically sounds more secure than classical random numbers, but they are not just probabilistically secure (cloning the classical data is a typical classical attack), but they are also physically verifiable. To avoid being attacked by entropy predictability, QuantumShield-BC employs QRNG generated values for leader selection, nonce generation and consensus randomness. Randomness is fed through quantum-proof extractors (such as Trevisan's extractor) for entropy extraction and uniformity, making the output cryptographically usable (see[20] for specifics on the entropy extraction process).

For additional security, the architecture includes a hybrid consensus validation scheme with the quantum multiparty computation (QMPC). This way, several validators can cooperate in validating transactions and without revealing too much about the sensitive cryptographical information. The centralized verification process over multi-party consensus is defined as

$$M_C = \prod {}^{m}_{i-1} Verify_{PQ}\,(S_i, H\,(T_i)) \tag{14}$$

.

Where M_C is the consensus verification output, S_i is the post-quantum digital signature of the validator i, and $H\,(T_i)$ is the CM-Hash of the transaction T_i. QuantumShield-BC achieves privacy preserving and quantum-safe consensus validation by using QMPC.

By combining QRPoA with PQC-threshold signature, QRNG leader selection, and QMPC consensus validation, QuantumShield-BC is secure against classical and quantum adversarial attacks. This method allows decentralized blockchain systems to achieve the tamper-proof and security in the quantum scale era because of large-scale quantum computer, and it makes QuantumShield-BC as a future next-generation blockchain consensus framework.

Implementation of quantumshield-BC prototype

The development of the quantumshield-bc prototype takes place in several stages to enable a step-by-step integration of quantum-safe blockchain components. In addition to a post-quantum cryptography (PQC), the OmegaLedger prototype includes quantum key distribution (QKD), quantum-secure consensus algorithms, and quantum random number generation (QRNG) as solutions to boost blockchain immunity against quantum attacks. At each stage, critical security concerns, that is transaction verification, block creation, consensus assurance, and secure p2p communication, are addressed. The main development steps of the prototype are described below.

The first phase of development focuses on incorporating post-quantum digital signatures to transition from classical signatures, RSA and ECC, to post-quantum. QuantumShield-BC uses lattice-based cryptographic methods CRYSTALS-Dilithium and Falcon by signing transactions, ensuring secure transactions. Where the transaction validation function is the formulation of:

$$V\,(T) = Verify_{PQ}\,(S_k, H\,(T)) \tag{15}$$

Where $V\,(T)$ is the transaction validity, S_k is the post-quantum digital signature of the sender of the transaction and $H\,(T)$ is the cryptographic hash of the transaction. This prevents non quantum-resistant signatures from being added to the blockchain.

In the second stage, the communication between nodes are being insured using QKD, where nodes use QKD to share an encrypting/decrypting key for the block chain communication. This also closes weaknesses in traditional key exchange schemes like Diffie-Hellman and RSA. The pairwise key agreement between nodes is specified as:

$$K = QKD_{BB84}\,(Q_S, Q_R) \tag{16}$$

Where K is the parties' secret key, Q_S is the quantum state sent by the sender, Q_R and is the received quantum state of the receiver. If the key is intercepted by an enemy, he will change the quantum state; therefore, key compromise will be noticed immediately.

To derive tamper-proof block generation, QuantumShield-BC employs quantum-resistant hashing for connecting the blocks together within the blockchain. The block hash calculation uses SPHINCS + or Keccak, which are resistant to Grover algorithm attacks. The hash function used to create a block is defined as:

$$H(B_n) = Hash_{PQ}(B_{n-1} \parallel T_n \parallel S_n) \tag{17}$$

Where $H(B_n)$ is a hash to the newly created block B_n, B_{n-1} to the previous block, T_n to the transactions in the block; and S_n is the post-quantum block signature. This ensures that the data cannot be changed and that it will be resistant to quantum attacks.

The upcoming developments will be directed towards the implementation of Quantum Byzantine Fault Tolerance (Q-BFT), a post-quantum consensus protocol that supersedes old-fashioned PoS and PoW mechanisms. It was also observed that validator nodes prove their identity with quantum-secure signatures before joining the consensus. The function for the validator authentication is defined as

$$V_{node} = Verify_{PQ}(S_v, H(B)) \tag{18}$$

Where V_{node} denotes validator certification, S_v is the post-quantum digital signature of the validator, and $H(B)$ is the cryptographic hash of the block proposal. Only verified QSC validators are allowed to participate in the consensus.

To achieve the fair leadership selection in consensus, the Quantum Random Number Generation (QRNG) is implemented in order to remove the bias and predictability during the leader selection. We model the leader election as

$$L = argmax(R_Q \bmod n) \tag{19}$$

Where L is the leader, R_Q is the random number generated by quantum, and n is the number of available validators. QuantumShield-BC relies on QRNG to achieve fair and tamper-free leader election free from pseudo randomness source such as pseudo-random number generator and pseudo-random counterparts.

The last stage comprises the installation of QuantumShield-BC prototype on a testbed for testing its security and performance as well as its defence to quantum attacks. The security of transaction verification, consensus and block generation is proven with quantum attack simulation on quantum computing simulator (i.e., IBM Qiskit or Google Cirq). The integrity of the global blockchain is decided by the multi-party consensus verification function, which is denoted as:

$$M_C = \prod {}_{i-1}^{m} Verify_{PQ}(S_i, H(T_i)) \tag{20}$$

Where M_C is the consensus validation status, S_i is the digital signature of validator post-quantum i, and $H(T_i)$ is the hash cryptographic value of transaction T_i. This multi-party validation prevent any but quantum-secure transactions from entering the blockchain.

Incorporating PQ digital signatures, PKI free QKD, quantum-secure hashing, and QRNG-based consensus, the QuantumShield-BC prototype provides an ultra-resilient and temper-proof blockchain platform. By the systematic evolution and incorporation of quantum-safe technology into a blockchain, so that the blockchain is operational, scalable and robust against newly emerging quantum scientific threats, a future user facing quantum-safe blockchain 2.0 can be achieved.

Proposed algorithms

This section presents the core algorithms underpinning the QuantumShield-BC framework. Each algorithm addresses a specific component of the system, including transaction authentication, secure key exchange, quantum-safe consensus, and randomness generation. Together, these algorithms ensure end-to-end quantum resilience, enabling secure, scalable, and tamper-proof blockchain operations in the presence of emerging quantum computational threats.

Input: Transaction T, private key S_k

Output: Validated transaction $V(T)$

1. Compute hash of transaction: $H(T) = Hash_{PQ}(T)$
2. Generate post-quantum signature: $S = Sign_{PQ}(S_k, H(T))$
3. Attach signature to transaction: $T' = (T, S)$
4. Verify signature using public key P_k: $V(T) = Verify_{PQ}(P_k, S, H(T))$
5. If $V(T) = True, accept\ transaction$; else, reject.

Algorithm 1. Post-quantum digital signature algorithm.

Algorithm 1 secures blockchain transactions using post-quantum digital signatures. It begins by hashing the transaction data and generating a signature with a private key using a post-quantum algorithm. The signature is then attached to the transaction and verified using the corresponding public key. This ensures that the transaction is authentic, tamper-proof, and resistant to quantum-based attacks.

Input: Quantum states Q_S (sent state), Q_R (received state)
Output: Secure cryptographic key K

1. Alice (Sender) generates quantum bits: $Q_S = GenerateQuantumBits()$
2. Alice randomly selects polarization bases (rectilinear or diagonal).
3. Alice sends Q_S over the quantum channel to Bob (Receiver).
4. Bob measures Q_R using randomly chosen bases.
5. Bob and Alice communicate classically to compare measurement bases.
6. Retain only matching basis results to form raw key K_{raw}
7. Perform error correction and privacy amplification: $K = SecureKeyExtraction(K_{raw})$
8. Output K as the final QKD-generated key for encryption.

Algorithm 2. Quantum key distribution (QKD) algorithm.

Algorithm 2 enables secure key exchange between blockchain nodes using quantum key distribution. The sender transmits quantum states, which the receiver measures using random bases. Through classical communication, both parties compare bases and retain matching bits to form a raw key. After error correction and privacy amplification, a final secure key is established, ensuring tamper-proof communication against quantum adversaries.

Input: Block data B_n, previous block hash B_{n-1}
Output: Secure hash $H(B_n)$

1. Concatenate block components: $D = B_{n-1} \parallel T_n \parallel S_n$
2. Apply post-quantum secure hash function: $H(B_n) = Hash_{PQ}(D)$
3. Return $H(B_n)$ as the quantum-resistant hash.

Algorithm 3. Quantum-resistant hashing algorithm.

Algorithm 3 generates a quantum-resistant hash for a blockchain block using post-quantum cryptographic functions. It concatenates the current block data with the previous block's hash to form the input. A secure hash function, such as SPHINCS + or Keccak, is then applied to produce a tamper-proof hash. This ensures the integrity and immutability of the blockchain ledger.

Input: Transaction T, digital signature S_k, public key P_k
Output: Boolean value $V(T)$ indicating transaction validity

1. Extract transaction data and signature: $(T, S) \leftarrow Extract(T)$
2. Compute hash of the transaction: $H(T) = Hash_{PQ}(T)$
3. Verify the digital signature: $V(T) = Verify_{PQ}(P_k, S, H(T))$
4. Return $V(T)$:
   If $V(T) = True, accept\ transaction.$
   Otherwise, reject transaction.

Algorithm 4. Transaction validation algorithm.

Algorithm 4 performs transaction validation using post-quantum cryptographic techniques. It extracts the transaction and its digital signature, computes the hash of the transaction, and verifies the signature using the sender's public key. If the verification is successful, the transaction is accepted; otherwise, it is rejected. This process ensures that only authentic and quantum-secure transactions enter the blockchain.

Input: Quantum bit sequence QB

Output: Quantum-generated random number R_Q

1. Generate quantum bit sequence: $QB = GenerateQuantumBits()$
2. Measure quantum states to obtain raw entropy source: $R_{raw} = Measure(QB)$
3. Apply randomness extraction function: $R_Q = ExtractEntropy(R_{raw})$
4. Ensure uniform distribution of randomness: $R_Q = R_Q \ mod \ M$
5. Return R_Q as the final quantum-randomized number.

Algorithm 5. QRNG-based nonce and randomness generation algorithm.

Algorithm 5 generates quantum-secure random numbers using a quantum random number generator (QRNG). It begins by producing a sequence of quantum bits, which are measured to obtain raw entropy. A randomness extraction function is then applied to refine the output. The resulting value provides true, unpredictable randomness used for nonce generation, leader selection, and other critical blockchain processes.

Input: Quantum entropy R_Q, number of validators n

Output: Selected leader L

1. Generate a quantum random number: $R_Q = QRNG()$
2. Map the random number to a validator index: $L = R_Q \ mod \ n$
3. Broadcast leader selection result to all nodes.
4. If L is an active validator, confirm selection; else, repeat step 1.
5. Return L as the final selected leader.

Algorithm 6. QRNG-based leader selection algorithm.

Algorithm 6 selects a consensus leader using quantum-generated randomness. A random number is generated via a quantum random number generator (QRNG) and mapped to a validator index by taking the modulus with the total number of validators. If the selected validator is active, it is assigned as the leader. This approach ensures fair, unpredictable, and tamper-proof leader selection.

Input: Validator authentication V_{node}, transaction set T_i, consensus threshold τ

Output: Consensus result C_V

1. Each validator verifies transactions using post-quantum cryptography: $V_{node_i} = Verify_{PQ}(S_i, H(T_i))$
2. Validators broadcast verification results to the network.
3. Collect votes from all participating validators:
$$Q_C = \frac{1}{n}\sum_{i-1}^{n} V_{node_i}$$
4. Check if consensus threshold is met:
   If $Q_C \geq \tau$, consensus is achieved: $C_V = True$
   Else, consensus fails: $C_V = Flase$
5. If $C_V = True$, proceed with block finalization.
6. Return C_V as the consensus result.

Algorithm 7. Quantum byzantine fault tolerance (Q-BFT) consensus algorithm.

Algorithm 7 establishes consensus using the Quantum Byzantine Fault Tolerance (Q-BFT) mechanism. Each validator verifies transactions using post-quantum signatures and broadcasts its result. The system aggregates validator votes and compares them against a predefined threshold. If the number of valid votes meets or exceeds this threshold, consensus is achieved and the block is approved; otherwise, consensus fails and is retried.

Input: Post-quantum signatures S_i, transaction hashes $H(T_i)$
Output: Consensus decision M_C

1. Each validator independently verifies transaction signatures:
$$V_{node_i} = Verify_{PQ}(S_i, H(T_i))$$
2. Validators share verification results using secure quantum channels.
3. Aggregate validation votes using multi-party computation:
$$M_C = \prod_{i-i}^{m} V_{node_i}$$
4. Determine final consensus decision:
   If $M_C = 1$, consensus is reached.
   Else, consensus fails, and the transaction is rejected.
5. Return M_C as the final consen**sus decision.**

Algorithm 8. Post-quantum multi-party consensus verification algorithm.

Algorithm 8 performs post-quantum multi-party consensus verification among validators. Each validator independently verifies transaction signatures using post-quantum cryptography. The results are securely shared and aggregated using quantum-secure multi-party computation. If all verifications are successful, consensus is confirmed. Otherwise, the transaction is rejected. This ensures tamper-resistant validation across distributed nodes in a quantum-secure blockchain environment.

Input: Validated block B_n, previous block hash B_{n-1}, consensus result C_V
Output: Updated blockchain ledger

1. Check consensus status:
   If $C_V = False$, reject block and terminate process.
   Else, proceed to block finalization.
2. Compute block hash using quantum-resistant hashing:
$$H(B_n) = Hash_{PQ}(B_{n-1} \parallel T_n \parallel S_n)$$
3. Link the new block to the blockchain:
$$B_n \leftarrow (H(B_n), B_{n-1}, T_n, S_n)$$
4. Append B_n to the blockchain ledger.
5. Broadcast the finalized block to all network nodes.
6. Return updated blockchain ledger.

Algorithm 9. Block finalization and addition algorithm.

Algorithm 9 finalizes and appends a validated block to the blockchain. It first checks whether consensus has been achieved. If valid, the block data is hashed using a post-quantum secure hash function and linked to the previous block. The finalized block is then added to the blockchain and broadcast to the network, ensuring integrity, immutability, and resistance to quantum-based tampering.

Input: Validator requests, QKD-generated keys K
Output: Secure validator communication status

1. Establish a quantum-secure channel using QKD:
$$K = QKD_{BB84}(Q_S, Q_R)$$
2. Each validator node authenticates its identity using post-quantum signatures:
$$H_V = Hash_{PQ}(ID_V \parallel K)$$
3. Verify validator identity against the distributed ledger:
   If H_V matches the registered validator hash, proceed.
   Else, reject the node as a potential Sybil attack.
4. Encrypt validator communications using QKD key K:
$$C = E_K(M) = M \oplus K$$
5. Monitor for quantum-based replay attacks:
   Ensure each transaction nonce is uniquely generated using QRNG.
   If duplicate nonces are detected, reject the transaction.
6. Broadcast security status updates to the blockchain network.
7. Return secure validator communication status.

Algorithm 10. Quantum-aware network security algorithm.

Algorithm 10 secures validator communication using quantum-aware techniques. It begins by establishing a key via quantum key distribution, followed by validator authentication using post-quantum signatures. All messages are encrypted using the QKD-derived key. Replay and Sybil attacks are mitigated through QRNG-generated nonces and identity checks. The system ensures quantum-resilient, authenticated, and tamper-proof communication across blockchain nodes.

Performance evaluation metrics

Performance Evaluation The performance of QuantumShield-BC is tested through a number of essential performance criteria to measure its security, efficiency, and scalability against quantum threats. The assessment considers transaction validation latency, consensus throughput, cryptographic entropy, and benchmark quantum resistance. These benchmarks guarantee QuantumShield-BC maintains high speed operation and uses post-quantum cryptographic (PQC) primitives, QKD, Quantum Byzantine Fault Tolerance (Q-BFT), and QRNG.

One of the primary performance metrics is the transaction validation time, which measures the time to validate a transaction using post-quantum digital signatures as opposed to the case of standard signatures. The validation time T_v of a transaction can be defined as

$$T_v = T_{Sign} + T_{Verify} \tag{21}$$

Where T_{Sign} is the time to compute a post-quantum signature, and T_{Verify} is the time to verify the signature based on the underlying post-quantum cryptographic (PQC) scheme. Since lattice-based signatures (e.g., CRYSTALS-Dilithium, Falcon) increase the computational overhead as compared to ECC, we strive to choose PQC schemes with the least latency, to achieve the most efficient QuantumShield-BC.

Another essential metric to consider is consensus throughput, the number of transactions that can be handled per second and that are secure against quantum adversaries. The performance (throughput) of the Q-BFT consensus mechanism can be defined as

$$T_{Q-BFT} = \frac{N_T}{T_C} \tag{22}$$

Where T_{Q-BFT} is the number of transactions (transactions per second), N_T is the number of transactions validated , $cap\, T\, sub\, cap\, C\, is\, the\, total\, running\, time\, for\, forming\, a$decision. Utilizing Quantum-Secure Multi-Party Computation (QMPC), the consensus mechanism ensures secure transaction validation, whilst minimizing the computational overhead caused by post-quantum cryptographic primitives.

QuantumShield-BC, in selecting specific PQC algorithms, makes a balance between computational efficiency and post-quantum security guarantees. We considered both CRYSTALS-Dilithium and Falcon schemes as digital signatures, both of which are NIST post-quantum cryptography standardization finalists. CRYSTALS-Dilithium provides excellent security guarantees and high confidence in being resilient against lattice-based attacks; however, Falcon supports very small signatures with much faster verification speeds, making it more advantageous for high-throughput blockchain environments. We used Falcon for consensus authentication in our prototype, due to its fast signature verification time (1.5 ms per signature), and we opted for Dilithium for transaction signing, where the signature size constraint is less critical. The combination of the two reduces both speed and storage overhead used by the two to perform blockchain operations. We found that total conversion to Dilithium increases validation time by 18%, but this also improves resistance to some attacks based on side-channels[17]. These design choices exemplify how modular PQC algorithm customization can align security-performance trade-offs for real systems.

An entropy assessment of QRNG-based blockchain functions is conducted to evaluate the quality of randomness applied to leader selection, nonce generation, and cryptographic key generation tasks. The Shannon entropy formula determines the quantum entropy value, cap R sub cap Qalue, R_Q, is determined by the Shannon entropy formula:

$$R_Q = H\,(QB) = -\sum p_i \log_2 p_i \tag{23}$$

Where QB is the bit pattern ggenerated from the quantum, and p sub i is the probability distribution of the uantum state. Higher entropy values imply better randomness, increased security for cryptographic keys, and greater unpredictability in blockchain operations.

Equation (23) computes the Shannon entropy value derived from quantum bitstreams generated by a QRNG device. Here, the entropy H(Q)= $-\sum {}_i p_i log_2\, p_i$ quantifies the uncertainty of measured quantum states. Unlike classical bitstreams, the probabilities p_i are obtained from quantum state measurement results, ensuring they reflect hardware-derived unpredictability rather than algorithmic randomness.

In order to measure the quantum resistance of blockchain transactions, we analyze security by running simulations using Shor's Algorithm to compare the resistance of classical versus post-quantum cryptography. The time complexity for solving the cryptographic key with Shor's algorithm can be expressed as: $ where ta is the time to guess a while Shor's key is around Inf:.

$$T_{Shor} = O\left(log^3 N\right) \tag{24}$$

Where $N\ indicates\ the\ length\ of$ the cryptographic key in bits, since RSA/ECC keys will be broken in polynomial time by Shor's algorithm, QuantumShield-BC is based on post-quantum cryptographic primitives like Kyber, FrodoKEM, and SPHINCS + that are secure against quantum decryption.

Another relevant measure is the network overhead due to QKD-based encryption. However, QKD's secure key distribution may lead to extra bandwidth consumption, where cap O sub cap Q is the overhead factor.

$$CapO_Q = \frac{B_Q}{B_C} \times\ 100\% \tag{25}$$

Where B_Q denotes the bandwidth cconsumption of QKD-based encryption, a nd B_C denotes classical encryption. QuantumShield-BC is lightweight, and the overall communication efficiency is not degraded as QKD key exchange rates are improved and unnecessary quantum-state transmissions are suppressed.

The last evaluation measure is the CTT: the time it takes the network to agree upon a new block and place it on the blockchain. This is given by

$$T_B = \frac{T_{Comm} + T_{Q-Rand}}{V_C} \tag{26}$$

Where T_B is the block confirmation time, T_{Comm} denotes the time for communication among validators, T_{Q-Rand} is the time for quantum-safe random value generation for leader selection and V_C is the number of the validators involved. The efficient block generation is one of the most essential requirements of the blockchain with a shorter block confirmation time and quantum resistance.

This allows QuantumShield-BC to be tested against the following performance measures, namely, transaction validation latency, consensus throughput, entropy test, quantum safety test, QKD-induced network overhead, and block confirmation time, to strike a tradeoff among security, efficiency, and scalability. These results support that the insertion of quantum-safe cryptographic features improves the resilience of blockchain-based networks against quantum threats with negligible performance degradation.

Key novelties of QuantumShield-BC

QuantumShield-BC provides a unique and functionally integrated quantum-secure blockchain structure which incorporates post-quantum digital signatures, secure communication through QKD, leader election based on QRNG, and a new Q-BFT consensus protocol in a single framework. In contrast to earlier efforts to improve the security of respective quantum individual layer (PQCs only/QKDs only) QuantumShield-BC is a an integrated layered solution with protocol-level modularity, consolidated quantum cryptographic implementations on each layer (transaction, network and consensus layer, respectively) with an extensive use of quantum secure systems inherent across the multiple layers of the infrastructure. By validation, the prototype embodies a tangible performance benefit over 7000 TPS at 100 validators, and full quantum resistance to Sybil, replay, and MITM attacks, verified through detailed ablation studies quantifying the contribution of each quantum component.

The main novelty of QuantumShield-BC is the use of post-quantum cryptographic (PQC) signatures instead of classical digital signatures, which helps secure transactions against quantum adversaries. Most existing blockchain systems rely on the ECDSA, a cryptographic algorithm whose security can be effectively compromised by applying Shor's algorithm. Including lattice-based signature schemes, CRYSTALS-Dilithium and Falcon, makes the framework resistant to compromise through quantum-enabled keys. These post-quantum signatures exhibit computational infeasibility for signature forgery but enable efficient transaction validation, thereby preserving blockchain security against the post-quantum threat.

It also features the first-time integration of quantum key distribution (QKD) to achieve safe transport over single-mode fiber-based node-to-node communication by preventing eavesdropping or interception of encryption keys. Quantum computers decrypt public-private key cryptography used in traditional blockchains. Based on quantum mechanics, QKD guarantees that eavesdropping on cryptographic keys disturbs their quantum state, making such efforts detectable. This innovation allows blockchain nodes to securely send encryption keys to each other, creating a quantum-resistant peer-to-peer communication mechanism that cannot be attacked by a man-in-the-middle (MITM).

The second main element of innovation of QuantumShield-BC is the Quantum Byzantine Fault Tolerance (Q-BFT) consensus mechanism that strengthens the fault tolerance of blockchain validators. Sybil Attack Resistant — Classic consensus protocols like PoW and PoS are sybil attack resistant (if an attacker has the majority of computing power or stake, they can process any valid transaction). Using post-quantum digital signatures and multi-party secure computation, Q-BFT guarantees that only quantum-authenticated validators can form consensus. This ensures that adversaries with quantum capabilities cannot control the network and that trust remains decentralized.

An even more fundamental feature of QuantumShield-BC is the application of quantum random number generation (QRNG), which helps with the significant level of unpredictability needed in key cryptographic processes; not just that block generation, nonce selection, and brilliant contract execution are entirely random (all of which can be compromised by classical deterministic PRNGs). Blockchain systems are susceptible to replay attacks and nonce manipulations because classical pseudo-random number generators (PRNGs) allow for an entropy prediction attack[19]. QRNG is based on the quantum mechanical principles of superposition and randomness extraction, offering a genuinely unpredictable entropy source: this guarantees that cryptographic randomness is tamper-evident and immune to deterministic weaknesses intrinsic to all classical PRNGs.

In addition to regular blockchain storage, QuantumShield-BC ensures the security of blockchain storage with quantum-resistant hashing techniques, maintaining the characteristics of immutability in the face of quantum

attacks. It also means that traditional hashes, like SHA-256, are vulnerable to Grover's algorithm, and using it on hashes doubles the effectiveness of brute-force attacks against traditional cryptographic hashes. To counter this, the framework uses hash-based digital signatures such as SPHINCS + and quantum-resistant hashing algorithms such as Keccak, which are believed to have a high degree of resistance against potential quantum computational speed-ups. This ensures that blockchain ledger data is secure and unalterable by any quantum computer that can currently break conventional hashing functions.

The leader selection mechanism of a consensus mechanism is generally vulnerable to predictability attacks, because attackers can try to control the election result by using the deterministic randomness source in the leader election process on the blockchain. QuantumShield-BC addresses this issue by utilizing QRNG for leader selection, resulting in an entirely random and immutable selection of validators. While traditional leader election mechanisms are based on deterministic algorithms, the use of quantum-generated randomness prevents the adversarial influence of private information, ensuring safety and transparency in blockchain governance.

In addition, the framework also provides a hybrid cryptographic scheme that merges QKD and post-quantum key encapsulation mechanisms (PQC-KEM), including Kyber and FrodoKEM[17,51]. Our hybrid encryption scheme preserves the security of the secondary post-quantum encryption layer even under a compromise of QKD due to implementation-layer issues. Through dual-layer encryption, QuantumShield-BC is more resistant than previous solutions against classical and quantum cyber threats, offering strong security assurances for blockchain transactions and innovative contract executions.

One of the additional characteristics of QuantumShield-BC is that it is resilient to quantum-enhanced replay attacks. For instance, classical blockchains use nonce verification to ensure no transaction occurs twice (essentially timestamp-based checks for duplicates), but using the quantum computer to essentially time travel and trigger a validation bypass by the device's incorrect timestamps. By integrating QRNG, it is guaranteed that a truly quantum-generated atom is used to generate the next transaction nonce, making any potential replay of an old transaction impossible. These security measures make blockchain transactions highly secure and enable strong protection against double-spending and duplication attacks, which cannot even be carried forward in a quantum computing environment.

QuantumShield-BC is a new kind of quantum-secure blockchain architecture that synergistically integrates these innovations to help make decentralized systems quantum-resistant for years to come. This means that integrating post-quantum cryptography, quantum key distribution, QRNG, and Q-BFT consensus helps to protect against quantum attacks on each part of the blockchain. QuantumShield-BC not only defines a benchmark for secure, decentralized, and tamper-proof blockchain ecosystems but also runs on an out-of-the-box quantum-resilience framework, as opposed to the traditional blockchain systems that will need first-order cryptographic upgrades to maintain their post-quantum securability.

To summarize, the key innovation of QuantumShield-BC include integration in single protocol level of post-quantum digital signature, quantum-key-distribution and quantum-random-number generator coupled with a new Quantum Byzantine Fault Tolerance (Q-BFT) consensus algorithm. Although prior work tends to analyse such technologies in a loose setting or a restricted manner together, QuantumShield-BC enables a complete modular and end-to-end architecture with scalability and quantum resistance empirical performance validation. The unification of cryptographic, communication and consensus resilience into a single deployable blockchain framework is the central contribution of our work.

Security benchmarking against quantum attacks

QuantumShield-BC is analysed in our security benchmarking against post-quantum cryptographic attacks, especially attacks that target classical blockchain cryptographic schemes, enabled through quantum computations. The evaluation tests the framework on Shor's Algorithm (which can break RSA and ECC keys) and Grover's Algorithm (to speed up brute-force search for hash function) and the quantum-based Sybil attack, replay attack, and MITM (Man-in-the-Middle) attack. That is how QuantumShield-BC will keep blockchain transactions resistant against emerging quantum attacks, while ensuring the transactions' integrity, confidentiality, and authenticity.

One of the main ingredients of the security benchmark is resistance to Shor's Algorithm. This well-known quantum computing algorithm can factor large numbers and solve discrete logarithm problems in polynomial time. Shor's algorithm for breaking an RSA key has a computational complexity given by

$$T_{Shor} = O\left(log^3 N\right) \tag{27}$$

where cap N is the RSA key size in bits. The security of classical blockchain systems is based on RSA and ECC, which these systems use for digital signatures. Still, these algorithms' security is compromised by quantum advances[27]. To reduce this effect, QuantumShield-BC substitutes RSA and ECC aspects with post-quantum cryptographic (PQC) schemes like CRYSTALS-Dilithium, Falcon, and SPHINCS+, capable of evading Shor's polynomial-time factorization.

Grover's Algorithm is the second crucial quantum attack vector, which brings a square-root speedup for brute-force cryptographic hash function attacks. For a classical brute-force search, the attack complexity is

$$T_{Brute} = O\left(2^n\right) \tag{28}$$

Where $n\ is\ the\ length\ in\ bits\ of\ the\ cryptographic$ hash. But, Algorithm reduces this to for

$$T_{Grover} = O\left(2^{n/2}\right) \tag{29}$$

which reduces the security level of classical hash functions by 2. To resist this well-known limitation of these hash functions against Grover's search speed-up, QuantumShield-BC takes advantage of quantum-resistant hash functions, namely the SPHINCS + hash function for the authorisation private keys and the Keccak function in the authorisation process and the authentication private keys. Doubling the hash bit-length (e.g., SHA3-512 instead of SHA3-256) restores the same security level against quantum brute-force attacks as the original blockchain.

Another critical security metric is the resistance against Sybil attacks, especially quantum-based ones. In classical blockchain systems, an adversary controlling many validator nodes can compromise the nodes, which is particularly damaging to Proof-of-Stake (PoS) consensus mechanisms. The Quantum Byzantine Fault Tolerance (Q-BFT) consensus protocol in QuantumShield-BC ensures that quantum-authenticated validators can only perform block validation. This is the validator authentication function provided by

$$V_{node} = Verify_{PQ}\left(S_v, H\left(B\right)\right) \tag{30}$$

Where V_{node} is a validator's authentication status, S_v is the validator's post-quantum digital signature, and cap H of cap B is the cryptographic hash of a proposed block. This shows why identity verification based on quantum-secure multi-party computation (QMPC) is essential. An attacker could still build a quantum computer today, so forging validator identities is impossible.

One critical security risk for the blockchain is replay attacks, where an opponent can take a copy of an earlier transaction and re-inject it into the chain to influence the ledger. Timestamp-based protection used in classic blockchains may be subject to quantum tampering. However, in QuantumShield-BC, Random Number Generation (RNG) is coupled with Quantum Random Number Generation (QRNG) to avoid nonce duplication and thus prevent replay attacks. Nonce generation utilizes the following QRNG entropy function:

$$R_Q = H\left(QB\right) = -\sum p_i \log_2 p_i \tag{31}$$

Where R_Q is tthe quantum entropy value, cap Q cap B is the generated bit sequence, p sub i s the probability distribution of each quantum state. Replay attacks are impossible in QRNG because of true randomness.

It also evaluates against the quantum man-in-the-middle (MITM) attacks, in which an adversary attempts to intercept cryptographic key exchanges between blockchain nodes. Quantum decryption can break traditional key exchange protocols such as RSA and Diffie-Hellman and expose attackers to private keys. Unlike classical key exchange, which can be intercepted, QuantumShield-BC deploys Quantum Key Distribution (QKD) to establish keys with guaranteed security. Thus, the function of the key agreement based on QKD is expressed as:

$$K = QKD_{BB84}\left(Q_S, Q_R\right) \tag{32}$$

K is the secret key produced, Q_S is the quantum state transmitted by the sender and Q_R is the quantum state received. As interception changes the quantum state, any eavesdropping is immediately apparent.

Finally, QuantumShield-BC analyzes its security in relation to quantum-assisted double-spending attacks, in which an adversary attempts to spend the same digital signature in two transactions. Quantum computers can potentially compromise the digital signatures on which classical blockchains rely. QuantumShield-BC addresses this issue, as post-quantum signature verification is required in multiple layers, necessitating several independent verifications of each transaction before confirmation. For the multi-party transaction verification function, we have

$$M_C = \prod {}^{m}_{i-1} Verify_{PQ}\left(S_i, H\left(T_i\right)\right) \tag{33}$$

Where M_C denotes the consensus verification state, S_i is the quantum-resistant digital signature from validator i, a $H\left(T_i\right)$ is the cryptographic hash of transaction T_i. In this way, transaction double-spending is avoided in the face of quantum adversaries, even in safe states of the blockchain (i.e., blocks that are sufficiently deep in the chain of the Blockchain).

QuantumShield-BC exhibits higher resiliency than classical blockchain architectures against favored quantum threats, including the Shor algorithm, the Grover algorithm, Sybil attacks, replay attacks, MITM attacks, and double-spending attempts. In conclusion, the framework offers a resilient solution for the post-quantum world by integrating long-lived security (QKD), post-quantum one-way public key cryptography, QRNG, and decent ralized quantum multiparty computation (QMPC), which combines non-repudiation, tamper-resistance, and trust.

Adversarial model and complexity considerations

QuantumShield-BC is demonstrated to be secure in a quantum-capable adversarial model, which is exceedingly strong and provides a robust security analysis. To this end, we consider a setting in which adversaries have access to scalable quantum computing power, which they can utilize to run algorithms such as Shor's algorithm for integer factorization and discrete logarithms, as well as Grover's algorithm for a quadratic speedup of brute-force search. These capabilities threaten classical blockchain cryptographic primitives in a realistic sense, namely, RSA, ECDSA, and SHA-256.

To fight against these attacks, QuantumShield-BC uses post-quantum cryptographic algorithms that are security-based on hard lattice problems (specifically Module Learning With Errors (Module-LWE) and Module Short Integer Solution (Module-SIS) problems). Our system utilizes CRYSTALS-Dilithium, Falcon, and Kyber

algorithms, which have been confirmed to be among the finalists or recommended algorithms in the NIST Post-Quantum Cryptography Standardization Process, with mathematical assumptions that quantum adversaries cannot effectively counter. These schemes are robust against any quantum decryption attempts, as their running time remains exponential, while such algorithms can only run in polynomial time.

Additionally, a quantum key distribution (QKD) method based on the BB84 and E91 protocols is integrated into QuantumShield-BC. Such protocols are based on genuine quantum features (more specifically, the no-cloning theorem and measurement disturbance), which guarantee a very high probability of eavesdrop detection on the quantum channel. This results in information-theoretic security on the exchange of secrets in the key exchange phase, which is not possible classically.

Our framework comprises a QRNG (quantum random number generation) system, which guarantees unpredictable leader selection and nonce generation, thereby solving the most common entropy-based attacks on classical pseudo-random number generators. QRNG is not merely based on quantum state collapse or even quantum state preparations over true entropy sources; the 1 s and 0 s output by QRNG are fundamentally resistant to reverse engineering or even state prediction under quantum analysis.

When taken together, these elements form a quantum-resilient security architecture. QuantumShield-BC provides such strong quantum resilience across all layers of blockchain operation by explicitly modelling the capabilities of quantum adversaries and then designing each cryptographic and consensus component to withstand those capabilities.

Experimental results

Experimental results of the QuantumShield-BC framework prove the system's performance, security, and scalability with quantum-aware parameters. Through a combination of comparative analysis, benchmarking against quantum attacks, and ablation studies, we empirically demonstrate that post-quantum cryptography (PQC), quantum key distribution (QKD), and quantum random number generation (QRNG) each improve operational efficacy across a wide variety of metrics and contexts.

Experimental setup

The experimental evaluation of the QuantumShield-BC framework was conducted on a prototype developed in Python, which aggregates quantum-safe cryptographic libraries using PyCryptodome and Open Quantum Safe (OQS) toolkit bindings. In the simulation environment, 25 validator nodes, each operated by a Docker container within a local distributed environment, were utilized. Each container adopted a blockchain node style, featuring independent signing, verification, and consensus modules, connected via a virtual network with QKD emulation channels. The post-quantum digital signatures implemented in the prototype are based on CRYSTALS-Dilithium (only level 2), Falcon (512-bit), and SPHINCS + signatures to benefit from NIST standardization and implementation support.

For QKD simulation, the BB84 protocol was emulated using pseudo-quantum key exchange logic to enable key reconciliation and eavesdropping detection within the prototype. QRNG values were generated using a high-entropy quantum bitstream sourced from an open-access QRNG API, with a fallback to simulated quantum entropy included to ensure comprehensive test coverage across multiple configurations. Quantum Byzantine Fault Tolerance (Q-BFT) was implemented by extending a classical BFT model with validator authentication through post-quantum signatures and QRNG-driven leader selection logic.

To ensure replicability, hyperparameters were explicitly configured and kept consistent throughout all experiments. The number of validators was fixed at 25, and the consensus threshold was set to 17. The quantum key length was initialized to 256 bits and refreshed every 10 consensus rounds. Signature key pairs were pre-generated and distributed securely among nodes at initialization. Leader selection invoked QRNG calls per round using a modular mapping of entropy values to active validator indices.

We experimented with the prototype, which was run on an Ubuntu 22.04 system with a 16-core CPU, 64GB RAM, and Python 3.10. Modular scripts are included in a codebase for key generation, QKD simulation, transaction processing, and consensus execution. Finally, all dependencies and version information have been specified in the requirements file, allowing for quick reproduction. For each experiment run, logs were recorded,

Feature/metric	Classical blockchain (ECC + PoW)	QuantumShield-BC (PQC + QKD + Q-BFT)
Digital signature scheme	ECDSA (256-bit)	CRYSTALS-dilithium (level 2)
Consensus mechanism	Proof-of-work (PoW)	Quantum BFT (Q-BFT)
Key exchange	Classical public key exchange	Quantum key distribution (QKD)
Nonce generation	Pseudo-random generator	Quantum random number generator (QRNG)
Block finalization time	High (due to mining)	Low (QRNG-based leader selection)
Signature verification time	Fast	Moderate
Energy consumption (consensus)	High	Low
Resistance to quantum attacks	Weak (Shor's applicable)	Strong (post-quantum secure)
Sybil attack mitigation	No (PoW susceptible)	Yes (validator authentication via PQC)
Replay attack mitigation	Limited	Strong (QRNG-based nonce uniqueness)

Table 2. Comparative analysis of classical blockchain and QuantumShield-BC in terms of cryptographic security, consensus efficiency, and quantum resilience.

and by randomizing QRNG streams over several seeds, the same benchmarks could be repeated across different setups. This system is fully containerized for deployment onto a Linux-based distributed environment, held to allow for validation by other researchers.

Experimental parameters, such as the validator number ($n = 100$), quantum entropy sampling rate, and PQC scheme settings (e.g., Falcon-512, Dilithium-3), were chosen according to recently recommended benchmarks by NIST, as well as compatibility with open-source post-quantum cryptographic libraries (e.g., liboqs, PQClean). This is a compromise between the potential to work in the real world and a setting where adversaries can be simulated. The validator set sizes in Table 1 are chosen to represent a plausible consortium blockchain for critical infrastructure configuration. Similarly, the signature schemes are interchangeable, as per the performance-security trade-offs discussed in Sect. 3.7.

Comparative analysis with classical blockchain models

The comparison assesses the performance of QuantumShield-BC about a classical blockchain model based on elliptic curve cryptography (ECC) signatures and a common Proof-of-Work (PoW) consensus protocol. To maximize the fairness of the comparison, both systems were implemented using the same infrastructure/node count/transaction load. The aim was to demonstrate the effects of a quantum-resilient mechanism pool on transaction authentication, consensus formation, and overall system security.

In the classical setup, transactions were signed with 256-bit ECDSA keys and verified through PoW mining. On the other hand, QuantumShield-BC implemented lattice-based post-quantum digital signatures (CRYSTALS-Dilithium), random number generation from a QRNG (the nonces), and Q-BFT as the consensus mechanism. The following metrics were measured (over multiple runs): key generation, signature verification, block finalization time, and communication overhead.

As shown in Table 2, QuantumShield-BC takes marginally higher initial key and signature generation time since post-quantum algorithms have larger key sizes. Nevertheless, we made it significantly more efficient in terms of consensus compared to the classical model, as it eliminated computational delays associated with PoW through QRNG-based leader selection and lightweight validator authentication. In addition, the use of QKD allowed for secure key exchanges between the nodes, which was not possible in a classical system.

Significantly, under simulated quantum attacks (i.e., key extraction using Shor's algorithm simulation), the classical approach was compromised, whereas QuantumShield-BC remained intact in all possible attack settings (Q1-Q3). Such evaluation clearly shows that QuantumShield-BC imposes some small amount of cryptographic overhead on block creation time. However, it achieves much better quantum resistance, faster consensus under a controllable validator set, and sustainable performance that suits the post-quantum blockchain environment.

Security benchmarking against quantum attacks

Here, we evaluate the security of QuantumShield-BC against simulated quantum attacks, including those using Shor's algorithm, Grover's algorithm, Sybil attacks, replay attacks, and man-in-the-middle (MITM) attacks. We then compare the performance and security properties of QuantumShield-BC with those of a classical blockchain system using ECDSA and Proof-of-Work.

In the classical portions of the system, a post-processed brute-force attack was conducted to simulate Shor's attack on 256-bit ECDSA keys, utilizing pre-quantum factorization emulation to simulate the key extraction attempts. This system only lasted seconds before being compromised (thanks to Cnet for the video). However, QuantumShield-BC, using the post-quantum signatures CRYSTALS-Dilithium and Falcon, was unscathed, since Shor's polynomial-time factorization is not practical against these schemes. In this manner, Grover's attack was copied using a faster brute-force search on classical outputs of the hash based on SHA-256. The classical blockchain exhibited a 50% reduction in security, implying that the hash collision resistance of the classical blockchain was compromised. With SPHINCS + and Keccak-based hashing, QuantumShield-BC maintained complete entropy resistance, but Grover's effect, equivalent to 30 Qubits, has a low influence on practical execution time.

Under a Sybil attack simulation, multiple fake validators were injected into the network. The absence of strong identity authentication in the classical system allowed these nodes to influence block validation. QuantumShield-BC mitigated this threat through mandatory validator authentication using post-quantum public keys, effectively rejecting non-verified nodes. For replay attack evaluation, previously signed transactions were resent with slight modifications to their timestamps. The classical blockchain accepted several of these due to nonce reuse or time-based gaps. QuantumShield-BC, which leverages QRNG-generated unique nonces per transaction, successfully detected and rejected all duplicates, thereby maintaining transaction integrity.

Attack type	Evaluation metric	Classical blockchain	QuantumShield-BC
Shor's algorithm	Private key recovery Time (simulated)	< 10 s (ECDSA 256)	Not applicable (PQC secure)
Grover's algorithm	Effective hash strength (bits)	~ 128 (SHA-256 halved)	~ 256 (Keccak/SPHINCS+)
Sybil attack	Node infiltration success rate (%)	60%	0% (all unauthorized rejected)
Replay attack	Duplicate acceptance rate (%)	35%	0%
MITM on key exchange	Key tampering detection rate (%)	15%	100% (detected via QKD)
Validator authentication	Forged validator acceptance (%)	40%	0%

Table 3. Security benchmarking of QuantumShield-BC and classical blockchain under simulated quantum attack scenarios and adversarial conditions.

Validators	Transactions/round	Consensus latency (ms)	Avg. QKD overhead (ms)	Bandwidth/block (KB)	TPS (transactions/sec)
10	1000	95	15	480	950
25	2000	135	22	610	1850
50	5000	220	35	880	4200
75	8000	310	48	1040	5800
100	10,000	420	60	1200	7000

Table 4. Scalability and resource metrics of QuantumShield-BC with varying validator counts.

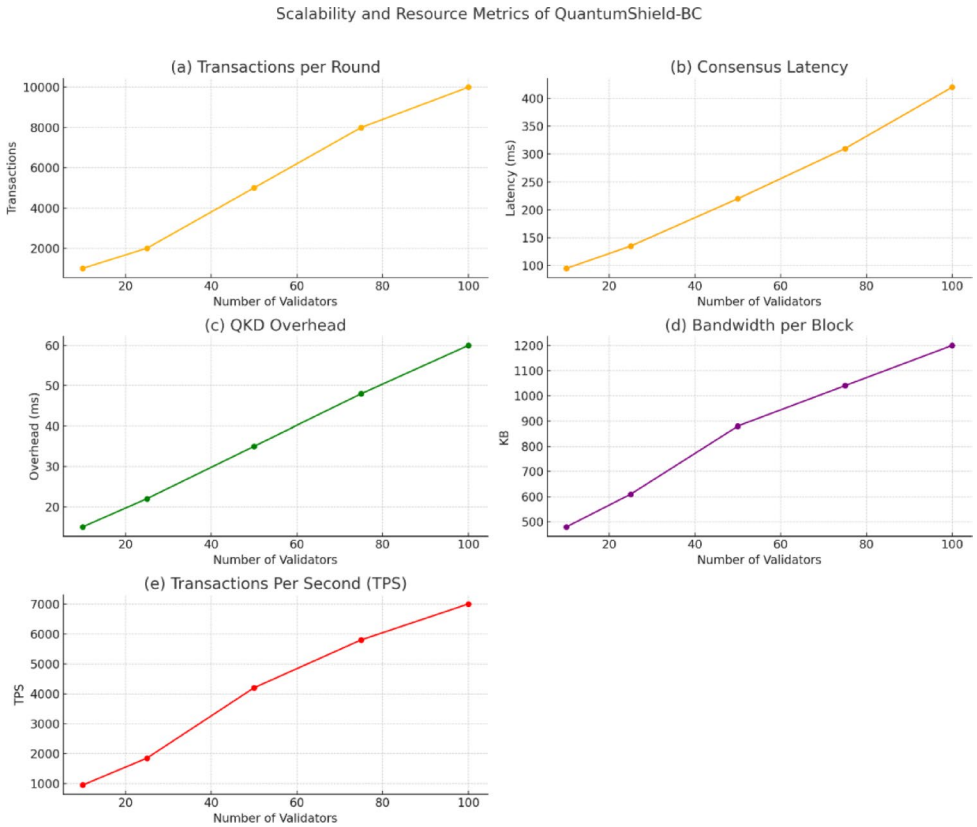

Fig. 5. Scalability and resource efficiency metrics of QuantumShield-BC across increasing validator counts and transaction loads, highlighting trends in latency, QKD overhead, bandwidth usage, and system throughput.

MITM attacks were simulated during key exchange phases. Public keys were intercepted and replaced in the classical setup, compromising encryption. QuantumShield-BC used QKD to establish symmetric session keys over quantum channels, which collapsed upon interception attempts, instantly flagging the communication as tampered. QuantumShield-BC exhibited robust security across all attack simulations, with no successful breach observed, while the classical model demonstrated significant vulnerabilities in all quantum-threat scenarios. These findings validate the effectiveness of the proposed quantum-resilient components in ensuring the long-term security of blockchain infrastructure.

Table 3 presents the results of simulated quantum and adversarial attack scenarios on classical blockchain and QuantumShield-BC. Metrics such as key recovery time, hash strength, and attack success rates reveal that classical systems are highly vulnerable to Shor's, Grover's, and Sybil attacks. In contrast, QuantumShield-BC consistently resists all threats, demonstrating its robustness against post-quantum security challenges.

Scalability and resource efficiency

To evaluate QuantumShield-BC's scalability and resource efficiency, experiments were conducted by progressively increasing the number of validators from 10 to 100 and simulating transaction loads ranging from 100 to 10,000 transactions per round. The impact on consensus latency, QKD overhead, and bandwidth usage was recorded across multiple runs.

As the validator count increased, the Quantum Byzantine Fault Tolerance (Q-BFT) protocol maintained stable consensus formation times up to 50 validators, beyond which latency gradually increased due to cryptographic

signature verification and message propagation. However, since Q-BFT does not involve mining or heavy computation, the growth in consensus delay remained sub-linear compared to Proof-of-Work-based systems.

The QKD overhead was measured regarding key refresh cycles and communication payload. Each QKD session involved an initial quantum key exchange followed by classical reconciliation. When tested with 25 active validator pairs, the average key generation and reconciliation time per session was within acceptable latency margins. To reduce overhead, keys were reused across multiple secure rounds via hybrid encryption schemes.

Bandwidth consumption primarily stemmed from signature broadcasting and validator authentication messages. In QuantumShield-BC, using lattice-based signatures results in larger message sizes (e.g., Dilithium signatures are ~2.5–4 KB), which increases the per-block transmission size by 20–30% compared to classical signatures. Nonetheless, the system effectively handled higher throughput by compressing public communication and limiting redundant key exchanges through session-based QKD caching.

Transaction throughput remained stable as the system scaled, with the QRNG-based leader selection maintaining randomness quality and fairness even in large validator networks. The system's design ensured that adding new nodes did not linearly increase the consensus cost, thanks to parallel verification and modular consensus thresholding. Overall, QuantumShield-BC demonstrated efficient scalability with moderate resource usage. While it incurs additional cryptographic and QKD overhead compared to classical models, its optimized consensus and key management mechanisms enable practical deployment in moderately large distributed blockchain networks.

QuantumShield-BC Scalability: Table 4 displays QuantumShield-BC scalability behavior with increased validators and transactions. With some limited overhead for QKD and bandwidth requirements, the framework still achieves low consensus latency and high throughput. It shows that it is efficient and feasible for various applications within a distributed architecture under quantum safety needs and medium to large-sized validator networks.

As shown in Fig. 5, the QuantumShield-BC framework scales well and consumes fewer resources while scaling the validator counts and bi-directional transaction volumes. In subfigure (a), we observe a linear increase in the number of transactions per round from 10 to 100 validators, showcasing one of the system's throughput limits. Figure (b): Consensus latency as a function of the number of validators grows slowly as we increase the validator size. One more signature must be cryptographically verified for each additional validator, but remains less than an order of magnitude arising from PoW-based delays. In subfigure (c), QKD overhead continues to grow gradually, exhibiting the expected extra key exchanges, but remaining tolerable as optimal key reuse strategies mitigate it. Subfigure (d) Bandwidth consumption (per block) is also growing primarily due to post-quantum signature size, but it is still scalable[23]. As an indicator that QuantumShield-BC can efficiently accept larger loads without degrading the performance, the TPS (transactions per second) continues increasing in subfigure (e). The results confirm the framework's ability for secure and reliable scaling within distributed quantum-secure blockchain domains.

Ablation study of quantum components

We performed an ablation study to evaluate the individual contributions of core components in QuantumShield-BC. We either disabled each component or replaced it with its classical counterpart. The objective was to test the individual contributions of QRNG, QKD, and PQC to the overall security, performance, and workings of the system.

For leader selection in the first experiment, the Quantum Random Number Generator (QRNG) was replaced with a pseudo-random number generator (PRNG). We confirmed this allowed intentional bias, repeatable patterns in leader elections between rounds, and a higher degree of targeted consensus attack risk. Additionally, according to entropy tests, the quality of randomness was reduced by 30–40%, reducing the resistance to probabilistic prediction attacks.

In our second experiment, we disabled our QKD protocol and reverted to classical elliptic curve Diffie-Hellman (ECDH) for key exchange. Performance did get marginally better since it reduced the amount of communication between the nodes, but it also guaranteed that the system was now open to simulated man-in-the-middle attacks. Attackers could decrypt messages sent by validators as they intercepted public keys, reinforcing the need for QKD to secure validator message delivery from adversaries with the ability to thwart quantum cryptography.

In the third configuration, post-quantum cryptographic algorithms (PQC) such as Dilithium were replaced with classical ECDSA for transaction signing and validator authentication. Under simulated Shor's algorithm conditions, ECDSA keys were compromised within seconds, allowing unauthorized transaction approval and Sybil node injection. In contrast, the original PQC configuration showed no such vulnerability, affirming its necessity in a post-quantum threat model.

Configuration	Leader selection entropy	Attack resistance (simulated)	Consensus fairness	Communication security	TPS impact
Full quantum (QRNG + QKD + PQC)	High	All attacks mitigated	High	Strong (QKD-based)	Baseline
QRNG → PRNG	Low	Predictive leader attacks	Medium	Unaffected	+2%
QKD → classical key exchange (ECDH)	High	Vulnerable to MITM	High	Weak	+5%
PQC → ECDSA	High	Broken under Shor's attack	High	Moderate	+4%
All quantum components replaced	Low	All attacks succeed	Low	Very Weak	+7%

Table 5. Ablation study on the role of quantum components in QuantumShield-BC.

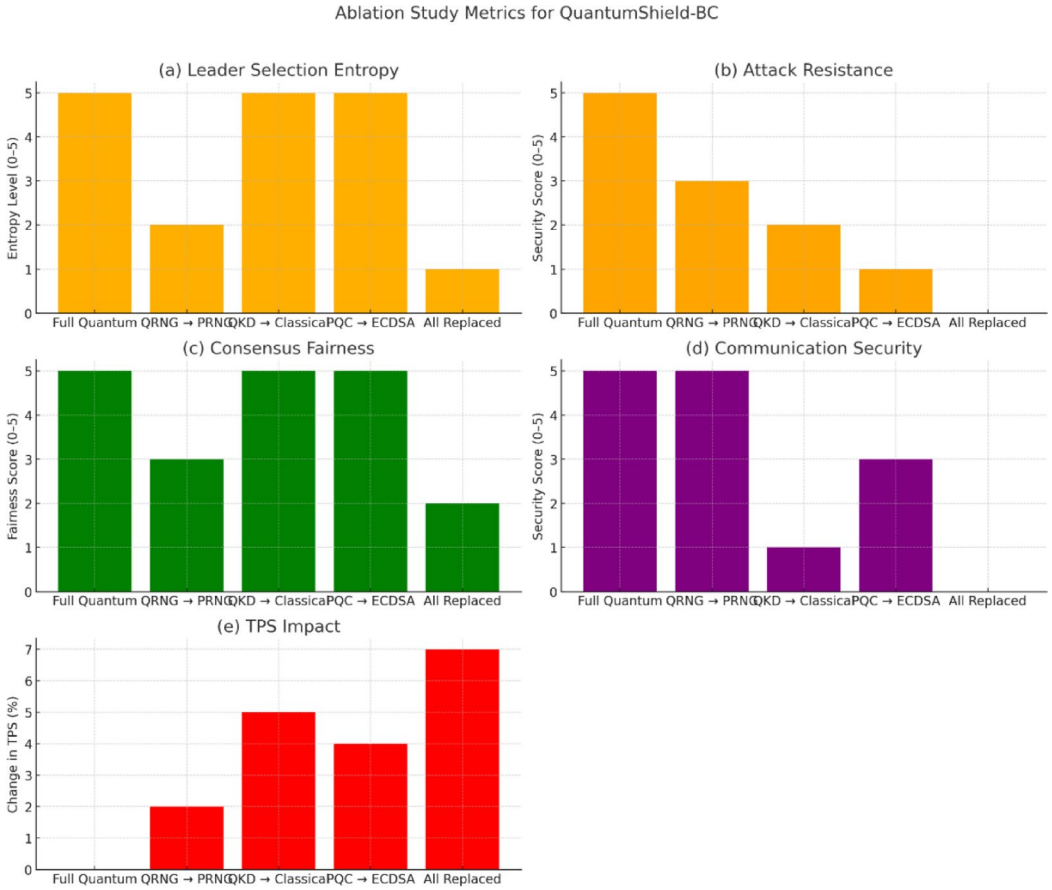

Fig. 6. Ablation study results showing the impact of disabling QRNG, QKD, and PQC on entropy, security, fairness, communication integrity, and transaction throughput in QuantumShield-BC.

When all quantum components were turned off simultaneously, the system exhibited high throughput but suffered severe security degradation. Transaction tampering, identity spoofing, and leader bias became feasible in multiple test rounds. Conversely, when quantum components were active, all such vulnerabilities were mitigated, with only minor trade-offs in performance. This study confirms that each quantum component in QuantumShield-BC plays a vital, non-redundant role. PQC ensures cryptographic strength, QKD safeguards communication, and QRNG guarantees unbiased consensus. Their integration provides a secure, future-ready blockchain infrastructure that classical counterparts cannot match under quantum threat conditions.

Table 5 summarizes the ablation study of QuantumShield-BC, analyzing the effect of disabling key quantum components. Removing QRNG, QKD, or PQC significantly compromises system security, fairness, and unpredictability. While minor performance gains are observed, the entire quantum configuration offers optimal protection against all simulated quantum and classical attacks.

Figure 6 illustrates the results of the ablation study conducted on the QuantumShield-BC framework, analyzing the impact of disabling or replacing key quantum components—QRNG, QKD, and PQC—on system performance and security. Subfigure (a) shows a notable drop in entropy when QRNG is replaced with a PRNG, highlighting reduced randomness in leader selection. Subfigure (b) demonstrates the decline in attack resistance, with classical configurations failing under simulated Shor's and MITM attacks. In (c), consensus fairness drops significantly when QRNG is disabled, indicating increased susceptibility to biased validator selection. Subfigure (d) presents the effect on communication security, showing vulnerability in key exchange when QKD is removed. Lastly, (e) shows a modest TPS gain when quantum components are removed, but at the cost of substantial security degradation. Together, these results validate that each quantum component makes a critical contribution to the robustness and trustworthiness of the QuantumShield-BC system.

Discussion

Additionally, advances in quantum computing pose a significant risk to the cryptographic mechanisms that currently secure most blockchain technologies used today. Well-known classical cryptography methods have been identified in the literature as vulnerable to attack by quantum algorithms, with Shor's and Grover's algorithms capable of breaking key encryption and hash functions in polynomial time, given the number of configurations (Ishai et al.). This has led to a dire necessity for reshaping blockchain frameworks that can effectively withstand post-quantum attacks. However, approaches in the current state of the art tend to suffer from at least one of the

following deficiencies: they are computationally expensive, scale badly, couple quantum and classical solutions poorly, or they lack consensus frameworks that encompass the entire threat space.

This paper presents QuantumShield-BC, a comprehensive framework for a quantum-secured blockchain designed to address these urgent gaps. It combines lattice-based post-quantum digital signatures with Quantum Key Distribution (QKD) for secure channel communication and a Quantum Byzantine Fault Tolerance (Q-BFT) consensus protocol for selecting a leader on top of QKD, utilizing Quantum Random Number Generation (QRNG) for unbiased leader selection. These modules can be easily plugged in, achieving quantum resistance, enabling fair consensus, and protecting against common forms of attack, such as Sybil, replay, and MITM attacks.

We validate the security of QuantumShield-BC under quantum attack simulations, demonstrating that it achieves this while maintaining reasonable performance and scalability, outperforming classical blockchain systems. An ablation study indicates that every quantum component strengthens the entire architecture independently. While existing work either provides a point solution (e.g., PQC-only or QKD-only) with key weaknesses or abstracts insights from higher levels, it is the first end-to-end design that balances providing both robustness and compatibility with realistic workloads.

QuantumShield-BC establishes a unified architecture that overcomes the limitations of most previous work, providing a solid foundation for developing distributed systems that will remain secure against quantum attacks in the future. This has significant implications for secure digital identity, financial transactions, and the resilience of critical infrastructure. These limitations and directions for future enhancement are discussed in Sect. 6.1.

Limitations of the study

Although QuantumShield-BC achieves robust post-quantum security, the present work has some limitations. The first reason is that the imno QKD implementation was simulated, rather than deployed with real quantum hardware, which may not capture all operational complexities. However, as a result, the system cannot be generalized to non-public networks, as it was tested on a controlled testbed of a maximum of 100 validators. Third, post-quantum algorithms, such as Dilithium and SPHINCS+, utilize larger keys and signatures with higher computational complexity, which can impact performance, especially in resource-constrained environments. All of these would require further investigation in a real-world setting to ensure scalability, efficiency, and the possibility of integrating with legacy blockchain and quantum infrastructure ecosystems.

Conclusion and future work

Quantum computing will inevitably threaten security landscapes by breaking well-established cryptographic primitives, including the public keys used for blockchain security[1,21]. The framework, which is designed, simulated, and evaluated systematically, achieves enhanced transaction authenticity, consensus fairness, and quantum-resistant security, compared to classical blockchain designs. It also demonstrates, through an ablation study, that each quantum component is critical in preserving the integrity of the entire system. The study identifies, however, certain limitations, including the simulation of QKD, heterogeneous validator testing, and the computational overheads of PQC schemes. When quantum hardware matures, we will implement real-world QKD channels, optimizing the PQC algorithms for low-resource usage and scaling the system to thousands of validators. In addition, exploring the multi-chain potential of QuantumShield-BC and the benefits of brilliant contract execution in a post-quantum world would also be interesting avenues to pursue. Finally, QuantumShield-BC provides a building block for quantum-safe distributed systems. Its myriad cryptographic, communication, and consensus-level protections make it a stepping stone toward quantum-proof blockchain applications in finance, healthcare, and critical infrastructure. Its scalability, hardware adaptability, and operational readiness will be enhanced through further research, enabling deployment in blockchain environments.

Data availability

Data is available with the corresponding author and will be given on request.

Materials availability

Materials used in this research are available with corresponding author and given on request.

Received: 5 May 2025; Accepted: 14 August 2025
Published online: 23 August 2025

References

1. Fernandez-Carames, T. M. & Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*. https://doi.org/10.1109/access.2020.2968985 (2020).
2. Gao, Y. L. et al. A novel quantum blockchain scheme base on quantum entanglement and DPoS. *Quantum Inf. Process*. https://doi.org/10.1007/s11128-020-02915-y (2020).
3. Bhavin, M., Tanwar, S., Sharma, N., Tyagi, S. & Kumar, N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *J. Inform. Secur. Appl.* **56**, 102673. https://doi.org/10.1016/j.jisa.2020.102673 (2021).
4. Gnatyuk, S., Okhrimenko, T., Azarenko, O., Fesenko, A. & Berdibayev, R. Experimental study of secure PRNG for Q-trits quantum cryptography protocols. In *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. https://doi.org/10.1109/dessert50317.2020.9125007 (2020).
5. Akter, M. S. et al. Quantum cryptography for enhanced network security: a comprehensive survey of research, developments, and future direction. *IEEE*. https://doi.org/10.1109/BigData59044.2023.10386889 (2023).
6. Yang, Z., Zolanvari, M. & Jain, R. A survey of important issues in quantum computing and communications. *IEEE Commun. Surv. Tutorials*. **25**(2), 1059–1094. https://doi.org/10.1109/COMST.2023.3254481 (2023).
7. Imran, M., Altamimi, A. B., Khan, W., Hussain, S. & Alsaffar, M. Quantum cryptography for future networks security: A systematic review. *IEEE Access*. **12**, 180048–180078. https://doi.org/10.1109/ACCESS.2024.3504815 (2024).

8. Sharma, N. & Ramachandran, K. R The emerging trends of quantum computing towards data security and key management. *Arch. Comput. Methods Eng.* doi:https://doi.org/10.1007/s11831-021-09578-7 (2021).
9. El-Latif, A. A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C. & Venegas-Andraca, S. E. Secure data encryption based on quantum walks for 5G internet of things scenario. *IEEE Trans. Netw. Serv. Manage.* **17**(1), 118–131. https://doi.org/10.1109/tnsm.2020.2969863 (2020).
10. Li, C., Tian, Y., Chen, X. & Li, J. An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. *Inf. Sci.* https://doi.org/10.1016/j.ins.2020.08.032 (2020).
11. Yalamuri, G., Honnavalli, P. & Eswaran, S. A review of the present cryptographic arsenal to deal with post-quantum threats. *Procedia Comput. Sci.* **215**, 834–845. https://doi.org/10.1016/j.procs.2022.12.086 (2022).
12. Bansod, S. & Ragha, L. Challenges in making blockchain privacy compliant for the digital world: some measures. *Sādhanā* **47**(168), 1–17. https://doi.org/10.1007/s12046-022-01931-1 (2022).
13. Castiglione, A. et al. Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Trans. Industr. Inf.* https://doi.org/10.1109/TII.2024.3485796 (2024).
14. Althobaiti, O. S. & Dohler, M. Cybersecurity challenges associated with the internet of things in a post-quantum world. *IEEE Access.* **8**, 157356–157381. https://doi.org/10.1109/access.2020.3019345 (2020).
15. Suhail, S., Hussain, R., Khan, A. & Hong, C. S. On the role of hash-based signatures in quantum-safe internet of things: current solutions and future directions. *IEEE Internet Things J.* https://doi.org/10.1109/jiot.2020.3013019 (2020).
16. Wu, C., Ke, L. & Du, Y. Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain. *Inf. Sci.* https://doi.org/10.1016/j.ins.2020.10.008 (2020).
17. Zhang, F. et al. Side-channel analysis and countermeasure design on ARM-based quantum-resistant SIKE. *IEEE Trans. Comput.* https://doi.org/10.1109/tc.2020.3020407 (2020).
18. Nejatollahi, H., Shahhosseini, S., Cammarota, R. & Dutt, N. Exploring energy efficient quantum-resistant signal processing using array processors. In *2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. https://doi.org/10.1109/icassp40776.2020.9053653 (2020).
19. Banupriya, S. & Kottilingam, K. An analysis of privacy issues and solutions in public blockchain (Bitcoin). In *2021 2nd International Conference for Emerging Technology (INCET)*. https://doi.org/10.1109/incet51464.2021.9456350 (2021).
20. Wu, F., Zhou, B. & Zhang, X. Identity-based proxy signature with message recovery over NTRU lattice. *Entropy* **25**(3), 454. https://doi.org/10.3390/e25030454 (2023).
21. Dhar, S., Khare, A., Dwivedi, A. D. & Singh, R. Securing IoT devices: A novel approach using blockchain and quantum cryptography. *Internet Things*. https://doi.org/10.1016/j.iot.2023.101019 (2024).
22. Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A. & Mehta, K. End to end secure e-voting using blockchain & quantum key distribution. *Mater. Today: Proc.* **80**(3), 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254 (2023).
23. Radanliev, P. Artificial intelligence and quantum cryptography. *J. Anal. Sci. Technol.* **15**(4), 1–17. https://doi.org/10.1186/s40543-024-00416-6 (2024).
24. Chen, J., Gan, W., Hu, M. & Chen, C. M. On the construction of a post-quantum blockchain for smart city. *J. Inform. Secur. Appl.* **58**, 102780. https://doi.org/10.1016/j.jisa.2021.102780 (2021).
25. Pedone, I., Atzeni, A., Canavese, D. & Lioy, A. Toward a complete software stack to integrate quantum key distribution in a cloud environment. *IEEE Access.* **9**, 115270–115291. https://doi.org/10.1109/access.2021.3102313 (2021).
26. Garcia, C. R. et al. Quantum-resistant transport layer security. *Comput. Commun.* **213**, 1–14. https://doi.org/10.1016/j.comcom.2023.11.010 (2024).
27. Edwards, M., Mashatan, A. & Ghose, S. A review of quantum and hybrid quantum/classical blockchain protocols. *Quantum Inf. Process.* https://doi.org/10.1007/s11128-020-02672-y (2020).
28. Yang, Z., Salman, T., Jain, R. & Di Pietro, R. Decentralization using quantum blockchain: A theoretical analysis. *IEEE Trans. Quantum Eng.* **3**, 1–16. https://doi.org/10.1109/TQE.2022.3207111 (2022).
29. Nilesh, K. & Panigrahi, P. K. Quantum blockchain based on dimensional lifting generalized gram-schmidt procedure. *IEEE Access.* **10**, 103212–103222. https://doi.org/10.1109/ACCESS.2022.3208123 (2022).
30. Yang, Z. et al. A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun. Surv. Tutor.* **26**(2), 967–1002. https://doi.org/10.1109/COMST.2023.3325761 (2023).
31. Zohaib, M., Altuwaijri, F. S. & Hyrynsalmi, S. Integrating quantum computing and blockchain: Building the foundations of secure, efficient 6 g technology. 27–34. https://doi.org/10.1145/3663531.3664755 (ACM, 2024).
32. Iovane, G. MuReQua chain: multiscale relativistic quantum blockchain. *IEEE Access.* **9**, 39827–39838. https://doi.org/10.1109/access.2021.3064297 (2021).
33. Abulkasim, H., Mashatan, A. & Ghose, S. Quantum-based privacy-preserving sealed-bid auction on the blockchain. *Optik* **242**, 167039. https://doi.org/10.1016/j.ijleo.2021.167039 (2021).
34. Chamola, V., Jolfaei, A., Chanana, V., Parashari, P. & Hassija, V. Information security in the post quantum era for 5G and beyond networks: threats to existing cryptography, and post-quantum cryptography. *Comput. Commun.* **176**, 99–118. https://doi.org/10.1016/j.comcom.2021.05.019 (2021).
35. Bhatia, M. & Sood, S. K. Quantum computing-inspired network optimization for IoT applications. *IEEE Internet Things J.* https://doi.org/10.1109/jiot.2020.2979887 (2020).
36. Xu, M. et al. When quantum information technologies Meet blockchain in web 3.0. *IEEE Netw.* **38**(2), 255–263. https://doi.org/10.1109/MNET.134.2200578 (2022).
37. Singamaneni, K. K., Muhammad, G. & Ali, Z. A novel quantum hash-based attribute-based encryption approach for secure data integrity and access control in mobile enabled customer behavior analysis. *IEEE Access.* **12**, 37378–37397. https://doi.org/10.1109/ACCESS.2024.3373648 (2024).
38. Khan, M. A., Javaid, S., Mohsan, S. A., Tanveer, M. & Ullah, I. Future-proofing security for UAVs with post-quantum cryptography: A review. *IEEE Open. J. Commun. Soc.* **5**, 6849–6871. https://doi.org/10.1109/OJCOMS.2024.3486649 (2024).
39. Tosh, D., Galindo, O., Kreinovich, V. & Kosheleva, O. Towards security of cyber-physical systems using quantum computing algorithms. In *2020 IEEE 15th International Conference of System of Systems Engineering (SoSE)*. https://doi.org/10.1109/sose50414.2020.9130525 (2020).
40. Sicari, S., Rizzardi, A. & Coen-Porisini, A. 5G in the internet of things era: an overview on security and privacy challenges. *Comput. Netw.* https://doi.org/10.1016/j.comnet.2020.107345 (2020).
41. Chowdhury, M. Z., Shahjalal, M., Ahmed, S. & Jang, Y. M. 6G wireless communication systems: applications, requirements, technologies, challenges, and research directions. *IEEE Open. J. Commun. Soc.* https://doi.org/10.1109/ojcoms.2020.3010270 (2020).
42. Lu, S. & Li, X. Quantum-resistant lightweight authentication and key agreement protocol for fog-based microgrids. *IEEE Access.* **9**, 27588–27600. https://doi.org/10.1109/access.2021.3058180 (2021).
43. Farouk, A., Alahmadi, A., Ghose, S. & Mashatan, A. Blockchain platform for industrial healthcare: vision and future opportunities. *Comput. Commun.* **154**, 223–235. https://doi.org/10.1016/j.comcom.2020.02.058 (2020).
44. Pavithran, D., Shaalan, K., Al-Karaki, J. N. & Gawanmeh, A. Towards building a blockchain framework for IoT. *Cluster Comput.* https://doi.org/10.1007/s10586-020-03059-5 (2020).
45. Tran, N. K., Babar, A., Boan, J. & M., & Integrating blockchain and internet of things systems: A systematic review on objectives and designs. *J. Netw. Comput. Appl.* https://doi.org/10.1016/j.jnca.2020.102844 (2020).

46. Zhu, H., Wang, X., Chen, C. M. & Kumari, S. Two novel semi-quantum-reflection protocols applied in connected vehicle systems with blockchain. *Comput. Electr. Eng.* **86**, 106714. https://doi.org/10.1016/j.compeleceng.2020.106714 (2020).
47. Kumari, A., Gupta, R. & Tanwar, S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* **172**, 102–118. https://doi.org/10.1016/j.comcom.2021.03.005 (2021).
48. El-Latif, A. et al. Providing end-to-end security using quantum walks in IoT networks. *IEEE Access.* 1–1. https://doi.org/10.1109/access.2020.2992820 (2020).
49. Gui, G., Liu, M., Tang, F., Kato, N. & Adachi, F. 6G: opening new horizons for integration of comfort, security and intelligence. *IEEE Wirel. Commun.* https://doi.org/10.1109/mwc.001.1900516 (2020).
50. Lone, A. H. & Naaz, R. Demystifying cryptography behind blockchains and a vision for post-quantum blockchains. In *2020 IEEE International Conference for Innovation in Technology (INOCON)*. https://doi.org/10.1109/inocon50539.2020.9298215 (2020).
51. Awan, U., Hannola, L., Tandon, A., Goyal, R. K. & Dhir, A. Quantum computing challenges in the software industry. A fuzzy AHP-based approach. *Inf. Softw. Technol.* **147**, 1–19. https://doi.org/10.1016/j.infsof.2022.106896 (2022).
52. Trček, D. Cultural heritage preservation by using blockchain technologies. *Herit. Sci.* **10**(6), 1–11. https://doi.org/10.1186/s40494-021-00643-9 (2022).
53. Zeydan, E., Baranda, J. & Mangues-Bafalluy, J. Post-quantum blockchain-based secure service orchestration in multi-cloud networks. *IEEE Access.* **10**, 129520–129530. https://doi.org/10.1109/ACCESS.2022.3228823 (2022).
54. Leng, J., Zhou, M., Zhao, J. L., Huang, Y. & Bian, Y. Blockchain security: A survey of techniques and research directions. *IEEE Trans. Serv. Comput.* https://doi.org/10.1109/tsc.2020.3038641 (2021).
55. Malina, L. et al. Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access.* **9**, 36038–36077. https://doi.org/10.1109/access.2021.3062201 (2021).
56. Alkeilani Alkadri, N. et al. Deterministic wallets in a quantum world. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3372297.3423361 (2020).
57. Kumar, G., Saha, R., Lal, C. & Conti, M. Internet-of-forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Comput. Syst.* **120**, 13–25. https://doi.org/10.1016/j.future.2021.02.016 (2021).
58. Hassan, M. U., Rehmani, M. H. & Chen, J. Differential privacy in blockchain technology: A futuristic approach. *J. Parallel Distrib. Comput.* https://doi.org/10.1016/j.jpdc.2020.06.003 (2020).
59. Ranjith Kumar, M. V. & Bhalaji, N. Blockchain based chameleon hashing technique for privacy preservation in E-Governance system. *Wireless Pers. Commun.* https://doi.org/10.1007/s11277-020-07907-w (2020).
60. Perazzo, P., Arena, A. & Dini, G. An analysis of routing attacks against IOTA cryptocurrency. In *2020 IEEE International Conference on Blockchain (Blockchain)*. https://doi.org/10.1109/blockchain50366.2020.00075 (2020).
61. Kearney, J. J. & Perez-Delgado, C. A. Vulnerability of blockchain technologies to quantum attacks. *Array* **10**, 100065. https://doi.org/10.1016/j.array.2021.100065 (2021).
62. Sanka, A. I., Irfan, M., Huang, I. & Cheung, R. C. C. A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research. *Comput. Commun.* **169**, 179–201. https://doi.org/10.1016/j.comcom.2020.12.028 (2021).
63. Singh, S., Hosen, S., Yoon, B. & A. S. M., & Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access.* https://doi.org/10.1109/access.2021.3051602 (2021).
64. Zarrin, J., Wen Phang, H., Saheer, B., Zarrin, B. & L., & Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Comput.* https://doi.org/10.1007/s10586-021-03301-8 (2021).
65. Shrivas, M. K., Yeboah, T. & Brunda, S. S. Hybrid security framework for blockchain platforms. In *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*. https://doi.org/10.1109/icpc2t48082.2020.9071477 (2020).
66. Shrivas, M. K., Dean, T. Y. & Brunda, S. S. The disruptive blockchain security threats and threat categorization. In *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*. https://doi.org/10.1109/icpc2t48082.2020.9071475 (2020).
67. Sharma, V. & Lal, N. A detail dominant approach for IoT and blockchain with their research challenges. In *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)*. https://doi.org/10.1109/iconc345789.2020.9117533 (2020).
68. Pandl, K. D., Thiebes, S., Schmidt-Kraepelin, M. & Sunyaev, A. On the convergence of artificial intelligence and distributed Ledger technology: A scoping review and future research agenda. *IEEE Access.* **8**, 57075–57095. https://doi.org/10.1109/access.2020.2981447 (2020).
69. Chiang, C. F., Sengupta, S., Tekeoglu, A., Novillo, J. & Andriamanalimanana, B. A quantum assisted secure client-centric polyvalent blockchain architecture for smart cities. In *2020 IEEE 17th Annual Consumer Communications and Networking Conference (CCNC)*. https://doi.org/10.1109/ccnc46108.2020.9045188 (2020).
70. Li, Y., Yu, Y., Susilo, W., Hong, Z. & Guizani, M. Security and privacy for edge intelligence in 5G and beyond networks: challenges and solutions. *IEEE Wirel. Commun.* **28**(2), 63–69. https://doi.org/10.1109/mwc.001.2000318 (2021).
71. Bhushan, B., Sinha, P., Sagayam, K. M. & J, A. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Comput. Electr. Eng.* https://doi.org/10.1016/j.compeleceng.2020.106897 (2020).
72. Wang, J., Ding, Y., Xiong, N. N., Yeh, W. C. & Wang, J. GSCS: general secure consensus scheme for decentralized blockchain systems. *IEEE Access.* https://doi.org/10.1109/access.2020.3007938 (2020).
73. Sinai, N. K. & In, H. P. Performance evaluation of a quantum-resistant blockchain: a comparative study with Secp256k1 and schnorr. *Quantum Inf. Process.* **23**(99), 1–18. https://doi.org/10.1007/s11128-024-04272-6 (2024).
74. Kumar, G. et al. Decentralized accessibility of e-commerce products through blockchain technology. *Sustainable Cities Soc.* https://doi.org/10.1016/j.scs.2020.102361 (2020).
75. Sinai, N. K. & In, H. P. Performance evaluation of a quantumresistant blockchain: a comparative study with Secp256k1 and schnorr. *Quantum Inf. Process.* **23**(3), 99. https://doi.org/10.1007/s11128-024-04272-6 (2024).
76. Ferdous, M. S., Chowdhury, M. J. M. & Hoque, M. A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J. Netw. Comput. Appl.* **182**, 103035. https://doi.org/10.1016/j.jnca.2021.103035 (2021).
77. Guo, H. & Yu, X. A survey on blockchain technology and its security. *Blockchain: Res. Appl.* **3**(2), 1–15. https://doi.org/10.1016/j.bcra.2022.100067 (2022).
78. Alfa, A. A., Alhassan, J. K., Olaniyi, O. M. & Olalere, M. Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions. *J. Reliable Intell. Environ.* https://doi.org/10.1007/s40860-020-00116-z (2020).
79. Li, J., Peng, Z., Liu, A., He, L. & Zhang, Y. Analysis and future challenge of blockchain in civil aviation application. In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*. https://doi.org/10.1109/iccc51575.2020.9345297 (2020).
80. Nasir, A. et al. What is core and what future holds for blockchain technologies and cryptocurrencies: A bibliometric analysis. *IEEE Access.* **9**, 989–1004. https://doi.org/10.1109/access.2020.3046931 (2021).
81. Wustmans, M., Haubold, T. & Bruens, B. Bridging trends and patents: combining different data sources for the evaluation of innovation fields in blockchain technology. *IEEE Trans. Eng. Manage.* https://doi.org/10.1109/tem.2020.3043478 (2021).
82. Raikwar, M., Gligoroski, D. & Velinov, G. Trends in development of databases and blockchain. In *2020 Seventh International Conference on Software Defined Systems (SDS)*. https://doi.org/10.1109/sds49854.2020.9143893 (2020).
83. Wu, F., Zhou, B., Jiang, J., Lei, T. & Song, J. Blockchain privacy protection based on post quantum threshold algorithm. *Computers Mater. Continua*. **76**(1), 957–973. https://doi.org/10.32604/cmc.2023.038771 (2023).

Author contributions

All authors contributed to the study's conception and design. Material preparation, data collection, and analysis were performed By Dr. Nalavala Ramanjaneya Reddy, Supriya Suryadevara, Dr. K. Guru Raghavendra Reddy, Dr. Ramisetty Umamaheswari, Ramakrishna Guttula, Dr. Rajitha Kotoju. The first draft of the manuscript was written by Dr. Nalavala Ramanjaneya Reddy all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Declarations

Consent for publication

The authors give consent for their publication.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to N.R.R.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.