

# Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense

Yaser Baseri, Abdelhakim Hafid, Yahya Shahsavari, Dimitrios Makrakis and Hassan Khodaiemehr

**Abstract**—The advent of Quantum Computing (QC) poses significant threats to the cryptographic foundations of Blockchain (BC) systems, as quantum algorithms like Shor’s and Grover’s undermine the security of public-key cryptography and hash functions. This research conducts a comprehensive risk assessment of quantum vulnerabilities across critical BC components, including consensus mechanisms, smart contracts, and digital wallets. Leveraging the STRIDE threat modeling framework, we analyze threat vectors specific to QC, identifying key areas most susceptible to quantum-enabled attacks, such as private key compromise, consensus disruptions, and smart contract integrity risks. Our contributions provide actionable recommendations and mitigation strategies, including a detailed security blueprint for quantum resilience, encompassing post-quantum cryptography, quantum-safe key exchange protocols, and quantum-resistant hash functions. We offer best practices for implementation, focusing on key management, secure coding, and network security to strengthen BC components against quantum threats. To mitigate the risk of QC during the transition period from classical to quantum-resistant BCs, we present two hybrid BC architectures. As part of a comprehensive quantum resilience strategy, these architectures facilitate a secure and scalable migration by integrating platform-specific adaptations that balance security, adaptability, and operational efficiency. Our analysis extends to major BC platforms, including Bitcoin, Ethereum, Ripple, Litecoin, and Zcash, providing platform-specific vulnerability assessments and highlighting unique weaknesses in the quantum era. By identifying vulnerabilities, developing proactive defense strategies, and adopting a structured hybrid migration approach, this research equips BC stakeholders with a robust framework to achieve long-term security and resilience against emerging quantum threats. Finally, we delve into the challenges and research directions associated with integrating emerging technologies, including quantum machine learning, artificial intelligence, and Web3, with BC systems, and discuss the new threats that may arise from this convergence in the QC era.

**Index Terms**—Quantum-Secure Blockchain, Risk Assessment, Migration Strategies, Hybrid Blockchain, Composite Approach, Non-Composite Approach, Proactive Defense, Post-Quantum Cryptography, Quantum Computing Threats.

## I. INTRODUCTION

THE cryptographic underpinnings of BC security are vulnerable to the significant threat posed by the rapidly advancing field of QC. Quantum computers, with their unparalleled processing power, undermine the integrity of digital signatures, encryption schemes, and hash functions—the

foundational components that enable secure transactions and tamper-resistant data storage within BC ecosystems [1], [2]. This vulnerability extends to both asymmetric and symmetric cryptographic algorithms, as well as cryptographic hash functions, all of which are integral to BC security. Quantum algorithms such as Shor’s [3], [4] directly threaten public-key cryptography, including RSA, Digital Signature Algorithm (DSA), and Elliptic Curve Digital Signature Algorithm (ECDSA), by efficiently solving the underlying mathematical problems upon which these algorithms rely. This compromises private keys in BC systems, such as those used in Bitcoin’s ECDSA-based transaction model. While symmetric cryptography is comparatively more resilient, Grover’s algorithm [5], [6] reduces the effective security of symmetric encryption schemes by accelerating brute-force attacks. Specifically, Grover’s algorithm reduces the key search space from  $2^n$  to  $2^{n/2}$ , effectively halving the security strength of the encryption. This necessitates longer key lengths (e.g., AES-256 instead of AES-128) to maintain equivalent security. Hash functions, which are critical for BC consensus mechanisms and data integrity, are also at risk. The Brassard-Hoyer-Tapp (BHT) algorithm [7] significantly accelerates the search for hash collisions, reducing the effective collision resistance of a hash function from  $2^n$  to  $2^{n/3}$  (i.e., one-third of the input size). For example, SHA3-256, frequently used for block hashing, would provide only around 85-bit security against quantum attacks. This reduction increases the risk of hash collisions, thereby undermining the immutability of BC systems. These vulnerabilities emphasize the urgent need for a dual approach: (1) implementing proactive quantum-resilient defense mechanisms and (2) transitioning to quantum-resistant cryptographic solutions across all BC ecosystems to safeguard their long-term viability.

This study investigates the risks associated with transitioning from non-quantum-safe cryptographic methods to quantum-resistant ones across various BC components [8]–[10]. It assesses vulnerabilities posed by quantum attacks on key components, such as the network, mining pools, transaction verification, smart contracts, and user wallets, which are susceptible to quantum threats. Such vulnerabilities can compromise BC integrity and security, posing risks of unauthorized access, data manipulation, and financial loss. To effectively counter these evolving threats during the transition phase, organizations must adopt a holistic security approach that integrates quantum-resistant cryptography with system design and continuous monitoring [11]–[13]. A hybrid migration strategy, gradually transitioning from classical to quantum-resistant cryptography, is essential to reduce risks during

Yaser Baseri, Abdelhakim Hafid, and Yahya Shahsavari are with Montreal Blockchain Lab, University of Montreal, Montreal, Canada. Emails: yaser.baseri@umontreal.ca; ahafid@umontreal.ca; yahya.shahsavari@umontreal.ca.

Dimitrios Makrakis is with School of Electrical Engineering and Computer Science, University of Ottawa, Canada. E-mail: dmakraki@uottawa.ca.

Hassan Khodaiemehr is with School of Engineering, The University of British Columbia (UBC), Canada. Email: hassan.khodaiemehr@ubc.ca.

this phase [14]–[16]. This approach is critical for ensuring robust security, as organizations may encounter challenges like increased key sizes, which require adjustments to network traffic handling, and implementation complexities that must be managed carefully throughout the transition [17]–[19].

While transitioning to quantum-resistant cryptography is essential, it does not fully address all potential threats, as BC systems remain vulnerable to sophisticated attack vectors beyond encryption weaknesses [20]–[22]. In the post-transition stage, organizations face challenges across system architecture, network infrastructure, and operational processes [23], [24]. For example, quantum-resistant cryptography may create new vulnerabilities in consensus mechanisms, allowing for unauthorized control or data tampering, and introduce complexities like increased latency and fragmented network traffic, which can lead to performance bottlenecks or expose systems to Denial of Service (DoS) attacks. Additionally, the coexistence of legacy and quantum-resistant protocols in hybrid architectures may result in security gaps, while side-channel attacks could exploit hardware-level details in cryptographic operations. These risks underscore the need for continuous refinement and vigilant monitoring of the BC ecosystem beyond just cryptographic upgrades.

This paper investigates the challenges and vulnerabilities posed by QC to BC security, leveraging the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) framework [25], [26] to identify and prioritize threats. We emphasize the importance of quantum-resistant measures and analyze vulnerabilities before, during, and after transitioning to quantum-safe algorithms, providing insights for effective countermeasures. As quantum threats escalate, especially during the transition to quantum-resistant BCs, a proactive approach to risk assessment and defense strategies becomes imperative. The urgency to identify and mitigate vulnerabilities is heightened, necessitating robust defense strategies to ensure the adaptability and resilience of BC ecosystems. By advocating for proactive measures, including quantum-resistant solutions, we aim to safeguard the integrity and longevity of BC networks. Through early vulnerability identification and promotion of quantum-resistant methods, we seek to fortify BC networks against potential quantum threats, ensuring their continued operation in the quantum era.

#### A. Contribution

This research offers substantial advancements in the field of BC security within the context of emerging QC technologies. The key contributions are as follows:

1. **Comprehensive Risk Assessment:** This research evaluates BC vulnerabilities and potential hazards posed by QC. It identifies weaknesses and assesses risk severity, providing valuable insights for proactive defense strategies.
2. **Platform-Specific Vulnerability Analysis:** An analysis of the vulnerabilities in leading BC platforms like Bitcoin, Ethereum, Ripple, Litecoin, and Zcash is included. This analysis highlights platform-specific weaknesses and their implications for security in the quantum era.

3. **Hybrid BC Approach for Secure Migration:** This research introduces innovative hybrid BC architectures designed to facilitate a seamless transition from legacy systems to quantum-resistant cryptography. These architectures balance security, adaptability, and migration efficiency, allowing stakeholders to navigate with confidence within the evolving QC landscape and ensure the long-term security and viability of their BC systems.

4. **Actionable Mitigation Strategies Empowering Stakeholders:** We provide practical guidance for developing secure migration strategies and proactive measures to fortify BC components against quantum threats. Our research emphasizes the adoption of quantum-resistant solutions and advocates for robust defense mechanisms to counter emerging quantum risks, equipping BC stakeholders with the knowledge and tools to ensure the long-term viability of BC technology.

These contributions collectively advance the understanding of quantum threats to BC security, offering actionable guidance for stakeholders to fortify their systems against emerging quantum-induced cyber threats.

TABLE I: List of Abbreviations

Abbreviation	Description
AI	Artificial Intelligence
AML	Anti-Money Laundering
BC	Blockchain
BFT	Byzantine Fault Tolerance
DAGs	Directed Acyclic Graphs
DeFi	Decentralized Finance
DH	Diffie–Hellman
DI-QRNGs	Device-Independent Quantum Random Number Generators
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECC	Elliptic-Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
FIFO	First In, First Out
I	Impact
IDS/IPS	Intrusion Detection and Prevention Systems
KEM/ENC	Key Encapsulation Mechanism/Encryption
KYC	Know Your Customer
L	Likelihood
MAC	Message Authentication Code
ML	Machine Learning
MPC	Multi-Party Computation
NIST	National Institute of Standards and Technology
PoA	Proof of Authority
PoR	Proof of Randomness
PoS	Proof of Stake
POSets	Partially Ordered Sets
PoW	Proof of Work
PQC	Post-Quantum Cryptography
PRF	Pseudorandom Function
QC	Quantum Computing
R	Risk
RNGs	Random Number Generators
SegWit	Segregated Witness
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TLS	Transport Layer Security
VDFs	Verifiable Delay Functions
VRFs	Verifiable Random Functions
ZKP	Zero-Knowledge Proof

#### B. Abbreviations

To ensure clarity and consistency, Table I provides a comprehensive list of abbreviations used throughout this document. This Table serves as a quick reference for readers to familiarize

themselves with the terminology and acronyms frequently referenced in the text.

### C. Related Works

Recent research in BC security for the quantum era has focused primarily on vulnerability analysis [1], [32], [34], proactive security measures [2], [28], [33], and stakeholder empowerment [2], [30], [32]. However, existing studies often treat these challenges in isolation, lacking a unified framework for ensuring BC security in the quantum era.

Our research distinguishes itself by offering a holistic approach to BC quantum-security. First, we provide a comprehensive risk assessment framework that systematically evaluates threats across all fundamental BC components, including consensus mechanisms, cryptographic algorithms, smart contracts, and network protocols. This approach goes beyond previous studies that focus only on specific vulnerabilities [1], [32], [34]. Second, we conduct a detailed vulnerability analysis of the major BC platforms, including Bitcoin, Ethereum, Ripple, Litecoin, and Zcash. Unlike previous works that provide general security discussions [1], [34], [35], our analysis offers in-depth platform-specific insights, including vulnerability analysis, threat modeling, and risk assessment, enabling a deeper understanding of quantum threats and their potential impact on specific cryptographic algorithms, consensus

mechanisms, and smart contract vulnerabilities. Third, we introduce novel hybrid BC architectures that leverage Post-Quantum Cryptography (PQC) to ensure a secure and efficient quantum-resistant future. Unlike existing approaches that rely on quantum cryptography [31], [38], [39], our focus on PQC, standardized by National Institute of Standards and Technology (NIST), provides a practical and sustainable solution. Our hybrid architectures combine the strengths of classical and quantum-resistant cryptographic primitives, offering a robust and flexible framework for securing BC systems [11]–[13]. Finally, we provide actionable guidance for stakeholders, empowering them to navigate the quantum era effectively. Unlike existing works that may focus on specific environments or pre-transition stages [2], [32], our research offers a comprehensive roadmap that covers all phases of the quantum transition, including risk assessment, vulnerability analysis, migration strategies, and post-migration security considerations.

Table II summarizes these distinctions, highlighting the unique contributions of our research. By combining a comprehensive risk assessment, platform-specific vulnerability analysis, hybrid architecture based on PQC and actionable stakeholder guidance, our work offers a robust solution to secure BCs in the quantum era.

TABLE II: Related Works on BC Security Risk Assessment in the Quantum Era

Reference	Focus	Risk Assessment	Vulnerability Analysis	Platform Analysis	Mitigation Strategies	Stakeholder Empowerment	Hybrid Migration Approach
Yang et al. (2024) [27]	Comparison of post-quantum and quantum BCs for securing transactions in the quantum era	–	Survey of vulnerabilities in core components	–	Highlights need for quantum-resistant cryptography without specific solutions	–	Brief mention of hybrid approaches, no detailed migration strategy
Gharavi et al. (2024) [28]	Survey on post-quantum BC security challenges and solutions for IoT	–	Vulnerability analysis focusing on IoT BC threats	–	Emphasizes post-quantum cryptographic methods for IoT security; no detailed migration strategy	Provides insights on integrating post-quantum cryptography in IoT environments	–
Karakaya & Ulu (2024) [29]	Survey on post-quantum based security for edge computing in IoT	–	Broad discussion on post-quantum vulnerabilities in edge and IoT systems	High-level review of edge platforms without specific technical analysis	Highlights importance of lattice-based approaches, lacks concrete solutions	–	–
Allende et al. (2023) [2]	Proposes an end-to-end framework for achieving quantum resistance in existing BC networks	–	Analyzes vulnerabilities of BC cryptographic protocols due to QC threats	Implementation demonstrated on Ethereum-compatible platform (LACChain)	Employs post-quantum methods like Falcon signatures and quantum entropy for security; lacks post-migration analysis	Empowers stakeholders specifically in Ethereum and EVM-compatible environments through open-source tools	Focuses on EVM compatibility for post-quantum signatures (e.g., Falcon); no detailed, BC-specific migration strategy.
Kaushik & Kumar (2023) [30]	Demystifying quantum BC for healthcare	–	General discussion on healthcare security challenges, lacks specific vulnerability analysis	–	Highlights potential of quantum BC but lacks concrete strategies	–	–
Liu et al. (2023) [31]	Proposing a quantum-secure BC scheme using hybrid classical-quantum communication protocols (uses quantum cryptography and not PQC, which is currently being standardized by NIST)	–	–	–	Implicitly addressed (considers security against quantum attacks using QPoA and IQS)	–	Proposes a hybrid classical-quantum communication protocol for managing classical BCs (not PQC, which is currently being standardized by NIST)
Khodaiemehr et al. (2023) [32]	Survey of quantum threats and cryptographic vulnerabilities with suggested mitigation strategies	–	Identifies vulnerabilities in cryptographic algorithms	–	Covers quantum-resistant defenses with a focus on pre- and mid-transition stages; lacks post-migration analysis	Guides stakeholders mainly for pre- and mid-transition, with limited post-migration guidance	Discusses hybrid strategies (KEMs and signatures) for general transition process not BC specific.
Swathi & Dragan (2022) [33]	Survey of the impact of quantum computing on BC security	–	Analyzes vulnerabilities across various BC layers	–	Mentions the need for quantum-resistant cryptography without specific solutions	–	Briefly mentions hybrid approaches related to cryptographic compatibility, not focused on migration
Faridi et al. (2022) [34]	Examines BC security in a quantum context with emphasis on post-quantum cryptography	–	Analyzes vulnerabilities at different BC layers against quantum threats	Broad analysis across multiple BC layers	Highlights post-quantum cryptography techniques as mitigation, but lacks post-migration analysis	–	–
Naz & Kumar (2022) [35]	Surveying Quantum-Proof BC Security: The Era of Exotic Signatures	–	Analysis of vulnerabilities of exotic post-quantum signatures	–	Highlights post-quantum cryptography techniques as mitigation, but lacks post-migration analysis	–	Briefly mentions hybrid approaches in the context of signature compatibility but does not focus on BC migration strategies
Yang et al. (2022) [36]	Theoretical analysis of quantum BC for decentralized identity management	–	–	–	–	Presents a conceptual framework for quantum-based decentralized identity; limited practical guidance	–
Kumar et al. (2021) [37]	Survey of quantum technologies with emphasis on drone networks and quantum communication	–	General discussion on potential quantum vulnerabilities	–	Explores basic post-quantum cryptographic techniques for drones and networks; lacks post-migration analysis	–	–
Kearney et al. (2021) [11]	Vulnerability analysis of specific BCs (Bitcoin, Ethereum, etc.) against quantum threats	–	Detailed vulnerability analysis of cryptographic protocols in selected BCs	Analysis of different platforms, including Bitcoin, Ethereum, etc.	–	–	Limited mention of hybrid approach; lacks detailed migration strategy
Edwards et al. (2020) [38]	Review of quantum and hybrid quantum/classical BC protocols (quantum protocols use quantum cryptography, not PQC, which is currently being standardized by NIST)	–	–	–	Mentions quantum cryptography but lacks specific mitigation strategies	–	Proposes analysis of possible hybrid approaches for combining classical and quantum cryptography in BCs (not using PQC, which is currently being standardized by NIST)
<b>Our Work</b>	Risk assessment & migration strategies for quantum-resistant BCs	Comprehensive risk assessment approach for fundamental BC components via analyzing threats, vulnerabilities, and assessing risks	Thorough analysis of vulnerabilities in core BC components	Vulnerability analysis of specific BCs (Bitcoin, Ethereum etc.)	Emphasizes the need for proactive measures and quantum-resistant solutions. Introduce mitigation strategies and proactive measures for all stages of the transition path (pre, throughout, and post).	Equips stakeholders with actionable insights for navigating the quantum era	Proposes comprehensive analysis of possible hybrid approaches for combination of classic and post quantum BC and provide a way to have smooth transition from classic BC to post-quantum one

## D. Organization

The rest of the paper is organized into the following sections: Section II describes the approach used to conduct a comprehensive risk assessment, focusing on quantum-specific threats and vulnerabilities that arise during the migration of BC systems. Section III discusses cryptographic standards and QC's potential cyber impact and risk assessment. Section IV explores the quantum impact on the components of the BC technology, covering the BC network, mining pools, transaction verification mechanisms, smart contracts, and user wallets. Section V analyzes the security implications of QC in different BC roles, presenting strategies for quantum-safe migration. Section VI addresses the challenges of mitigating QC impacts and transitioning to quantum-secure BC systems. Section VII details a groundbreaking approach using hybrid BCs to facilitate a smooth transition to quantum-resistant cryptography in BCs. Section VIII analyzes the security posture of major BC platforms such as Bitcoin, Ethereum, Ripple, Litecoin and Zcash in the context of QC threats. Section IX examines the current landscape of post-quantum BCs, their cryptographic underpinnings, associated security concerns, and the challenges of achieving quantum-resilient interoperability. Section X explores future research directions to address QC challenges facing BC, particularly as the integration with emerging technologies like Web3 and quantum AI intensifies these issues. Section XI summarizes key findings, emphasizes proactive security measures and collaboration, and calls for ongoing efforts to protect BC systems from QC threats.

## II. QUANTUM-SAFE MIGRATION RISK ASSESSMENT APPROACH

This study utilizes a comprehensive risk assessment methodology to evaluate the security risks associated with BC migration towards quantum-safe systems. We employ a four-stage risk assessment methodology (preparation, assessment, communication, maintenance), following NIST guidelines [40]. The focus is on the assessment stage, prioritizing threat, vulnerability, likelihood, impact, and risk. Figure 1 provides an overview of this risk assessment approach.

### A. Prepare for Risk Assessment

Aligned with NIST guidelines [40], this risk assessment framework prepares for BC migration to quantum-safe systems by defining the purpose, scope, assumptions, and a tailored risk model. The primary goal is to identify and prioritize quantum-related threats at all migration stages (pre-, during, and post-migration) across BC components such as consensus mechanisms, cryptographic algorithms, and network protocols. While this analysis assumes both the emergence of quantum threats within the migration timeframe and the availability of PQC solutions, the current limitations in PQC efficiency and interoperability present substantial challenges. This research leverages a qualitative, STRIDE-based risk model [26], [41] to categorize threats identified in academic literature and industry reports on known BC vulnerabilities. Evaluation criteria (Low, Medium, High) are defined for likelihood and impact to effectively prioritize risks. This structured approach provides a

comprehensive understanding of the quantum threat landscape, supporting the development of robust mitigation strategies.

### B. Conduct Assessment

Conducting the assessment involves five key tasks: (1) identifying potential threat sources and events; (2) identifying vulnerabilities within the system; (3) determining the likelihood of each identified vulnerability; (4) determining the impact of each vulnerability; and (5) aggregating these factors to assess the overall risk. Figure 1 summarizes the assessment process.

*Task 1. Identify Threat Sources and Events:* To identify potential threats, we consider quantum-specific risks such as quantum algorithm attacks (e.g., Shor's and Grover's algorithms), quantum side-channel attacks (exploiting timing or power differences), and quantum hardware attacks (malicious quantum devices). These threats can compromise BC systems at various levels, including cryptographic algorithms, consensus mechanisms, and smart contracts. By understanding these risks, we can develop effective mitigation strategies to protect BC systems in the quantum era.

*Task 2. Identify Vulnerabilities and Predisposing Conditions:* We conduct a comprehensive review of BC components to identify vulnerabilities that could be exploited by quantum attacks. Key focus areas include quantum-resistant cryptographic algorithms (lattice-based, code-based, and multivariate), BC protocols (consensus mechanisms, smart contracts, and network protocols), and quantum-safe key management (key generation, distribution, and storage).

TABLE III: Evaluation Criteria for Likelihood Levels

Likelihood	High	<ul style="list-style-type: none"> <li>• High likelihood of exploitation due to critical vulnerabilities or weak cryptographic protections.</li> <li>• Broad network exposure, making exploitation accessible to adversaries with quantum capabilities.</li> <li>• High probability of intent and capability from quantum threat actors.</li> </ul>
	Medium	<ul style="list-style-type: none"> <li>• Known vulnerabilities, but partial mitigations limit ease of exploitation.</li> <li>• Moderate network exposure; some access restrictions, but feasible for a skilled quantum adversary.</li> <li>• Exploitation possible with moderate quantum resources and expertise.</li> </ul>
	Low	<ul style="list-style-type: none"> <li>• No significant vulnerabilities for quantum exploitation; strong quantum-resistant cryptography in place.</li> <li>• Minimal network exposure; attacks require highly specialized access and resources.</li> <li>• Unlikely exploitation due to high barriers and limited feasibility.</li> </ul>

*Task 3. Determine Likelihood of Occurrence:* Using a qualitative risk assessment approach, we evaluate the likelihood of vulnerabilities being exploited by a quantum attacker. We establish a set of qualitative criteria and categorize the likelihood into three levels: *Low (L)*, *Medium (M)*, and *High (H)*. The criteria used for this assessment are detailed in Table III. To assess cyber risks associated with PQC algorithms, we evaluate factors such as exploitability, availability

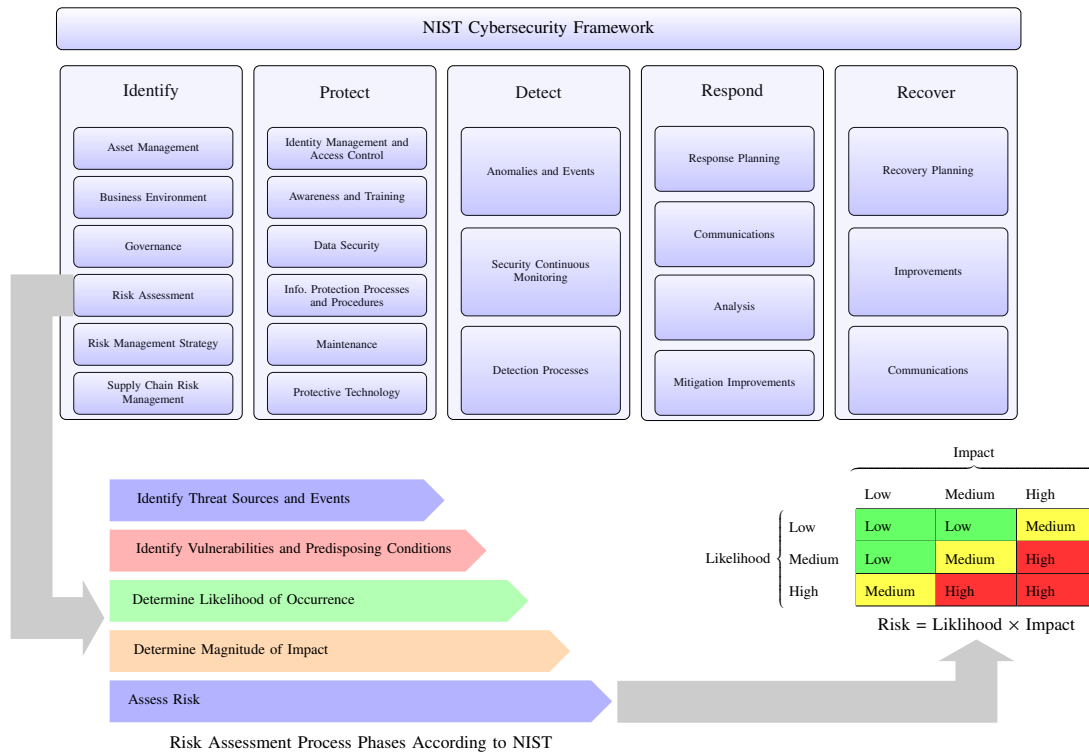


Fig. 1: Quantum-Safe Migration Risk Assessment Approach

of countermeasures, and criteria from NIST-SP 800-30 Appendix G [42]. Likelihood levels are categorized based on exploitability, attack complexity, attacker motivation, and the effectiveness of countermeasures.

TABLE IV: Evaluation Criteria for Impact Levels

		Criteria
Impact	High	<ul style="list-style-type: none"> <li>Severe compromise, including exposure of critical data or loss of cryptographic integrity.</li> <li>Extensive operational downtime or significant disruptions to BC consensus mechanisms.</li> <li>High financial, regulatory, and reputational risks with long-term effects.</li> </ul>
	Medium	<ul style="list-style-type: none"> <li>Partial compromise of data integrity or limited operational impact.</li> <li>Moderate data or service disruption with manageable recovery time.</li> <li>Moderate financial or reputational consequences; potential regulatory concerns.</li> </ul>
	Low	<ul style="list-style-type: none"> <li>Minimal operational disruption or data exposure; negligible security implications.</li> <li>Temporary disruptions without lasting effects on BC integrity or user trust.</li> <li>Limited financial or reputational risk.</li> </ul>

*Task 4. Determine Magnitude of Impact:* The impact levels, defined as *Low (L)*, *Medium (M)*, and *High (H)*, reflect the potential severity of a quantum threat event (see Table IV for evaluation criteria). These criteria, based on NIST-SP 800-30 Appendix H [42], consider the possible harm to BC assets, system stability, user satisfaction, data confidentiality, and organizational reputation.

*Task 5. Assess Risk:* Risk is determined by combining likeli-

hood and impact levels, visualized in a risk matrix (see Figure 2). Risk levels—High, Medium, and Low—help prioritize vulnerabilities and guide mitigation strategies.

		Impact		
		Low	Medium	High
Likelihood	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Fig. 2: Qualitative Risk Assessment based on Likelihood and Impact Levels

### III. CRYPTOGRAPHIC STANDARDS AND QUANTUM COMPUTING: CYBER IMPACT AND RISK ASSESSMENT

This paper proposes a security framework to safeguard BC technology from QC threats. The framework prioritizes securing critical components for robust BC protection. However, to effectively mitigate these risks, we must understand the threat QC poses to classical cryptographic algorithms, the foundation of BC security. This section assesses the impact on both traditional and post-quantum cryptographic algorithms standardized by the NIST. This risk assessment prioritizes threats based on their potential impact and exploitability. Advances in QC significantly threaten both public-key and symmetric-key cryptography, necessitating a thorough risk assessment that accounts for emerging quantum-resistant solutions under development by NIST.

## A. Classic Cryptographic Standards and Quantum Computing: Cyber Impact and Risk Assessment

Widely used classical cryptographic algorithms—both symmetric and asymmetric—are increasingly vulnerable to QC. Quantum algorithms such as Shor’s, Grover’s and Brassard et al.’s algorithm [7] can compromise the hard problems underlying modern cryptography, threatening the security of diverse applications and communications. This section analyzes the vulnerabilities of existing cryptographic systems to motivate the need for quantum-resistant alternatives.

### A.1. Risk Assessment

Understanding the risks of migrating to quantum-resistant cryptography requires predicting the arrival of powerful quantum computers and their impact on classical cryptosystems. This analysis examines the timeline for the potential emergence of such computers within the next 5 to 30 years. We assess the cumulative likelihood of significant quantum threats to classical cryptosystems over this timeframe. Figure 3 summarizes this progression, incorporating insights from various quantum experts on the “quantum threat” timeline [43]. Here, “quantum threat” specifically refers to the ability to break RSA-2048 encryption within 24 hours using a quantum computer. However, this threat also applies to other cryptosystems, notably ECC, which is widely used in BC and may be more vulnerable to attack by Shor’s algorithm than RSA at equivalent security levels. A thorough risk assessment therefore requires comparing algorithms’ “quantum strength” relative to this RSA benchmark, considering their susceptibility to Shor’s, Grover’s, and Brassard et al.’s algorithms.

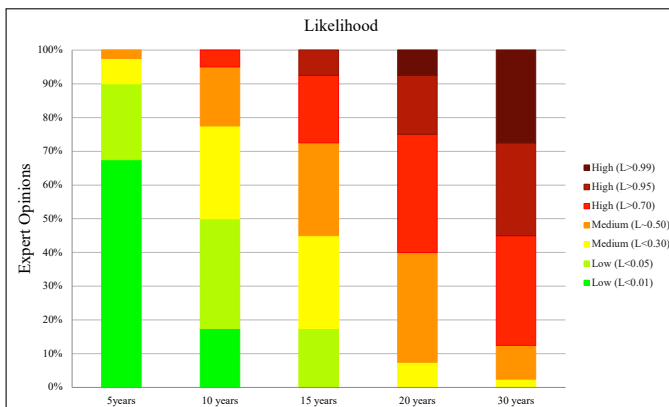


Fig. 3: Cumulative Expert Opinions Related to Quantum Threat to Classic Cryptography

**A.1.1. Expected Likelihood of Quantum Threat** To assess the “expected likelihood of the quantum threat for classical cryptosystems” over different periods (5, 10, 15, 20, and 30 years), we analyze predictions made by experts in Figure 3. For each period (e.g., 5 years), the expected likelihood is calculated by multiplying the agreed-upon likelihoods of predictions for that period by the probability of those predictions, and then

summing them up:

$$E_{\text{period}_j}[\text{likelihood}] = \sum_{\omega_i \in [0,1]} \text{likelihood}_{\text{period}_j}(\omega_i) \times \Pr_{\text{period}_j}(\omega_i),$$

where,  $\omega_i$  represents subsets of  $[0, 1]$ , with their union equaling  $[0, 1]$ .  $\Pr_{\text{period}_j}(\omega_i)$  for each period  $j$  is determined by the fraction of expert opinions that agreed on prediction  $\omega_i$  for that period, relative to the total number of predictions. Our

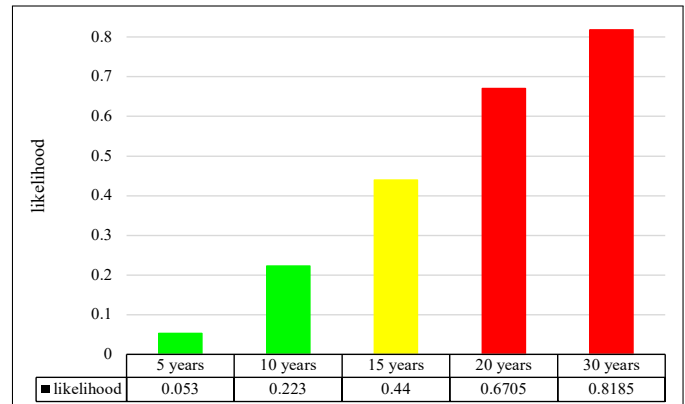


Fig. 4: Expected Likelihood of Quantum Threat for Classic Cryptography Within 30 Years

likelihood assessment categorizes quantum threat likelihood into three levels: low, medium, and high. As depicted in Figure 4, the expected likelihood of a quantum threat within 10 years is low, within 15 years is medium, and beyond 20 years is high.

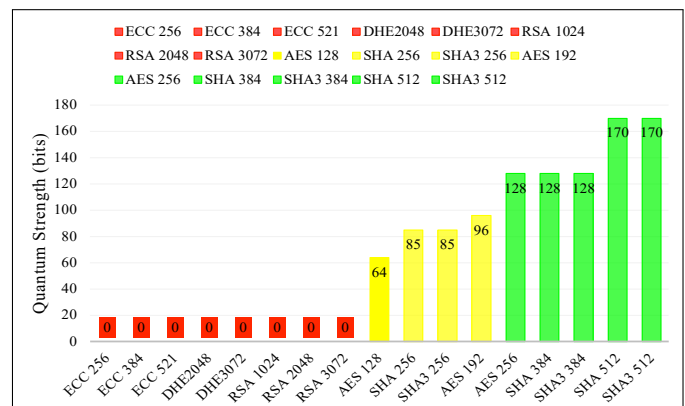


Fig. 5: Expected Impact of Quantum Threat for Classic Cryptography

### A.1.2. Quantum Impact Assessment

To assess the impact of quantum threats on different classical cryptographic algorithms, we evaluate their quantum security strength, which quantifies their resilience against attacks from quantum computers [44]. This measure is crucial for understanding the vulnerabilities of existing systems and prioritizing mitigation efforts. The impact of QC on a cryptographic algorithm is considered high if the algorithm’s quantum strength is less than 64 bits, low if it is greater than or equal to 128 bits, and medium for values between these

TABLE V: Classic Cryptographic Standards and Quantum Computing: Cyber Impact and Risk Assessment

Crypto Type	Algorithms	Variants	Key Length (bits)	Strengths (bits)		Vulnerabilities	STRIDE threats	L	I	R	QC-Resistant Alternatives
				Classic	Quantum						
Asymmetric	ECC [45]	ECC 256	256	128	0	Broken by Shor's Algorithm [3].	For digital signature: <ul style="list-style-type: none"> <li>• Spoofing: Shor's Algorithm allows forging of digital signatures.</li> <li>• Tampering: Integrity checks can be bypassed due to signature forgery.</li> <li>• Repudiation: Valid signatures can be forged, denying the origin of the message.</li> </ul> For Key Encapsulation Mechanism/Encryption (KEM/ENC): <ul style="list-style-type: none"> <li>• Info. Disclosure: KEM/ENC algorithms can be broken, revealing encrypted data.</li> </ul>	M	H	H	Algorithms presented in Table VI.
		ECC 384	384	256	0			M	H	H	
		ECC 521	521	256	0			M	H	H	
	FFDHE [46]	DHE 2048	2048	112	0			M	H	H	
		DHE 3072	3072	128	0			M	H	H	
	RSA [47]	RSA 1024	1024	80	0			M	H	H	
		RSA 2048	2048	112	0			M	H	H	
		RSA 3072	3072	128	0			M	H	H	
Symmetric	AES [48]	AES 128	128	128	64	Weakened by Grover's Algorithm [5].	• Info. Disclosure: Grover's algorithm reduces the effective key length, making brute-force attacks feasible.	M	M	M	Larger key sizes are needed.
		AES 192	192	192	96			M	M	M	
		AES 256	256	256	128			M	L	L	
	SHA2 [49]	SHA 256	-	128	85			M	M	M	
		SHA 384	-	192	128			M	L	L	
		SHA 512	-	256	170			M	L	L	
	SHA3 [49]	SHA3 256	-	128	85			M	M	M	
		SHA3 384	-	192	128			M	L	L	
		SHA3 512	-	256	170			M	L	L	
								M	L	L	

(see Figure 5).

### A.1.3. Evaluating Risk

The overall Risk (R) associated with a cryptographic algorithm is evaluated based on both the Likelihood (L) of a successful exploit and the potential Impact (I) of such an attack. This evaluation is visualized using a risk matrix, as depicted in Figure 2. By analyzing both likelihood and impact, we can effectively assess the security posture of existing algorithms and develop appropriate mitigation strategies for the transition to quantum-resistant cryptography. Table V provides a detailed analysis of conventional cryptographic algorithms before transitioning to quantum-safe solutions. This analysis considers classical and quantum security strength, inherent vulnerabilities, emerging quantum threats, potential quantum-resistant remedies, and associated risks. For our evaluation, we consider a 15-year timeline during which the likelihood of quantum threats to classical cryptosystems is assessed as medium (see Figure 4). This assumption can be easily changed for other periods.

### B. Selected Quantum-Resistant Cryptographic Standards: Cyber Impact and Risk Assessment

The threat of QC necessitates a transition to post-quantum cryptography (PQC). NIST has led a standardization effort and PQC algorithms are designed to safeguard public-key cryptography (key encapsulation/encryption and digital signatures) against quantum attacks. Several promising PQC categories have emerged, including lattice-based [50]–[52], code-based [53]–[55], hash-based [56], and isogeny-based [57] approaches. However, ongoing research remains vital to ensure their long-term security. NIST announced the first four PQC candidates for standardization in 2022, along with candidates for a fourth round of analysis [58]. Additionally, NIST has solicited comments on the initial public drafts of three Federal Information Processing Standards: FIPS 203 [59], FIPS 204 [60], and FIPS 205 [61]. These drafts outline quantum-resistant key establishment and digital signature schemes to safeguard against future quantum attacks [62].

#### B.1. Security Evaluation and Vulnerability Analysis

Recent discoveries of side-channel vulnerabilities in some NIST-standardized PQC algorithms highlight the critical need

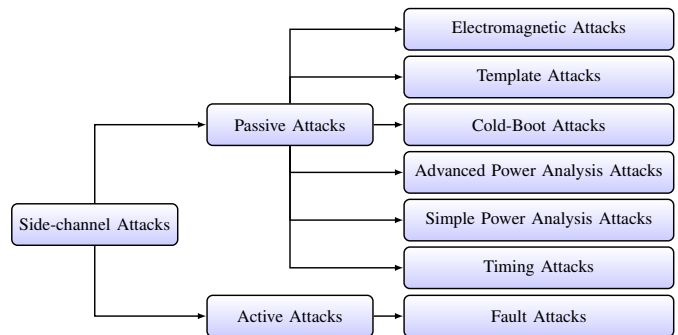


Fig. 6: Taxonomy of Attacks for NIST-Standardized Cryptographic Algorithms

for ongoing security assessments (see Figure 6). This section delves into these security challenges, examining the nature of attacks, potential mitigation strategies, and associated risks. Quantum attackers primarily aim to recover secret keys or forge digital signatures, exploiting information leakage during cryptographic operations, such as power consumption, electromagnetic radiation, or timing data, to potentially extract sensitive information like private keys. Table VI provides a specific overview of vulnerabilities in PQC algorithms, highlighting potential exploits and associated risks. This information is invaluable for ongoing NIST standardization efforts and the development of robust security measures against quantum threats.

#### B.2. Risk Assessment

To assess cyber risks associated with PQC algorithms, we evaluate factors such as exploitability (e.g., requirements for physical access, network or internet accessibility), availability of countermeasures (as detailed in Table VI), and criteria from NIST-SP 800-30 Appendix G [42]. Likelihood levels are categorized based on exploitability, attack complexity, attacker motivation, and the effectiveness of countermeasures:

- High:** Known vulnerabilities that can be exploited remotely (e.g., over the internet or network) without effective countermeasures, or that require minimal attacker sophistication or resources.
- Medium:** Known vulnerabilities that require physical access or specific conditions, or lack robust countermeasures when exploited remotely. Moderate attack complexity or skill

TABLE VI: NIST-Standardized Quantum-Resistant Cryptographic Algorithms: Cyber Impact and Risk Assessment

Algorithms	Description	FIPS Compliance	Attacks	Possible Countermeasures	STRIDE Threats	L	I	R	
Kyber [50]	Key encapsulation mechanism based on the Module Learning with Errors (M-LWE) problem, in conjunction with cyclotomic rings	Pending FIPS certification (FIPS 203 [59])	Fault Attacks [63]–[65]	<ul style="list-style-type: none"> <li>Masking decryption process by splitting secret key [64], [65].</li> <li>Checking the secret and error components of the LWE instances for known trivial weaknesses [63].</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure (by recovery of message and key [63]–[65]).</li> </ul>	M	M	M	
			Simple Analysis [66]	Power	<ul style="list-style-type: none"> <li>Masking of input [66].</li> <li>Randomizing the order of executed operations within an NTT computation or by inserting random dummy operations inside the NTT [66].</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure (by recovery of key [66]).</li> </ul>	M	M	M
			Advanced Power Analysis [67]–[69]	<ul style="list-style-type: none"> <li>Masking the Number Theoretic Transform (NTT), which is an integral part of efficient implementations of many lattice-based schemes [67].</li> <li>No countermeasures for the attack mentioned in [69].</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure (recovery of the transmitted symmetric key [67]).</li> </ul>	H	M	H	
			Electromagnetic Attacks [65], [70], [71]	<ul style="list-style-type: none"> <li>Masking the ECC procedures, including masking the decryption/decapsulation operations [64], [70], masking to protect the FO transform operations in the CCA setting [70], masking to protect the secret key [71].</li> <li>Discarding ciphertexts with a special structure or low entropy [71].</li> <li>Splitting the secret into random shares and thereafter randomizing the entire decryption or decapsulation [71].</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure (by full key extraction [70], [71] or by disclosing bits of the secret message [65]).</li> </ul>	L	M	L	
			Template Attacks [72]	<ul style="list-style-type: none"> <li>No countermeasures for the attack mentioned in [72].</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure (by message recovery [72]).</li> </ul>	M	M	M	
			Cold-Boot Attacks [73]	<ul style="list-style-type: none"> <li>Storing the secret in the time domain instead of the frequency domain [73].</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure (recovery of the secret key [73]).</li> </ul>	L	M	L	
Dilithium [51]	Lattice-based digital signature scheme that uses Lyubashevsky's Fiat-Shamir with Aborts technique and rejection sampling to ensure compactness and relies on the hardness of module lattice problems	Pending FIPS certification (FIPS 204 [60])	Fault Attacks [63], [74]	<ul style="list-style-type: none"> <li>Checking the secret and error components of the LWE instances for known trivial weaknesses [63].</li> <li>Generic countermeasures including Double computation, Verification-after-sign, and Additional randomness [74].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by recovery of key [63], [74]).</li> <li>Tampering and Repudiation (by forging a signature on any given message [74]).</li> <li>Elevation of Privilege (by elevating the privileges and gaining access to restricted systems or data via forged signatures [74]).</li> </ul>	M	M	M	
			Advanced Power Analysis [75], [76]	<ul style="list-style-type: none"> <li>Masking using linear secret sharing scheme [75].</li> <li>Boolean and arithmetic masking by leveraging splitting and sharing sensitive variable [76].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing, Tampering, and Repudiation (by forging signature [76]).</li> <li>Elevation of Privilege (by elevating the privileges and gaining access to restricted systems or data via forged signature [76]).</li> <li>Spoofing, Tampering, Repudiation and Elevation of Privilege (by disclosing secret variables [75]).</li> </ul>	M	M	M	
			Electromagnetic Attacks [77], [78]	<ul style="list-style-type: none"> <li>Re-ordering of operations within the signing procedure and embedding the vulnerable addition operation deep enough inside the signing procedure [77].</li> <li>Bit-slicing design for NTT, the most critical sub-block, to provide a spatial intra-instruction redundancy [78].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing, and Tampering (by disclosing some info. about secret key [78]).</li> <li>Tampering, Repudiation and Elevation of Privilege (by forging a signature on any given message [77]).</li> </ul>	L	M	L	
			Template Attacks [79]	<ul style="list-style-type: none"> <li>Shuffling and Secret sharing [79].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by revealing information on the signer's secret key [79]).</li> <li>Repudiation and Elevation of Privilege (by forging signature via revealed signer's secret key [79]).</li> </ul>	M	M	M	
SPHINCS+ [56]	Stateless hash-based signature scheme relying on the hardness of finding collisions in hash functions	Pending FIPS certification (FIPS 205 [61])	Fault Attacks [80], [81]	<ul style="list-style-type: none"> <li>Making the signature computation redundant [80].</li> <li>Computing the index of the few-time signatures (FTS) from public values instead of secret ones [80].</li> <li>Linking the different layers of the hyper-tree to detect faults in the computation of the tree, which results in a non-valid signature [80].</li> <li>Detecting faults by recomputing of sub-trees with swapped nodes, as well as an enhanced hash function that inherently protects against faults [81].</li> <li>Computing and storing one-time signatures to reuse the results whenever needed [81].</li> <li>Recomputing the vulnerable instructions on different hardware modules to detect mismatches [81].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by recovering parts of the secret key [80] or universal signature forgery [81]).</li> <li>Tampering and Repudiation (by forging any message signature [80] or by creating a universal forgery with a voltage glitch injection on the targeted platform and collecting faulty signatures to create [81]).</li> </ul>	M	M	M	
			Advanced Power Analysis [82]	<ul style="list-style-type: none"> <li>Hiding the order of the Mix procedures [82].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by recovering secret key [82]).</li> <li>Tampering, Repudiation and Elevation of Privilege (by generating signature on arbitrary messages [82]).</li> </ul>	M	M	M	
Falcon [52]	Lattice-based digital signature algorithm based on the hardness of the shortest vector problem in structured NTRU lattices	Pending FIPS certification	Fault Attacks [83]	<ul style="list-style-type: none"> <li>Double computation of signature [83].</li> <li>Immediate verification after signing [83].</li> <li>Zero checking of the sampled vector [83].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by retrieving the private-key [83]).</li> <li>Repudiation and Elevation of Privilege (by forging signature via retrieved private key [83]).</li> </ul>	M	M	M	
			Timing Attacks [83]	<ul style="list-style-type: none"> <li>Blind-Vector algorithm extended the use of the Fisher-Yates shuffling procedure to enhance random shuffles for side-channel protection [83].</li> <li>Sample discard performing extra cache read from random addresses to distort statistics [83].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by retrieving the private-key [83]).</li> <li>Repudiation and Elevation of Privilege (by forging signature via retrieved private key [83]).</li> </ul>	M	M	M	
			Simple Analysis [84]	Power	<ul style="list-style-type: none"> <li>Practically lower the Hamming weight gap [84].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing, Tampering, Repudiation and Elevation of Privilege (by complete recovery of the secret keys [84]).</li> </ul>	M	M	M
			Electromagnetic Attacks [85]	<ul style="list-style-type: none"> <li>Hiding by making power consumption constant, [85].</li> <li>Masking using randomizing the intermediates values [85].</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing and Tampering (by extracting the secret signing keys [85]).</li> <li>Tampering, Repudiation and Elevation of Privilege (by forging signatures on arbitrary messages [85]).</li> </ul>	L	M	L	

\* We perform risk evaluation with the presumption of considering the countermeasures mentioned in the table.

- level may also contribute to a medium likelihood rating.
- c) *Low*: No known vulnerabilities, or only highly complex attacks that require administrative or physical privileges and have effective countermeasures in place, with limited attacker motivation.

The impact assessment, grounded in NIST-SP 800-30 Appendix H [42], evaluates the potential consequences of quantum attacks on user satisfaction, data confidentiality, and organizational reputation. According to the criteria outlined in Table IV, PQC attacks are assessed as having a Medium Impact. This assessment indicates that such attacks could lead to partial data compromise, limited operational disruption, and manageable recovery times, with moderate financial and reputational consequences. Risk evaluation integrates likelihood

and impact, as summarized in the risk matrix (Figure 2). Table VI provides algorithm-specific risk insights essential for developing robust PQC transition strategies to mitigate quantum threats and enhance cybersecurity resilience.

#### IV. QUANTUM IMPACT ON BC TECHNOLOGY COMPONENTS

Quantum attacks pose a significant threat to various components of BC technology, including (a) BC network, (b) mining pools, (c) transaction verification mechanisms, (d) smart contracts, and (e) user wallets. These attacks can compromise the trust and immutability that BC technology aims to provide. Understanding these vulnerabilities and implementing effective mitigation strategies is crucial for safeguarding the



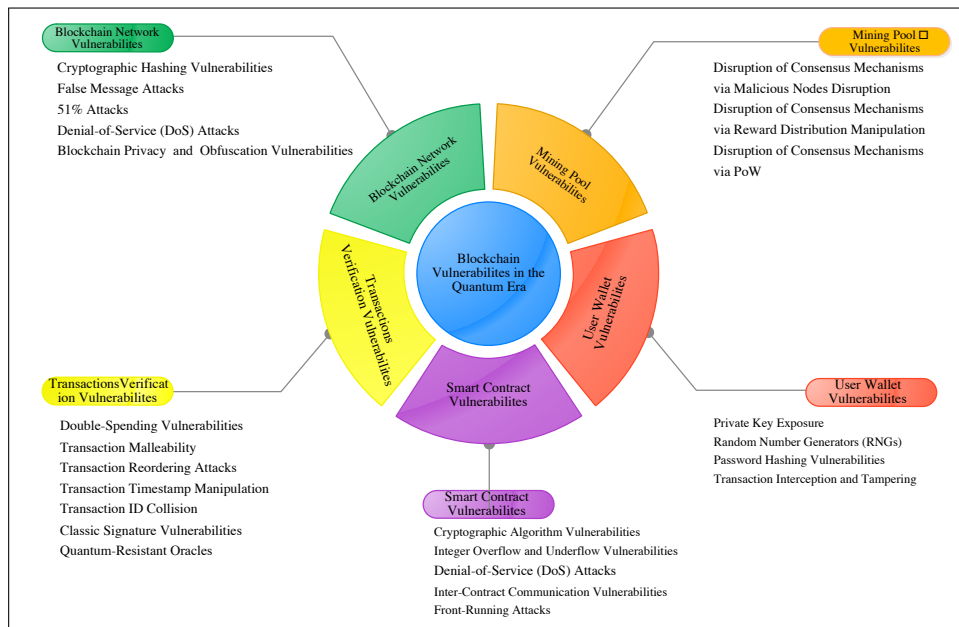


Fig. 7: Quantum Impact on BC Technology Components

integrity and security of BC ecosystems. This section will delve deeper into each of these components and explore potential solutions to safeguard their integrity and security in the quantum age.

#### A. BC Network and Quantum Computing Threats

QC poses a significant threat to BC networks by potentially exploiting weaknesses in core functionalities. Here is a breakdown of some key vulnerabilities along with mitigation strategies.

##### A.1. Cryptographic Hashing Vulnerabilities

BC networks rely heavily on cryptographic hashing functions to ensure data integrity and immutability. However, advancements in QC present a potential challenge to the security of hash functions, including widely used algorithms like SHA 256. These vulnerabilities, as highlighted in Table V, can weaken the security strength of hash functions and introduce risks such as transaction forgery or alteration of ledger history [1], [86]. Effective mitigation strategies to address these vulnerabilities include:

- **Standardization of Quantum-Resistant Hashing:** Promote and support the standardization of quantum-resistant hashing algorithms, ensuring they meet the required security levels for BC applications as outlined in NIST's post-quantum cryptography transition strategies [87].
- **Increased Hash Output Length:** Increase the output length of the hash function. While Grover's algorithm speeds up collision finding, a longer hash output length increases the computational resources (and time) required for successful attacks. This mitigates the threat but doesn't eliminate it.
- **Migration Plans:** Develop clear migration plans for transitioning from vulnerable hashing algorithms to quantum-resistant alternatives with minimal disruption to

the network [8], [88].

##### A.2. False Message Attacks

Quantum algorithms can compromise the security of digital signatures and hash functions, enabling attackers to forge signatures or manipulate data within the network. This could allow the injection of false information or the spread of misinformation, undermining the integrity of the BC system [89]. Additionally, quantum computational power, including *quantum parallelism* and *exponential speedup* (via algorithms like Shor's and Grover's), could facilitate *Sybil attacks*, where attackers deploy numerous fake nodes to manipulate identities or votes. This threat is particularly concerning for BCs utilizing Proof of Work (PoW) consensus mechanisms, where quantum acceleration could make it easier to create and manage fake nodes, potentially disrupting network operations [1]. However, the risks are not exclusive to PoW-based systems, as QC could also affect cryptographic vulnerabilities in Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT) systems, potentially undermining consensus or enabling false message injection by compromising digital signatures or private keys. Effective mitigation strategies for these quantum threats include:

- **PQC Algorithms:** Implementing PQC algorithms, such as lattice-based cryptography, is essential to secure digital signatures and other cryptographic primitives in a post-quantum world [90], [91].
- **Network Reputation Systems:** Developing and enhancing network reputation systems can help nodes identify and filter out messages originating from unreliable sources, preventing the spread of misinformation. These systems must be adapted to address quantum-specific vulnerabilities, ensuring resilience in a post-quantum world [92].
- **Incentivize Honest Behavior:** Designing incentive mechanisms that reward nodes for verifying the validity

of information and penalize those spreading false data is crucial. These mechanisms, although effective in current systems, need to be adapted to account for QC vulnerabilities to ensure their effectiveness in the future [93].

### A.3. 51% Attacks

A significant concern for PoW-based BCs is the possibility of a 51% attack. In this scenario, a malicious actor or group could control more than half of the network's mining hash rate, allowing them to manipulate transaction confirmations, potentially double-spend cryptocurrency, and ultimately compromise the network's integrity. While achieving a 51% attack with traditional computers is already computationally expensive, quantum computers could significantly reduce the resources needed, making it a more realistic threat for some BCs [94], [95]. Mitigation strategies to proactively defend against 51% attacks on BC networks include:

- **Transition to Alternative Consensus Mechanisms:** Exploring alternative consensus mechanisms like PoS that are less susceptible to 51% attacks, as they rely on coin ownership for validation, not raw computational power [96]. Quantum-resistant consensus mechanisms beyond those discussed above include QRL's proof-of-stake (QPoS) [97] and quantum PoW (QPoW) [98] algorithms.
- **Enhanced Difficulty Adjustment Algorithms:** Implementing dynamic difficulty adjustment algorithms that automatically adjust the mining difficulty based on the network hash rate can make it more expensive for attackers to acquire a controlling stake, thereby enhancing the network's resilience against 51% attacks [99].
- **Merged Mining:** While merged mining can provide security benefits by leveraging the hash power of larger networks, it introduces additional complexities. If a malicious actor gains control over a significant portion of the hash rate in a merged mining setup, they could potentially launch 51% attacks on multiple BCs simultaneously. Therefore, although merged mining may strengthen smaller BCs by sharing computational resources, it also poses a risk by potentially affecting multiple BCs at once. Careful consideration is required to manage these risks and ensure that the security of all participating networks is maintained [100].

### A.4. DoS Attacks

QC significantly amplifies the threat of DoS attacks on BC networks. By leveraging their immense computational power, quantum attackers could overwhelm nodes or critical network infrastructure with a deluge of traffic, disrupting transaction processing, delaying block confirmations, and potentially centralizing control. Quantum-accelerated attacks can exploit network vulnerabilities more efficiently, leading to more severe and prolonged disruptions. Mitigation strategies for quantum-enhanced DoS attacks on BC networks include:

- **Resource Reservation and Rate Limiting:** Implement mechanisms to reserve resources and impose rate limits to prevent malicious actors from monopolizing network

resources [101], [102].

- **Distributed Network Architecture:** Maintain a distributed network architecture to minimize the impact of DoS attacks on any single node [103].
- **Redundancy and Fault Tolerance:** Design systems with redundancy and fault tolerance to ensure network operability even during DoS attacks [104], [105].
- **Network Optimization Techniques:** Explore network optimization techniques such as efficient data compression, sharding, traffic filtering, or congestion control mechanisms to mitigate bandwidth and processing bottlenecks [106].
- **PQC and Quantum-Safe Consensus Protocols:** Transition to quantum-resistant cryptographic protocols and consensus mechanisms to prevent quantum-enhanced DoS attacks that could exploit vulnerabilities in classical cryptographic systems [90].

### A.5. Data Privacy and Obfuscation Vulnerabilities

The transparency and anonymity inherent in BC transactions can be compromised by quantum attacks. Quantum computers could potentially intercept and manipulate transaction data, exposing sensitive information such as transaction amounts and participant identities. Additionally, quantum attacks could compromise the pseudonymity of BC addresses, linking them to real-world identities and undermining privacy [107].

Privacy-centric BCs like Monero and Zcash employ advanced cryptographic protocols such as Bulletproofs and zk-SNARKs to protect transaction details. However, both of these protocols rely on ECC, which is vulnerable to Shor's algorithm. Additionally, the cryptographic hash functions used in these BCs (such as Keccak in Monero and BLAKE2b in Zcash) could be affected by Grover's algorithm, potentially reducing their security strength. These quantum threats could expose sensitive transaction metadata, including amounts and participant identities [1], [108], [109]. To mitigate the risk of data privacy and obfuscation vulnerabilities, several strategies can be adopted:

- **PQC:** Implement quantum-resistant cryptographic algorithms to safeguard transaction data from quantum manipulation [90], [91].
- **ZKPs:** ZKPs allow for the verification of transactions without revealing underlying data. To maintain security in a post-quantum world, ZKPs should be based on quantum-resistant cryptographic primitives such as lattice-based cryptography [110].
- **Layered Security Approach:** Combining techniques such as ring signatures with quantum-resistant zero-knowledge proofs, like zk-STARKs, can offer an additional layer of protection. Ring signatures help obfuscate transaction initiators, while zk-STARKs validate transaction amounts without revealing sensitive details, providing a robust defense against quantum attacks [111].
- **Adoption of Quantum-Resistant Obfuscation Protocols:** Transitioning to quantum-resistant cryptographic protocols, such as lattice-based cryptography and the Dilithium signature algorithm, is essential for preserving transaction confidentiality in the quantum era. Privacy-focused BCs like

TABLE VII: Analysis of BC Network Component Vulnerabilities to Quantum Computing Threats with Likelihood, Impact, and Risk Assessment

Layer	Exploited Vulnerabilities	Attack Vector	Potential Impacts	STRIDE Threats	Mitigation Strategies	Actionable Parties	L	I	R
BC Network	Cryptographic Hashing Vulnerabilities	Exploiting hashing algorithms	<ul style="list-style-type: none"> <li>Transaction Malleability</li> <li>Ledger history alteration.</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Potential modification of transaction details or blocks</li> <li>Spoofing: Forging or bypassing digital signatures.</li> </ul>	<ul style="list-style-type: none"> <li>Standardization of Quantum-Resistant Hashing</li> <li>Migration Plans</li> <li>Increasing Hash Output Length</li> <li>PQC Standards Development.</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Miners</li> <li>Auditors</li> </ul>	L	H	M
	False Message Attacks	Injecting false information through forging signatures and Compromising the security of hash functions	<ul style="list-style-type: none"> <li>Disrupted Consensus Process</li> <li>Invalid Transactions</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Manipulation of transaction data or blocks</li> <li>Reputation: Forged signatures allow attackers to deny responsibility or implicate others</li> <li>Info. Disclosure: Exposure of sensitive transaction data</li> </ul>	<ul style="list-style-type: none"> <li>PQC</li> <li>Network Reputation Systems</li> <li>Incentivize Honest Behavior</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Node Operators</li> <li>Governance Participants</li> </ul>	H	H	H
	51% Attacks	Control of network hash rate	<ul style="list-style-type: none"> <li>Double Spending</li> <li>Network Disruption</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: False confirmations of transactions</li> <li>DoS: Potential for network downtime or congestion due to malicious control of the mining hash rate</li> </ul>	<ul style="list-style-type: none"> <li>Transition to Alternative Consensus Mechanisms</li> <li>Enhanced Difficulty Adjustment Algorithms</li> <li>Merged Mining (with careful risk management)</li> </ul>	<ul style="list-style-type: none"> <li>Miners</li> <li>Developers</li> <li>Community Participants</li> </ul>	M	H	H
	DoS Attacks	Overwhelming network resources	<ul style="list-style-type: none"> <li>Network Congestion</li> <li>Service Outages.</li> </ul>	<ul style="list-style-type: none"> <li>Leveraging quantum power for large-scale resource exhaustion, overwhelming nodes, disrupting transactions, and destabilizing the network.</li> </ul>	<ul style="list-style-type: none"> <li>Resource Reservation and Rate Limiting</li> <li>Distributed Network Architecture</li> <li>Redundancy and Fault Tolerance.</li> </ul>	<ul style="list-style-type: none"> <li>Node Operators</li> <li>Service Providers</li> </ul>	H	H	H
	Data Privacy and Obfuscation Vulnerabilities	Interception of transaction data, exploiting vulnerabilities in obfuscation protocols (e.g., Bulletproofs, zk-SNARKs) and ECC-based cryptography	<ul style="list-style-type: none"> <li>Exposure of sensitive transaction data (amounts, identities)</li> <li>Loss of privacy and trust.</li> </ul>	<ul style="list-style-type: none"> <li>Info. Disclosure: Exposure of sensitive data (amounts, identities)</li> <li>Tampering: Data alteration, including transaction amounts and metadata.</li> </ul>	<ul style="list-style-type: none"> <li>PQC</li> <li>Zero-Knowledge Proof (ZKP)s</li> <li>Off-Chain Data Storage</li> <li>Transition to Quantum-Resistant Cryptographic Protocols</li> <li>Layered Security with Quantum-Resistant Techniques</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Service Providers</li> <li>Regulators</li> </ul>	H	H	H

Monero and Zcash can enhance their obfuscation mechanisms by adopting such quantum-resistant protocols [108], [112].

- **Off-Chain Data Storage:** Storing non-essential transaction data off-chain, possibly using decentralized storage solutions, can reduce the quantum attack surface. However, this approach requires careful security evaluation to avoid introducing new vulnerabilities [113].

By implementing the proactive mitigation strategies outlined above, BC networks can significantly strengthen their resilience against the emerging threats posed by QC. These measures collectively address critical vulnerabilities in BC networks, including cryptographic weaknesses, network disruptions, and privacy concerns, ensuring the continued security, integrity, and privacy of transactions in a post-quantum world.

#### A.6. Risk Assessment for Quantum Threat to BC Network Component

To assess the risks posed by QC threats to BC networks, we evaluate vulnerabilities based on the likelihood of occurrence and their potential impact, using the established criteria in Tables III and IV. Then, based on the evaluated level of likelihood and impact, overall risk is determined using the risk matrix in Figure 2.

The likelihood levels for quantum threats to BC networks are assessed based on the availability of QC<sup>1</sup>, the nature of the vulnerability, and the resources required to exploit it. The levels are categorized as High, Medium, or Low, reflecting both the probability of occurrence and feasibility of an attack.

<sup>1</sup>The likelihood evaluations presented for all components—blockchain networks, mining pools, transaction verification mechanisms, smart contracts, and user wallets—assume the availability of large-scale quantum computers capable of breaking or weakening current cryptographic primitives. Projected timelines for QC availability are critical factors that may alter these assessments (refer to Figure 4 for potential adjustments).

Below is a more precise breakdown:

- High:** DoS attacks are highly likely because they rely on computational power to overwhelm network resources rather than cryptographic weaknesses. These attacks could exploit quantum parallelism to amplify their scale, leading to network destabilization and significant disruption of operations. Similarly, false message attacks pose a high risk, as quantum systems can break digital signature schemes (e.g., ECDSA) using Shor’s algorithm. This enables attackers to forge signatures, inject false messages, and compromise consensus. Furthermore, data privacy and obfuscation vulnerabilities are also highly likely, given that quantum computers could exploit weaknesses in zk-SNARKs or elliptic curve cryptography to expose sensitive transaction data.
- Medium:** 51% attacks present a medium likelihood due to the potential of quantum acceleration to reduce the computational resources required to control the majority of network hash power. While such an attack would still demand substantial quantum hardware, ongoing developments elevate the feasibility of this threat. Achieving quantum dominance sufficient to compromise PoW consensus mechanisms remains a concern as quantum technologies progress.
- Low:** Cryptographic hashing vulnerabilities remain unlikely in the near term. Breaking robust hash functions like SHA-256 using Grover’s algorithm provides only a quadratic speedup, which is insufficient to pose a significant threat to adequately designed systems with sufficiently long hash outputs. Additionally, the requirement for large-scale, fault-tolerant quantum computers to execute such attacks remains speculative, keeping this threat at a low likelihood.

Impact reflects the potential severity of a successful attack. This encompasses critical consequences for BC users, such as loss of privacy, service disruption, data manipulation, financial losses, and damage to the trust and reputation of the BC network. Given the critical nature of BC systems, all vulnerabilities within the BC network are categorized as *High* impact

due to their potential to cause significant and potentially irreversible consequences. The overall risk is determined by combining likelihood and impact assessments using the risk matrix (Figure 2). Table VII provides a detailed analysis of BC network vulnerabilities to QC threats, including likelihood, impact, and risk assessments for each vulnerability, alongside potential mitigation strategies. This information serves as a guide for developers and BC communities to understand and address these emerging threats. By proactively implementing appropriate mitigation strategies, BC communities can ensure the continued security and stability of these decentralized networks.

### B. Mining Pool and Quantum Computing Threats

Mining pools are pivotal in upholding the security of PoW BCs by dedicating computational resources to solve cryptographic puzzles and validate transactions. However, QC introduces unique threats to mining pools, potentially undermining the decentralized nature of these networks. Here is a breakdown of some key concerns:

#### B.1. Disruption of Consensus Mechanisms via Malicious Nodes

QC introduces significant risks to mining pools by enhancing attackers' ability to infiltrate with malicious nodes masquerading as legitimate participants. These attacks disrupt the consensus process through methods such as *Pool Flooding* and *Selfish Mining*. In pool flooding, attackers leverage QC's immense computational power and parallelism to overwhelm the pool's infrastructure. By rapidly generating and injecting a large number of malicious nodes (Sybil nodes), attackers hinder transaction processing and disrupt consensus procedures [114]. In selfish mining, using quantum-enhanced computational efficiency, attackers exploit vulnerabilities in reward distribution algorithms. They strategically withhold computational power or selectively participate in block validation to maximize personal rewards, disrupting fair reward distribution and reducing pool security [115], [116]. These disruptions can result in delayed block confirmations, inconsistent transactions, or even forks in the BC [116]. QC amplifies the scale and efficiency of these attacks, necessitating tailored mitigation strategies:

- **Voting-Based Consensus Protocols:** Implement voting-based consensus mechanisms like BFT protocols, which are designed to tolerate a certain percentage of Byzantine (malicious) nodes without compromising the network [117], [118]. These protocols ensure consensus even under large-scale attacks facilitated by QC.
- **Stake-Based Admission:** Require miners to stake a certain amount of cryptocurrency to participate in the pool. This increases the cost of entry for attackers, making it more difficult to introduce numerous malicious nodes, even with quantum capabilities [119].
- **Decentralized Reputation Systems:** Develop reputation systems to identify and exclude nodes with suspicious behavior patterns. These systems help detect and mitigate the presence of malicious nodes, including those generated

rapidly by quantum-enhanced attackers [120].

#### B.2. Disruption of Consensus Mechanisms via Reward Distribution Manipulation

By leveraging QC's computational power, attackers can manipulate reward distribution mechanisms to gain an unfair advantage in receiving block rewards. Quantum-enhanced optimization and parallel processing enable them to exploit vulnerabilities in deterministic reward algorithms more efficiently, centralizing mining power and compromising network security [116]. Mitigation strategies to protect mining pools from disruption of consensus mechanisms via reward distribution manipulation include:

- **Transparent Reward Distribution Mechanisms:** Implement transparent and verifiable reward distribution mechanisms that are publicly auditable to deter manipulation attempts [121], [122].
- **Verifiable Random Functions (VRFs):** Utilize VRFs to generate unpredictable and verifiable randomness for block selection and reward distribution, making it harder for attackers to predict outcomes and manipulate rewards [123].
- **Pool Diversification:** Encourage users to distribute their mining power across multiple pools to reduce the impact of a single pool being compromised [124].

#### B.3. Disruption of Consensus Mechanisms via PoW

QC poses significant threats to PoW systems by exploiting vulnerabilities in public-key cryptography and hashing functions, which are critical to maintaining BC integrity and trust. PoW systems use public-key cryptography to secure communications and validate transactions. However, quantum computers, leveraging Shor's algorithm, could potentially break asymmetric cryptographic keys, enabling attackers to forge digital signatures, manipulate transactions, double-spend, disrupt consensus, and execute Sybil attacks. Although classical systems remain secure against these threats today, quantum advancements threaten to compromise current cryptographic protocols.

In addition to cryptographic signatures, PoW relies on hashing functions like SHA 256 to secure mining operations. Quantum computers, using Grover's algorithm, could significantly reduce the computational effort required to solve these cryptographic puzzles, enabling attackers to generate blocks faster than legitimate miners. While this does not directly affect digital signatures, it exposes mining pools that rely on outdated hashing algorithms to quantum-enabled disruptions, jeopardizing the fairness and security of the BC [94], [116]. Mitigation strategies to proactively defend against disruption of consensus mechanisms via PoW include:

- **Transition to PQC:** Implementing PQC algorithms is essential to safeguard transaction data and digital signatures from manipulation by quantum computers. Standardization efforts are ongoing [90], [91].
- **Hybrid Mining Models:** Investigating hybrid models that combine PoW with alternative consensus mechanisms like PoS could offer increased resilience against quantum attacks. PoS relies on coin ownership for validation, making

TABLE VIII: Analysis of Mining Pool Component Vulnerabilities to Quantum Computing Threats with Likelihood, Impact, Risk Assessment, and Potential Impacts

Layer	Exploited Vulnerabilities	Attack Vector	Potential Impacts	STRIDE Threats	Mitigation Strategies	Actionable Parties	L	I	R
Mining Pool	Disruption of Consensus Mechanisms via Malicious Nodes	Overwhelming Pool Infrastructure, Exploiting Reward Distribution Algorithms	<ul style="list-style-type: none"> <li>Loss of network integrity</li> <li>DoS</li> <li>Double-spending attacks</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Malicious nodes impersonate legitimate participants.</li> <li>Tampering: Manipulation of reward algorithms disrupts fairness.</li> <li>DoS: Pool flooding disrupts operations.</li> <li>Elevation of Privilege: Attackers gain unauthorized control.</li> </ul>	<ul style="list-style-type: none"> <li>Byzantine Fault Tolerance Protocols</li> <li>Stake-Based Admission</li> <li>Decentralized Reputation Systems</li> </ul>	<ul style="list-style-type: none"> <li>Miners,</li> <li>Developers,</li> <li>Node Operators,</li> <li>Auditors.</li> </ul>	H	H	H
	Disruption of Consensus Mechanisms via Reward Distribution Manipulation	Exploiting Reward Distribution Systems	<ul style="list-style-type: none"> <li>Reduced Miner Participation</li> <li>Centralization of mining power</li> <li>Double-spending attacks</li> </ul>	<ul style="list-style-type: none"> <li>Reputation: Attackers deny manipulating rewards.</li> <li>Tampering: Unfair reward distribution due to manipulation.</li> </ul>	<ul style="list-style-type: none"> <li>Transparent Reward Distribution Mechanisms</li> <li>Verifiable Random Functions</li> <li>Pool Diversification</li> </ul>	<ul style="list-style-type: none"> <li>Miners,</li> <li>Developers,</li> <li>Auditors.</li> </ul>	H	H	H
	Disruption of Consensus Mechanisms via PoW	Exploiting vulnerabilities in digital signatures or hashing algorithms	<ul style="list-style-type: none"> <li>Forged transactions (digital signatures)</li> <li>Re-mining blocks/double-spending (hashing functions)</li> <li>Loss of trust in the network</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Forged digital signatures allow impersonation.</li> <li>Tampering: Attackers modify BC data or re-mine blocks.</li> <li>Info. Disclosure: Weak cryptography exposes transaction details.</li> </ul>	<ul style="list-style-type: none"> <li>Transition to PQC</li> <li>Hybrid Mining Models</li> <li>Quantum-Safe Communication Protocols</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Node Operators,</li> <li>Regulators,</li> <li>Community Participants.</li> </ul>	M	H	H

it less susceptible to computational power manipulation, a potential vulnerability in PoW [125].

- **Quantum-Safe Communication Protocols:** While primarily a concern beyond mining pools, adopting quantum-safe communication protocols within the broader BC ecosystem (including wallets and exchanges) can further mitigate the risk of eavesdropping and data manipulation by attackers wielding quantum computers [2], [126].

By adopting the proactive mitigation strategies outlined above, mining pools can significantly enhance their resilience against the amplified threats posed by QC. These strategies address the infrastructural and systemic vulnerabilities that QC exploits, including malicious node infiltration, reward manipulation, and weaknesses in PoW, thereby ensuring the ongoing security and stability of BC networks in the face of emerging quantum challenges.

#### B.4. Risk Assessment for Quantum Threats to Mining Pool Component

QC advancements pose significant risks to mining pools, potentially impacting both BC users and overall network stability. These risks are evaluated based on their likelihood and impact, following the criteria outlined in Tables III and IV. The likelihood of each threat is assessed by considering factors such as the availability of QC advancements, the specific vulnerability being targeted, and the existence of effective mitigation strategies. Here is the categorization of the likelihood of QC threats to mining pools:

- High:** Disruption of consensus mechanisms due to malicious nodes and reward distribution manipulation is highly probable with the emergence of QC. Quantum computers, leveraging their immense computational power, can facilitate Sybil attacks by rapidly generating numerous malicious nodes or exploiting selfish mining tactics. These actions disrupt consensus, delay block confirmations, and threaten mining pool stability. Additionally, quantum algorithms enable efficient exploitation of deterministic reward systems, centralizing mining power and undermining fair reward distribution. These vulnerabilities underscore the critical

need for mitigation strategies such as BFT protocols, stake-based admission, VRFs, and pool diversification to ensure mining pool security.

- Medium:** The disruption of consensus mechanisms via PoW is moderately likely. QC using Grover’s algorithm can accelerate the solving of cryptographic puzzles, enabling attackers to potentially generate blocks faster than legitimate miners. However, the high computational resources currently required for such attacks limit their immediate feasibility. As quantum technology progresses, this risk could increase, emphasizing the importance of transitioning to hybrid models or alternative consensus mechanisms, such as PoS, to mitigate potential threats effectively.

As with the BC networks component mentioned earlier, a successful attack has a *High* impact, causing disruptions like loss of network integrity, denial-of-service attacks, double-spending vulnerabilities, reduced miner participation, and centralization of mining power. These issues can significantly harm the security and stability of the entire network. The overall risk is determined based on likelihood and impact levels using the risk matrix in Figure 2. The comprehensive analysis, including likelihood, impact, risk assessments, and mitigation strategies, for each vulnerability is detailed in Table VIII.

#### C. Transaction Verification Mechanism and Quantum Computing

The process of verifying transactions on a BC ensures the integrity of the network and prevents fraudulent activities. However, QC poses a significant threat to these verification mechanisms, which can lead to manipulated transactions and compromised network security. Here is a detailed breakdown of potential vulnerabilities:

##### C.1. Double-Spending Vulnerabilities

QC threatens BC security by accelerating attacks such as double-spending. Grover’s algorithm [5] can expedite the search for valid transaction signatures, enabling attackers to manipulate the BC and fraudulently spend the same digital currency multiple times [1]. Consequently, existing double-spending attacks, such as race conditions (exploiting the

confirmation time gap for multiple transactions [127]) and Finney attacks (pre-mining a conflicting transaction [128]), could become more efficient in the future. Mitigating future double-spending vulnerabilities due to QC requires a proactive approach. Here are some potential mitigation strategies:

- **Transition to Quantum-Resistant Signatures:** Current digital signatures may be susceptible to quantum attacks. Implementing quantum-resistant signature schemes, as recommended by NIST [129], is vital for enduring security.
- **Enhanced Consensus Mechanisms:** Traditional consensus mechanisms like PoW are vulnerable to quantum attacks, which can significantly accelerate hash computations and compromise the system's integrity. Transitioning to alternative mechanisms, such as PoS or BFT, enhances security by reducing reliance on computational power and instead leveraging economic incentives or fault-tolerant principles to maintain network robustness [130].
- **Sharding and Directed Acyclic Graphs (DAGs):** Scalability solutions like sharding and DAGs can reduce transaction confirmation times, mitigating the risk of quantum-accelerated double-spending. By enabling faster validations, these techniques limit the time window available for such attacks [131].
- **Verifiable Delay Functions (VDFs):** Use VDFs to create a time-based computational barrier, ensuring that transaction processing involves a provable delay. This makes it more challenging for quantum systems to exploit double-spending vulnerabilities by extending the time needed to validate or manipulate transactions [132].
- **Quantum-Resistant Sidechains:** Establish quantum-resistant sidechains for high-value transactions requiring enhanced security. By confining critical transactions to quantum-secure environments, the risk of exploitation is minimized while maintaining compatibility with the main BC [2], [133].

### C.2. Transaction Malleability

The potential to exploit transaction malleability is one of the significant threats posed by QC to the security of BC. This vulnerability allows attackers to manipulate weaknesses in transaction formatting to alter specific details (e.g., transaction fees or recipient addresses) without invalidating the signature [134], [135]. By accelerating the identification of cryptographic vulnerabilities, quantum computers could enable attackers to modify transaction details, potentially leading to double-spending, altered transaction amounts, or other fraudulent activities [136]. To address transaction malleability in the quantum era, the following mitigation strategies are recommended:

- **Adoption of Quantum-Resistant Cryptography:** Given the increased exploitability of malleability vulnerabilities using quantum attacks, the transition to quantum-resistant digital signature algorithms is a critical priority. [90], [91].
- **Strict Transaction Format Enforcement:** Implement stricter rules for transaction formatting to ensure all required information is included and standardized. This reduces the likelihood of exploiting malleability vulnerabilities arising

from inconsistent or incomplete transaction data [134].

- **Transaction Standardization Protocols:** Explore the use of protocols that define a canonical transaction format. A standardized approach ensures that transactions are consistent across the network, mitigating opportunities for malleability attacks [135].
- **Use of Segregated Witness (SegWit):** Adopt protocol upgrades like SegWit, which separate signature data from the transaction ID calculation. By decoupling these elements, SegWit directly addresses transaction malleability and enhances the overall robustness of legacy BC systems [137].

### C.3. Transaction Reordering Attacks

Transaction reordering attacks pose a significant threat to the security and integrity of BC networks, especially those reliant on precise transaction order, such as Decentralized Finance (DeFi) protocols or auction-based systems. QC, with its exponential computational power, can exacerbate these threats by breaking cryptographic primitives (e.g., RSA, ECC) and accelerating the identification of vulnerabilities in consensus mechanisms. By exploiting compromised digital signatures or manipulating consensus processes, quantum attackers could reorder transactions within blocks, leading to malicious activities such as double-spending, front-running, and smart contract manipulation [22]. To mitigate these threats, BC systems must adopt a layered and quantum-resistant approach that addresses both the computational and structural aspects of transaction reordering:

- **Sequence Numbers:** Use cryptographically secured sequence numbers or timestamps to explicitly define transaction order. These numbers create a tamper-proof sequence, reducing opportunities for reordering attacks and ensuring transaction consistency [138].
- **Unspendable Inputs:** Introduce transaction outputs specifically marked as unusable in future transactions. By invalidating attempts to reuse outputs, unspendable inputs prevent order manipulation and add a layer of protection against double-spending [139].
- **Partially Ordered Sets (POSets):** Implement POSets in consensus mechanisms to define partial ordering relationships within blocks. POSets provide flexibility in transaction ordering while maintaining overall consistency and resilience against tampering, particularly in asynchronous or distributed environments [140], [141].
- **VDFs:** Use VDFs to enforce provable computation delays, creating time-based barriers that make it infeasible for quantum attackers to rapidly reorder transactions. VDFs ensure that transaction validation involves a verifiable and computationally expensive process, adding resilience against quantum-accelerated attacks targeting transaction ordering [132].
- **Enhanced Consensus Mechanisms:** Quantum-resistant consensus protocols, such as those based on voting or staking, should be prioritized. These mechanisms reduce reliance on computationally intensive operations vulnerable to quantum acceleration and enhance block

validation security by leveraging economic incentives or fault-tolerance principles [130].

#### C.4. Transaction Timestamp Manipulation

Quantum attacks can exploit vulnerabilities in BC timestamp generation, leading to inconsistencies in transaction history and potential disruptions in the consensus process. Quantum computers can undermine the cryptographic algorithms that secure timestamp data, allowing attackers to alter transaction times and sequences. This manipulation can result in out-of-order transactions, enabling malicious activities such as double-spending and hindering the network's ability to reach consensus [31]. The following mitigation strategies are technically sound and effectively address these concerns:

- **VRFs:** Utilizing VRFs to generate unpredictable and verifiable timestamps enhances security by introducing cryptographic randomness. This approach preserves the integrity of transaction ordering and makes it significantly harder for attackers to alter timestamp data [123], [132].
- **Synchronized Clocks:** Implement synchronized clocks across validating nodes to ensure uniform timestamp generation. This strategy prevents discrepancies that could otherwise be exploited for manipulation and ensures the accurate sequencing of transactions [142].
- **BFT Protocols:** Leverage BFT protocols to tolerate malicious or faulty nodes attempting to manipulate timestamps. By maintaining consensus even in the presence of adversarial behavior, BFT protocols safeguard the network's reliability [118].

#### C.5. Transaction ID Collisions

Transaction IDs, critical for ensuring the uniqueness and integrity of BC transactions, may become vulnerable to quantum attacks. These identifiers are fundamental to maintaining consensus and preventing fraud within the network. Quantum algorithms like Grover's can significantly reduce the computational complexity of finding hash collisions, potentially enabling malicious actors to create multiple transactions with the same ID. Such collisions can lead to network confusion, disruption of consensus mechanisms, and exploitation scenarios, including double-spending or interference with smart contract execution [143]. The following mitigation strategies are proposed to address these challenges:

- **Migration to Quantum-Resistant Hashing:** Transition to quantum-resistant hashing algorithms specifically designed to resist attacks from quantum computers. While NIST has been actively standardizing post-quantum public-key cryptographic algorithms, it has not yet established specific standards for quantum-resistant hash functions. Active involvement in the development and future standardization of these algorithms is essential to maintain cryptographic security in a post-quantum world [144], [145].
- **Extended Transaction IDs:** Increase the length of transaction IDs to make collisions statistically less likely, even under the computational advantage provided by Grover's algorithm. While this approach enhances security, it may introduce trade-offs, such as increased storage and

processing requirements [144], [145].

#### C.6. Classic Signature Vulnerabilities

Classic digital signature algorithms, such as the ECDSA and RSA, are foundational to BC transaction verification and are widely used for signing transactions and ensuring authenticity. However, these algorithms are vulnerable to Shor's Algorithm [3]. A successful quantum attack would allow adversaries to forge digital signatures, inject unauthorized transactions, and compromise the integrity and trust of the BC network [1]. This vulnerability is especially critical for major BC platforms like Bitcoin and Ethereum, which rely on ECDSA for transaction security. The mitigate strategies for this type of vulnerabilities, includes:

- **Migration to Quantum-Resistant Signatures:** Transition to quantum-resistant signature algorithms mentioned in Table V. These algorithms are specifically designed to withstand attacks from quantum computers and are being standardized through initiatives like NIST PQC [90].

#### C.7. Quantum-Resistant Oracles

In the world of BC, smart contracts rely on oracles to bridge the gap between their internal logic and external data sources. These oracles fetch crucial information from the outside world, feeding it into the smart contract for transaction verification. However, traditional oracles pose a significant vulnerability to quantum attacks, as quantum computers could potentially manipulate the data they provide, compromising transaction verification integrity. Key strategies to mitigate this challenge and proactively enhance security include the following:

- **Decentralized Oracles:** Leveraging decentralized oracles that distribute data retrieval across a network of independent nodes significantly reduces the risk of a single point of failure. This redundancy makes it considerably more difficult for attackers to manipulate data streams and disrupt transaction verification [146], [147].
- **Quantum-Secure Data Providers:** Collaborating with data providers that utilize quantum-resistant solutions for data storage and transmission ensures the integrity of data feeding into smart contracts. Integrating such data providers strengthens the overall resilience of BC networks against potential quantum threats [148].
- **Data Validation Mechanisms:** Implementing robust data validation mechanisms in smart contracts is essential. These mechanisms ensure that the data received from oracles is thoroughly authenticated and verified before being used for transaction verification. This significantly mitigates the risk of attackers tampering with data and influencing transaction outcomes [149].

To protect transaction verification mechanisms, various stakeholders—including BC developers, node operators, auditors, service providers, and community members—should work together to create a quantum-resistant ecosystem. It is important to Migrate to quantum-resistant algorithms to defend against potential quantum attacks. Improving validation processes with stricter transaction formats, additional checks,

TABLE IX: Analysis of Transaction Verification Mechanism Component Vulnerabilities to QC Threats with Likelihood, Impact, Risk Assessment, and Potential Impacts

Layer	Exploited Vulnerabilities	Attack Vector	Potential Impacts	STRIDE Threats	Mitigation Strategies	Actionable Parties	L	I	R
Transaction Verification Mechanism	Double-Spending Vulnerabilities	Grover's algorithm, Race Condition Attack, Finney Attack	<ul style="list-style-type: none"> <li>Financial Losses,</li> <li>Network Instability</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: An attacker could impersonate a legitimate spender to conduct fraudulent transactions.</li> <li>Elevation of Privilege: Exploiting quantum efficiency, attackers may manipulate transaction validation to execute unauthorized double-spends.</li> </ul>	<ul style="list-style-type: none"> <li>Transition to Quantum-Resistant Signatures,</li> <li>Enhanced Consensus Mechanisms,</li> <li>Sharding and DAGs,</li> <li>Verifiable Delay Functions,</li> <li>Quantum-Resistant Sidechains.</li> </ul>	<ul style="list-style-type: none"> <li>Miners,</li> <li>Developers,</li> <li>Auditors,</li> <li>Community Participants.</li> </ul>	H	H	H
	Transaction Malleability	Exploiting weaknesses in transaction formatting to create a malleated transaction that retains a valid signature	<ul style="list-style-type: none"> <li>Compromised Transaction Integrity</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Attackers alter transaction content without invalidating its signature.</li> </ul>	<ul style="list-style-type: none"> <li>Adoption of Quantum-Resistant Cryptography,</li> <li>Strict Transaction Format Enforcement,</li> <li>Transaction Standardization Protocols,</li> <li>Use of Segregated Witness.</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Service Providers,</li> <li>Auditors.</li> </ul>	H	H	H
	Transaction Reordering Attacks	Manipulating the order of transactions within a block	<ul style="list-style-type: none"> <li>Transaction Censorship,</li> <li>Reordering Attacks</li> </ul>	<ul style="list-style-type: none"> <li>Repudiation: Malicious nodes deny the authenticity of the correct transaction order.</li> <li>Tampering: Transaction sequences are intentionally altered to facilitate attacks.</li> </ul>	<ul style="list-style-type: none"> <li>Sequence Numbers,</li> <li>Unspendable Inputs,</li> <li>Partially Ordered Sets,</li> <li>Verifiable Delay Functions,</li> <li>Enhanced Consensus Mechanism.</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Node Operators,</li> <li>Auditors.</li> </ul>	H	H	H
	Transaction Timestamp Manipulation	Manipulating timestamps to disrupt the consensus process	<ul style="list-style-type: none"> <li>Disruption of Consensus Process,</li> <li>Denial of service</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Altered timestamps impact transaction order and consensus stability.</li> </ul>	<ul style="list-style-type: none"> <li>VRFs,</li> <li>Synchronized Clocks,</li> <li>BFT Protocols</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Node Operators,</li> <li>Service Providers,</li> <li>Auditors.</li> </ul>	L	H	M
	Transaction ID Collisions	Creating multiple transactions with the same transaction ID	<ul style="list-style-type: none"> <li>Double spending</li> </ul>	<ul style="list-style-type: none"> <li>Elevation of Privilege: Quantum attackers exploit hash collisions to execute unauthorized transactions.</li> </ul>	<ul style="list-style-type: none"> <li>Migration to Quantum-Resistant Hashing Functions,</li> <li>Extended Transaction IDs</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Auditors,</li> <li>Community Participants.</li> </ul>	M	H	H
	Classic Signature Vulnerabilities	Exploiting weaknesses in ECDSA, RSA, or similar algorithms	<ul style="list-style-type: none"> <li>Compromised Security,</li> <li>Loss of Funds,</li> <li>Disruption of Entire BC</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Forged signatures allow malicious impersonation.</li> <li>Tampering: Attackers modify transaction data (e.g., recipient addresses or amounts) and forge corresponding signatures, compromising data integrity.</li> </ul>	<ul style="list-style-type: none"> <li>Migration to Quantum-Resistant Signatures.</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Service Providers,</li> <li>Auditors,</li> <li>Regulators</li> </ul>	H	H	H
	Quantum-Resistant Oracles	Manipulating data fed into smart contracts through oracles	<ul style="list-style-type: none"> <li>Smart contract manipulation,</li> <li>Data Integrity Attacks,</li> <li>Potential Loss of Funds</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Data inputs to smart contracts are manipulated.</li> </ul>	<ul style="list-style-type: none"> <li>Decentralized Oracles,</li> <li>Quantum-Secure Data Providers,</li> <li>Data Validation Mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Service Providers,</li> <li>Node Operators.</li> </ul>	H	H	H

and decentralized oracles can help reduce manipulation risks. Formal verification of smart contracts will also enhance security against quantum threats. However, we must carefully consider the scalability and integration of these strategies, as some, like VDFs, may affect transaction speed, and others, like POSets, might require major protocol changes. Ongoing surveillance and alignment with evolving post-quantum standards are vital for maintaining the resilience of BC systems.

### C.8. Risk Assessment for Quantum Threats to Transaction Verification Mechanism Component

To assess the risks posed by QC threats to BC transaction verification mechanisms, we evaluate their likelihood and impact based on the criteria established in Tables III and IV. The likelihood of a successful attack hinges on the availability of QC and the specific vulnerability targeted. Here is a breakdown of likelihood categories for transaction verification vulnerabilities:

- a) *High*: This category includes double-spending attacks, transaction malleability, transaction reordering attacks, classic signature vulnerabilities, and quantum-resistant oracles. Double-spending represents one of the most critical threats, as Grover's algorithm enables attackers to expedite the search for valid transaction signatures, especially affecting BCs with slow confirmation times. Transaction malleability and reordering attacks are highly susceptible to quantum systems, which can exploit cryptographic weaknesses or for-

matting inconsistencies to alter transaction data or sequence. Classic signature vulnerabilities are particularly pressing, with Shor's algorithm capable of breaking elliptic curve cryptography, exposing digital signatures to forgery and manipulation. Similarly, oracles, which serve as external data providers for BC systems, are vulnerable to quantum-enabled manipulation, further amplifying these risks.

- b) *Medium*: This category includes transaction ID collisions, where Grover's algorithm reduces the effort required to find hash collisions. While these attacks are not yet practical under current conditions, employing quantum-resistant hashing algorithms and sufficiently long hash functions can effectively mitigate this risk. Nonetheless, proactive adoption of quantum-resistant measures is necessary to safeguard against future exploitation as QC evolves.
- c) *Low*: Transaction timestamp manipulation falls under this category. Advanced defenses such as VRFs, synchronized clocks across nodes, and BFT protocols significantly mitigate this threat. These measures ensure accuracy and consistency in transaction timestamps, making such attacks highly infeasible, even as quantum technologies mature.

All transaction verification vulnerabilities carry a *High* impact rating, mirroring the assessments for BC networks and mining pools. This reflects the critical role transaction verification plays in safeguarding BC transactions. A successful attack could wreak havoc, causing financial losses from double-spending or compromised integrity, network instability due to disrupted consensus mechanisms or manipulated



transaction ordering, and even a complete compromise of the BC's security, shattering user trust and confidence.

Table IX provides a detailed analysis of potential vulnerabilities, their likelihood and impact assessments, and potential mitigation strategies for transaction verification mechanisms. This information empowers the community to ensure the continued security and stability of these critical components in the quantum era.

#### *D. Smart Contract Attacks and Quantum Computing Threats*

Smart contracts, self-executing programs stored on the BC, offer immense potential for automating agreements and facilitating trustless interactions. However, the emergence of QC introduces significant vulnerabilities that could compromise the security of these crucial components. Here is a deeper look at the potential threats posed by quantum computers to smart contracts:

##### *D.1. Cryptographic Algorithm Vulnerabilities*

Cryptographic algorithms like ECDSA and RSA, vital for smart contract security, are vulnerable to QC. Shor's algorithm allows attackers to forge signatures, steal funds, alter contract logic, and introduce malicious code, jeopardizing the integrity and trust of BC systems [2], [86]. These vulnerabilities not only threaten financial stability by enabling fund theft but also compromise the functionality of BC systems by allowing tampering with contract logic, leading to unintended behavior, malicious code execution, and disrupted contract execution. To mitigate these threats and ensure the long-term security of smart contracts, several strategies can be employed:

- **Quantum-Resistant Code Audits:** Conduct code audits specifically focusing on the cryptographic primitives used within smart contracts. Identify potential vulnerabilities that could be exploited by quantum computers and prioritize their remediation [150], [151].
- **Formal Verification with Quantum-Safe Assumptions:** Utilize formal verification techniques along with assumptions about the security of quantum-resistant algorithms to ensure the correctness and security of smart contracts in the quantum era [152], [153].
- **Phased Migration to Quantum-Resistant Cryptography:** Develop a phased migration plan to transition smart contracts from vulnerable algorithms to quantum-resistant alternatives as they become standardized and widely adopted [13].

##### *D.2. Integer Overflow and Underflow Vulnerabilities*

Integer overflow and underflow vulnerabilities are common programming errors that can lead to unexpected behavior in smart contracts. These occur when arithmetic operations exceed the maximum or minimum storage capacity of a variable, causing unpredictable outcomes. Quantum computers, with their ability to perform calculations significantly faster, could accelerate the identification and exploitation of such vulnerabilities, making traditional detection methods less effective [35]. For instance, a poorly designed smart contract may allow a large number to overflow the intended variable size,

resulting in unintended behavior or even enabling malicious actors to manipulate funds. Exploitation of such vulnerabilities could destabilize not only individual smart contracts but also broader BC ecosystems, leading to cascading failures across interconnected decentralized applications. To mitigate these threats and enhance resilience against quantum-accelerated attacks, the following strategies are recommended:

- **Static Code Analysis Tools:** Utilize advanced static code analysis tools specifically designed to identify potential integer overflow and underflow vulnerabilities within smart contracts. These tools provide proactive vulnerability detection during the development phase [154], [155].
- **Safe Math Libraries:** Integrate safe math libraries into smart contract development. These libraries offer secure arithmetic operations by enforcing strict checks, effectively preventing overflows and underflows even when handling large numbers [156], [157].
- **Formal Verification with Bounded Arithmetic:** Employ formal verification techniques that use bounded arithmetic assumptions to mathematically prove the absence of integer overflow and underflow vulnerabilities in the code. This method ensures robust security guarantees against such issues [158].
- **Proactive Development Practices:** Encourage secure coding practices during smart contract development, such as testing boundary conditions and adhering to strict validation rules, to minimize the risk of introducing arithmetic vulnerabilities from the outset.

##### *D.3. DoS Attacks on Smart Contracts*

DoS attacks target smart contracts by overwhelming them with a high volume of requests, far exceeding normal traffic, and impeding legitimate user access. While QC does not directly enable DoS attacks, its immense computational power could accelerate aspects such as attack generation and execution, enabling attackers to overwhelm smart contracts more rapidly and efficiently [159]. This surge in malicious traffic disrupts contract operations, causing delays in transactions or even preventing their processing entirely. To enhance smart contract security against DoS attacks and improve the overall resilience of the BC ecosystem, the following mitigation strategies are recommended:

- **Resource Limits:** Implement resource limits within smart contracts to restrict the number of transactions or computational operations a single user can perform within a specific timeframe. This helps prevent abuse, resource exhaustion, and overload, maintaining the overall integrity of the system [101], [102].
- **Circuit Breaker Patterns:** Integrate circuit breaker patterns that automatically halt contract execution when a surge in requests is detected. This prevents system overload and allows for recovery after a predefined downtime, minimizing the impact of a DoS attack [160].
- **Rate Limiting Mechanisms:** Implement rate-limiting protocols to control the frequency of interactions with smart contracts. These mechanisms ensure fair access for all users and prevent the system from becoming overwhelmed by

excessive requests. Rate limiting can be further enhanced by integrating transaction or gas fee mechanisms, which help regulate network load and provide additional deterrents to malicious actors [103], [161].

- **Network Optimization Techniques:** Explore various network optimization techniques to reduce the on-chain computational load and mitigate the effects of DoS attacks. Methods such as off-chain computation, transaction batching, and caching can help minimize delays and alleviate congestion during periods of high activity [162]–[164].
- **Gas Optimization and Batching:** Optimize gas usage by grouping multiple operations into a single transaction or offloading non-essential tasks to off-chain computations. Batching transactions reduces the overall load on the BC, minimizing resource consumption and enhancing system resilience during DoS attacks [165].

#### D.4. Inter-Contract Communication Vulnerabilities

In the intricate network of smart contracts, the pathways facilitating communication between these digital entities serve as critical conduits for data exchange and the execution of complex workflows. However, these channels are susceptible to vulnerabilities, offering potential entry points for exploitation by quantum attackers. These vulnerabilities may manifest in various forms, including the interception of sensitive data transmitted between contracts, the injection of malicious data into communication streams, or the disruption of interaction flows among contracts. Such actions could lead to severe consequences, ranging from the exposure of confidential information to the manipulation of data flows and the disruption of essential contract [166], [167]. Consequently, implementing robust mitigation strategies becomes paramount to safeguarding against these risks. Mitigation strategies and proactive measures to immunize against inter-contract communication vulnerabilities include:

- **Standardized Communication Protocols:** Develop and adopt standardized communication protocols for inter-contract interactions that prioritize security and offer built-in mechanisms for data integrity verification [8], [168].
- **Access Control Mechanisms:** Implement robust access control mechanisms within smart contracts to restrict unauthorized access to sensitive data and functionalities during inter-contract communication [169]–[171].
- **Quantum-Resistant Serialization Mechanisms:** Utilize quantum-resistant serialization mechanisms for data exchange between smart contracts, ensuring the integrity of data even if intercepted by attackers with quantum computers [172], [173].

#### D.5. Front-Running Attacks

In some BC networks, transaction fees are used to prioritize transaction processing. Quantum computers could potentially exploit this mechanism by analyzing pending transactions and strategically placing their own transactions before others (front-running). This could give attackers an unfair advantage in scenarios where transaction order is crucial. To effectively mitigate front-running attacks, especially in the context of

potential quantum threats, the following migration strategies for can be implemented:

- **Quantum-Resistant Encryption for Transaction Concealment:** Utilize post-quantum cryptographic algorithms to encrypt transaction details, ensuring that even with quantum computational capabilities, attackers cannot access sensitive information before transactions are confirmed. This approach maintains the confidentiality of transaction data, thwarting front-running attempts [129].
- **Commit-Reveal Schemes with Post-Quantum Security:** Adopt commit-reveal protocols enhanced with quantum-resistant cryptographic techniques. In this approach, transaction details are committed to the BC in an encrypted form and revealed only after a certain condition is met, such as the inclusion of the transaction in a block. This process minimizes the risk of front-running by delaying the disclosure of transaction specifics [95].
- **Threshold Cryptography for Transaction Processing:** Implement threshold cryptography, where transaction decryption requires collaboration among multiple network nodes. This method ensures that no single entity can prematurely access transaction details, thereby preventing front-running [174].
- **Implementation of Fair Transaction Ordering Protocols:** Introduce protocols that enforce fair ordering of transactions, such as First In, First Out (FIFO) queues, combined with quantum-resistant verification methods to ensure that transactions are processed in the order they are received, regardless of fee amounts [174].
- **Delayed Execution Mechanisms:** Implement delayed execution mechanisms to delay transaction execution until mining or validation is complete. By withholding transaction details from public access during the interim period, this strategy ensures that attackers cannot exploit pending transactions in real time [175].

By adopting these mitigation strategies, developers can create more secure and quantum-resistant smart contracts. Additionally, promoting awareness and best practices within the smart contract development community is crucial for building a more robust BC ecosystem prepared for the challenges of QC. Key mitigation strategies include rigorous testing and formal verification of smart contracts before deployment to detect and rectify vulnerabilities, particularly those vulnerable to quantum attacks. Additionally, leveraging programming languages engineered to withstand QC threats enhances the security of smart contracts. Regular audits and adherence to robust security practices further bolster resilience against potential exploits. Furthermore, designing smart contracts with upgradable features enables developers to swiftly address vulnerabilities and integrate quantum-resistant solutions as they emerge.

#### D.6. Risk Assessment for Quantum Threats to Smart Contract Component

To assess the risks posed by QC advancements to smart contracts, we evaluate their likelihood and impact based on

TABLE X: Analysis of Smart Contract Component Vulnerabilities to Quantum Computing Threats with Likelihood, Impact, and Risk Assessment

Layer	Exploited Vulnerabilities	Attack Vector	Potential Impacts	STRIDE Threats	Mitigation Strategies	Actionable Parties	L	I	R
Smart Contract	Cryptographic Algorithm Vulnerabilities	Exploiting weaknesses in cryptographic primitives	<ul style="list-style-type: none"> <li>Steal Funds</li> <li>Manipulate Contract Logic</li> <li>Disrupt Contract Execution</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Forged signatures allow impersonation.</li> <li>Tampering: Attackers modify contract logic or execution flow.</li> </ul>	<ul style="list-style-type: none"> <li>Quantum-Resistant Code Audits</li> <li>Formal Verification with Quantum-Safe Assumptions</li> <li>Phased Migration to Quantum-Resistant Cryptography</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Auditors,</li> <li>Regulators,</li> <li>Community Participants.</li> </ul>	H	H	H
	Integer Overflow and Underflow Vulnerabilities	Programming errors leading to unexpected behavior	<ul style="list-style-type: none"> <li>Financial Loss</li> <li>Data Corruption</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Attackers exploit vulnerabilities to modify contract behavior.</li> </ul>	<ul style="list-style-type: none"> <li>Static Code Analysis Tools</li> <li>Safe Math Libraries</li> <li>Formal Verification with Bounded Arithmetic</li> <li>Proactive Development Practices</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Auditors.</li> </ul>	M	H	H
	DoS Attacks	Overloading smart contracts with excessive requests, potentially accelerated by QC's computational power	<ul style="list-style-type: none"> <li>Service Disruption</li> <li>Financial Loss</li> <li>Transaction Failures or Logic Corruption</li> </ul>	<ul style="list-style-type: none"> <li>DoS: Attackers overwhelm the contract with excessive requests, potentially accelerated by QC.</li> </ul>	<ul style="list-style-type: none"> <li>Resource Limits</li> <li>Circuit Breaker Patterns</li> <li>Rate Limiting Mechanisms</li> <li>Network Optimization Techniques</li> <li>Gas Optimization and Batching</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Auditor,</li> <li>Node Operators,</li> <li>Service Providers.</li> </ul>	M	H	H
	Inter-Contract Communication Vulnerabilities	Exploiting weaknesses in communication channels between contracts	<ul style="list-style-type: none"> <li>Unauthorized Access to Sensitive Data</li> <li>Manipulated Contract Execution</li> </ul>	<ul style="list-style-type: none"> <li>Information Disclosure: Data interception reveals sensitive information.</li> <li>Tampering: Injected data alters inter-contract communication flows.</li> </ul>	<ul style="list-style-type: none"> <li>Standardized Communication Protocols</li> <li>Access Control Mechanisms</li> <li>Quantum-Resistant Serialization Mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>Developers,</li> <li>Service Providers,</li> <li>Auditors.</li> </ul>	H	H	H
	Front-Running Attacks	Strategically placing transactions before others for unfair advantage	<ul style="list-style-type: none"> <li>Financial Loss</li> <li>Market Manipulation</li> </ul>	<ul style="list-style-type: none"> <li>Elevation of Privilege: Attackers exploit quantum efficiency for prioritization.</li> <li>Information Disclosure: Attackers analyze pending transactions to gain advantage.</li> </ul>	<ul style="list-style-type: none"> <li>Quantum-Resistant Encryption for Transaction Concealment,</li> <li>Commit-Reveal with Post-Quantum Security,</li> <li>Threshold Cryptography for Transaction Processing,</li> <li>Fair Transaction Ordering,</li> <li>Delayed Execution Mechanisms.</li> </ul>	<ul style="list-style-type: none"> <li>Service Providers,</li> <li>Node Operators.</li> </ul>	H	H	H

the criteria established in Tables III and IV. The likelihood of a successful attack depends on the availability of QC technology and the specific vulnerabilities being exploited. As QC technology progresses, certain vulnerabilities become more feasible to exploit, necessitating proactive mitigation strategies.

- a) *High*: Vulnerabilities include cryptographic algorithm weaknesses, inter-contract communication vulnerabilities, and front-running attacks. Cryptographic algorithm vulnerabilities are the most critical due to the susceptibility of widely used schemes like ECDSA and RSA to Shor's algorithm. If compromised, these algorithms would allow attackers to forge digital signatures, alter contract logic, or steal funds. Inter-contract communication vulnerabilities also pose a significant risk, as QC could intercept or manipulate sensitive data exchanged between contracts, leading to unauthorized access or disruption of workflows. Similarly, front-running attacks gain feasibility as quantum systems can analyze pending transactions more quickly, enabling attackers to exploit priority mechanisms and gain unfair advantages in financial or auction-based systems.
- b) *Medium*: Vulnerabilities include integer overflow and underflow issues and DoS attacks on smart contracts. Integer overflow and underflow vulnerabilities depend on specific coding flaws within the smart contract, which QC could exploit more efficiently by accelerating vulnerability detection. However, these are less likely than cryptographic issues due to the specific conditions required for exploitation. DoS attacks, while potentially amplified by quantum computational power, are application-layer threats reliant on specific design flaws in contract execution or resource management rather than systemic cryptographic weaknesses.

A successful attack on any smart contract vulnerability carries a *High* impact rating across the board. This highlights the potential for catastrophic consequences. Exploiting these

vulnerabilities could lead to financial ruin for users and businesses through stolen funds, disrupted transactions, or manipulated contract logic. Furthermore, attackers could gain access to sensitive data or inject malicious content through inter-contract communication breaches. Additionally, DoS attacks and communication vulnerabilities can cripple smart contract functionality, disrupting workflows and causing widespread disruptions. Even seemingly less severe attacks like front-running can manipulate markets by giving attackers an unfair advantage. This *High* impact rating reflects the critical role smart contracts play in BC ecosystems. A compromised smart contract can destroy trust and security, posing significant risks to all participants.

The overall risk associated with each vulnerability is determined by combining the likelihood and impact assessments. Proactive understanding of these risks and implementing appropriate mitigation strategies is crucial for developers and BC communities. Table X provides a detailed analysis of potential vulnerabilities, their likelihood and impact assessments, and potential mitigation strategies for smart contract components.

### E. User Wallet Attacks and Quantum Computing Threats

The security of user wallets is paramount for ensuring trust and confidence in BC technology. However, the emergence of QC poses a significant threat to user wallets, potentially leading to stolen cryptocurrency and compromised financial security [2], [176]. Here is a breakdown of the vulnerabilities user wallets face in the quantum era:

#### E.1. Private Key Exposure

User wallets rely on robust cryptographic algorithms to protect private keys, which grant access to the funds within the wallet. Popular algorithms like ECDSA are currently used for key generation and signing transactions. However, vulnerability of these schemes to Shor's Algorithm could potentially render

the wallet susceptible to theft, allowing attackers to gain unauthorized access, derive the private key from the public key, and siphon off associated funds. Furthermore, it could facilitate the forging of seemingly legitimate transactions without the user's knowledge or consent, resulting in unauthorized transfers. To mitigate such threats, several migration strategies can be adopted:

- **Quantum-Resistant Key Generation:** Implement quantum-resistant algorithms for private key generation within user wallets. Research on these algorithms is ongoing, and some promising options are already emerging [177].
- **Multi-Party Computation (MPC) Wallets with PQC:** Explore MPC-based wallets where private key generation and transaction signing occur in a distributed manner without revealing the actual key material. To defend against quantum threats, integrate MPC protocols with quantum-resistant cryptographic primitives. This approach ensures the benefits of distributed trust while safeguarding against quantum attacks on underlying cryptography [178], [179].

#### *E.2. Random Number Generators (RNGs) Manipulation*

Many wallets rely on RNGs to create strong cryptographic keys. While traditional RNGs might suffice currently, they could be vulnerable to manipulation by quantum computers [180], [181]. Attackers could exploit weaknesses in RNGs to generate predictable keys, compromising the security of user wallets. To mitigate quantum-specific attacks on RNGs, the following strategies can be employed:

- **Device-Independent Quantum Random Number Generators (DI-QRNGs):** Implement DI-QRNGs that leverage quantum nonlocality to certify randomness without assumptions about the trustworthiness of the devices. This ensures secure and unpredictable randomness even under quantum adversarial conditions [182].
- **Post-Processing with Quantum-Proof Extractors:** Utilize quantum-resistant randomness extractors to refine raw random data into uniformly random outputs. This step eliminates potential biases or partial predictability, ensuring robustness against quantum computational attacks [183].
- **Adoption of Entropy Sources Resistant to Quantum Tampering:** Rely on entropy sources based on quantum physical processes, such as photon measurements or nuclear decay. These sources provide inherent resistance to quantum manipulation and ensure secure randomness generation [184].
- **Continuous Entropy Monitoring:** Deploy real-time entropy monitoring systems to detect anomalies or patterns that could indicate quantum interference or RNGs manipulation. This proactive approach helps maintain the integrity of randomness outputs under potential quantum threats [185].

#### *E.3. Password Hashing Vulnerabilities*

User accounts are typically protected with passwords, which are hashed (one-way encrypted) for secure storage. Popu-

lar hashing algorithms like SHA 256 are currently used in password storage. However, some quantum algorithms could potentially accelerate brute-force attacks, making it easier for attackers to guess passwords by trying a large number of combinations [186], [187]. To address these vulnerabilities, the following mitigation strategies are recommended:

- **Use Cryptographic Hash Functions with Adequate Bit Security:** Transition to cryptographic hash functions with a sufficiently large output size to withstand quantum attacks (e.g., SHA 3 or SHA 512) to withstand Grover's algorithm. This ensures that even with the quantum speed-up, the hash function remains computationally infeasible to attack [87].
- **Implementation of Memory-Hard Functions:** Utilize password hashing algorithms like Argon2, which are computationally expensive and memory-intensive. These algorithms significantly increase the resource requirements for each brute-force attempt, reducing the practicality of large-scale password guessing by both classical and quantum adversaries [188].
- **Increased Hash Iterations with Adaptive Difficulty:** Use password hashing algorithms that allow for adjustable iteration counts. By increasing the number of iterations, the computational cost per guess is raised, countering the speedup advantage provided by QC. Adaptive difficulty can ensure that the hashing cost remains proportional to current computational capabilities, including quantum advancements [187].
- **Password Policies with Enhanced Complexity:** Enforce policies that require longer, more complex passwords to increase entropy. This strategy mitigates quantum threats by increasing the effective search space for brute-force attacks, aligning with both classical and quantum security practices [189].

#### *E.4. Transaction Interception*

Quantum attackers leveraging advanced quantum computational capabilities could exploit vulnerabilities in traditional cryptographic protocols to intercept or tamper with transaction data during transmission. This poses significant risks, including theft or redirection of funds, unauthorized modifications, and exposure of sensitive transactional details. Quantum-specific attacks focus on breaking encryption or exploiting flaws in transaction validation mechanisms. To mitigate these threats, the following strategies are recommended:

- **Quantum-Resistant Encryption Protocols:** Adopt post-quantum cryptographic algorithms for securing data-in-transit, ensuring that intercepted data cannot be decrypted or altered even with quantum computational capabilities [190].
- **Enhanced BC Integrity Measures:** Strengthen BC protocols by incorporating cryptographic techniques like Merkle trees, secure MPC, or threshold cryptography to ensure the authenticity and integrity of transactions. These measures make it computationally infeasible for quantum adversaries to tamper with BC data [191].
- **Quantum-Resistant Transaction Verification:** Develop and deploy verification methods resilient to quantum attacks, such as hash-based digital signatures or quantum-

TABLE XI: Analysis of User Wallet Component Vulnerabilities to Quantum Computing Threats with STRIDE Threats and Risk Assessment

Layer	Exploited Vulnerabilities	Attack Vector	Potential Impacts	STRIDE Threats with Reasoning	Mitigation Strategies	Actionable Parties	L	I	R
User Wallet	Private Key Exposure	Deriving private keys from public keys using Shor's algorithm	<ul style="list-style-type: none"> <li>Loss of Funds</li> <li>Identity Theft</li> <li>Compromised Transactions</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Impersonation of legitimate users by deriving private keys and signing unauthorized transactions.</li> <li>Tampering: Forging transactions using compromised private keys allows attackers to manipulate the ledger.</li> </ul>	<ul style="list-style-type: none"> <li>Quantum-Resistant Key Generation</li> <li>MPC Wallets with Post-Quantum Cryptography</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Service Providers</li> <li>End Users</li> <li>Auditors</li> </ul>	H	H	H
	RNGs Manipulation	Manipulation of RNGs to generate predictable keys	<ul style="list-style-type: none"> <li>Compromised Security</li> <li>Unauthorized Access</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Alter or manipulation of RNGs process to produce predictable keys, compromising wallet security.</li> <li>Information Disclosure: Weak RNGs could reveal key generation patterns, exposing cryptographic material to attackers.</li> </ul>	<ul style="list-style-type: none"> <li>DI-QRNGs</li> <li>Post-Processing with Quantum-Proof Extractors</li> <li>Adoption of Entropy Sources Resistant to Quantum Tampering</li> <li>Continuous Entropy Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Service Providers</li> <li>Auditors</li> <li>Regulators</li> </ul>	M	H	H
	Password Hashing Vulnerabilities	Accelerated brute-force attacks on hashed passwords	<ul style="list-style-type: none"> <li>Data Breach</li> <li>Unauthorized Transactions</li> </ul>	<ul style="list-style-type: none"> <li>Repudiation: Attackers or users could deny responsibility for compromised accounts, especially in cases of weak password policies.</li> <li>Information Disclosure: Quantum-powered brute-force attacks could reveal hashed passwords, granting unauthorized access.</li> </ul>	<ul style="list-style-type: none"> <li>Cryptographic Hash Functions with Adequate Bit Security.</li> <li>Memory-Hard Functions.</li> <li>Increased Hash Iterations with Adaptive Difficulty.</li> <li>Password Policies with Enhanced Complexity.</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Service Providers</li> <li>End Users</li> <li>Auditors</li> </ul>	M	H	H
	Transaction Interception	Altering transaction data leading to theft or redirection of funds	<ul style="list-style-type: none"> <li>Financial Loss</li> <li>Data Manipulation</li> </ul>	<ul style="list-style-type: none"> <li>Tampering: Quantum attackers could alter transaction data in transit, redirecting funds or changing transaction details.</li> <li>Information Disclosure: Intercepted transactions could expose sensitive data, such as recipient addresses and transaction amounts.</li> </ul>	<ul style="list-style-type: none"> <li>Quantum-Resistant Encryption Protocols</li> <li>Enhanced Transaction Security</li> <li>BC Integrity Measures</li> <li>Quantum-Resistant Transaction Verification</li> <li>Secure Transmission Channels</li> </ul>	<ul style="list-style-type: none"> <li>Developers</li> <li>Service Providers</li> <li>Auditors</li> <li>Node Operators</li> <li>Regulators</li> </ul>	H	H	H

resistant zero-knowledge proofs. These mechanisms ensure that transactions remain valid and untampered even under quantum adversarial conditions [2].

- **Secure Transmission Channels:** Implement secure communication channels between users and BC nodes using post-quantum Transport Layer Security (TLS) protocols to prevent eavesdropping or data interception during transaction propagation [192].

By implementing these mitigation strategies, user wallet systems can significantly enhance resilience against password hashing vulnerabilities in the quantum era.

#### E.5. Risk Assessment for Quantum Threats to User Wallet Component

To assess the risks posed by QC advancements to user wallets, we evaluate the likelihood and impact of potential attacks using criteria established in Tables III and IV. The likelihood of a successful attack is influenced by the availability of QC technology and the nature of the specific vulnerability. The following breakdown summarizes the likelihood categories for user wallet vulnerabilities:

- High:* Private key exposure represents a critical vulnerability with a high likelihood of exploitation as QC advancements progress. Shor's algorithm makes it feasible to derive private keys from public keys, posing a severe threat to wallet security. Additionally, transaction interception could also fall into the high-likelihood category. Advanced quantum systems might compromise encryption protocols, allowing attackers to intercept or alter transaction data. While current secure communication protocols mitigate this risk, insufficiently updated encryption methods will be vulnerable to future quantum threats.
- Medium:* RNGs manipulation is a potential threat, with quantum systems capable of exploiting weaknesses in tradi-

tional RNGs to generate predictable keys. Although robust quantum-resistant random number generation techniques significantly reduce this risk, poorly implemented RNGs remain vulnerable. Password hashing vulnerabilities are also categorized as medium likelihood, as Grover's algorithm could accelerate brute-force attacks, making it easier for attackers to exploit weak password hashing implementations. However, the adoption of strong password policies, memory-hard hashing algorithms, and cryptographic schemes with higher security margins can help mitigate this threat.

A successful attack on a user wallet vulnerability carries a *High* impact rating. Exploiting these vulnerabilities could lead to catastrophic consequences for users. This includes loss of funds, identity theft, and compromised transactions. Attackers could gain unauthorized access to user accounts, steal funds, or manipulate transaction data for personal gain.

The overall risk associated with each vulnerability is determined by combining the likelihood and impact assessments. Proactive understanding of these risks and implementing appropriate mitigation strategies, such as quantum-resistant cryptography, strong password hashing, and regular key rotation, is crucial for wallet providers to ensure user security. Table XI provides a detailed analysis of potential vulnerabilities, their likelihood and impact assessments, and potential mitigation strategies.

## V. ROLES AND RESPONSIBILITIES IN MITIGATING QUANTUM COMPUTING IMPACTS ON BC

BC technology relies on cryptographic techniques to ensure security and integrity. Each role within the ecosystem—miners, service providers, end users, developers, regulators, auditors, and community participants—faces unique quantum-related challenges, necessitating tailored strategies to address potential vulnerabilities and ensure resilience.

TABLE XII: Roles and Responsibilities in Mitigating Quantum Computing Impacts on BC

Role	Attack Vector	STRIDE Threats	Quantum Implications	Possible Vulnerabilities	Quantum-Resistance Measures
Miners	Quantum Accelerated Mining	<ul style="list-style-type: none"> <li>Spoofing: Quantum speed allows impersonation within mining pools.</li> <li>Tampering: Quantum-accelerated hashing enables modification of blocks or mining history.</li> </ul>	Quantum computers may significantly speed up mining processes, especially in PoW, potentially disrupting consensus by enabling faster hash solving [193], [194].	Higher vulnerability to 51% attacks if mining power is concentrated among quantum-equipped miners [94], [95].	Adopting longer hash outputs, quantum-resistant hashing algorithms, and hybrid cryptographic techniques can help mitigate mining centralization [32], [195].
	Threat to Consensus Mechanisms	<ul style="list-style-type: none"> <li>Spoofing: Quantum power enables impersonation of network nodes.</li> <li>Tampering: Quantum attacks allow altering transaction data.</li> <li>Repudiation: Attackers may deny responsibility for malicious transactions.</li> <li>Info. Disclosure: Decryption powered by quantum technology could expose private transaction data.</li> <li>DoS: High-speed processing enables flooding of network nodes.</li> <li>Elevation of Privilege: Quantum power could give attackers control over nodes.</li> </ul>	QC's ability to break cryptographic primitives could undermine PoW and PoS security and affect scalability in BFT systems [95], [196].	Cryptographic vulnerabilities in consensus algorithms and scalability issues in BFT protocols [197], [198].	Development of quantum-resistant cryptographic algorithms, hybrid cryptographic systems, and restructuring BFT protocols for quantum resilience [8], [32].
	Energy Consumption	<ul style="list-style-type: none"> <li>Elevation of Privilege: Quantum efficiency enables unauthorized operations at lower energy costs.</li> </ul>	QC may improve mining efficiency, potentially reducing energy consumption, though security implications remain critical [32], [198].	Trade-offs between energy efficiency and security as quantum capabilities increase [193].	Design of low-energy quantum-resistant protocols for sustainable BC mining [194].
Service Providers	Quantum Crypt-analysis	<ul style="list-style-type: none"> <li>Spoofing: Quantum attacks could enable impersonation of legitimate service providers.</li> <li>Tampering: Decryption allows unauthorized data modifications.</li> <li>Info. Disclosure: Breaking encryption exposes sensitive data.</li> </ul>	Quantum attacks on encryption expose sensitive data and allow unauthorized access [3], [5], [6].	Encryption vulnerabilities compromise data confidentiality and integrity [3], [5], [6].	Implementation of quantum-resistant and hybrid cryptographic approaches [3], [5], [6].
	Smart Contract Vulnerabilities	<ul style="list-style-type: none"> <li>Tampering: Quantum attacks enable unauthorized changes to contract states.</li> <li>Repudiation: Attackers may deny malicious actions within contracts.</li> <li>Info. Disclosure: Quantum attacks could expose confidential contract data.</li> <li>Elevation of Privilege: Quantum bypasses enable unauthorized access to contract functions.</li> </ul>	Quantum threats could compromise contract integrity, allowing unauthorized control or data manipulation [28], [199].	Increased risk of smart contract exploitation due to compromised cryptographic primitives [28], [199].	Adoption of quantum-resistant cryptographic protocols, formal verification, and regular auditing [28], [199].
	Data Confidentiality	<ul style="list-style-type: none"> <li>Spoofing: Quantum attacks enable impersonation of authorized data handlers.</li> <li>Tampering: Unauthorized modifications to stored data due to broken encryption.</li> <li>Info. Disclosure: Quantum decryption reveals sensitive stored data.</li> </ul>	Quantum attacks threaten data confidentiality by breaking encryption [200].	Risk of sensitive data exposure and data manipulation [200].	Post-quantum cryptographic algorithms for data protection [200].
	Access Control Compromise	<ul style="list-style-type: none"> <li>Spoofing: Quantum-assisted impersonation bypasses access controls.</li> <li>Elevation of Privilege: Breaking cryptography grants unauthorized access.</li> </ul>	Quantum attacks could undermine role-based access and multi-signature wallets [201], [202].	Unauthorized access to sensitive functions or data [201], [202].	Quantum-resistant multi-signature schemes and hybrid authentication protocols [201], [202].
End Users	Quantum Key Extraction (Wallet Security Compromise)	<ul style="list-style-type: none"> <li>Spoofing: Quantum decryption enables impersonation of wallets.</li> <li>Tampering: Unauthorized transactions using compromised private keys.</li> <li>Info. Disclosure: Quantum attacks reveal private keys.</li> </ul>	Quantum attacks on ECC can expose private keys, compromising wallet security [203], [204].	Private keys and wallet data are vulnerable, risking asset security [203].	Quantum-resistant wallets with advanced cryptography and hardware wallets [203].
	Transaction Verification	<ul style="list-style-type: none"> <li>Tampering: Quantum attacks enable unauthorized transaction modifications.</li> <li>Repudiation: Attackers may deny responsibility for fraudulent transactions.</li> <li>Elevation of Privilege: Unauthorized transaction approvals via compromised signatures.</li> </ul>	Quantum threats may compromise digital signatures, affecting transaction integrity [196], [205].	Risk of fraud and financial loss due to compromised transaction verification [196].	Quantum-resistant digital signatures, multi-signature protocols, and threshold cryptography [196].
	Phishing Attacks	<ul style="list-style-type: none"> <li>Spoofing: Quantum attacks enable impersonation of trusted sources.</li> <li>Info. Disclosure: Quantum attacks expose credentials by breaking secure channels.</li> </ul>	Quantum threats to secure channels increase phishing risks and exposure of credentials [206], [207].	Higher risk of credential theft and unauthorized access [206].	Quantum-resistant communication protocols and user education on phishing risks [206].
	Privacy Breaches	<ul style="list-style-type: none"> <li>Info. Disclosure: Quantum decryption reveals user identities and transaction history.</li> <li>Spoofing: Quantum-assisted impersonation could lead to data leaks.</li> </ul>	Quantum decryption could reveal user identities and transaction history, risking privacy [95], [208].	Compromised anonymity and data confidentiality [209].	Quantum-resistant privacy technologies like zero-knowledge proofs and data anonymization [95].
Developers	Quantum Crypt-analysis	<ul style="list-style-type: none"> <li>Spoofing: Impersonation of smart contract owners or developers to deploy malicious updates.</li> <li>Tampering: Unauthorized modifications to cryptographic protocols or contract logic using quantum-powered attacks.</li> </ul>	QC undermines cryptographic primitives (e.g., RSA, ECC) used in BC protocols and smart contracts [3], [4].	Risk of protocol compromise, unauthorized updates, and systemic security failures if cryptographic primitives are not updated.	Adoption of lattice-based and hash-based cryptography, hybrid cryptographic schemes, and integration of post-quantum cryptographic libraries [210].
	Digital Signature Vulnerabilities	<ul style="list-style-type: none"> <li>Spoofing: Impersonation of valid signers in multi-signature schemes.</li> <li>Repudiation: Attackers deny responsibility for signed malicious transactions.</li> <li>Info. Disclosure: Exposure of private keys due to quantum decryption.</li> </ul>	Digital signatures, critical for authentication and authorization, are rendered insecure by quantum attacks [95], [211].	Compromised transaction authenticity, multi-signature wallets, and node authorization in consensus protocols.	Adoption of quantum-resistant digital signatures, such as lattice-based schemes, and regular validation of security mechanisms [211].
	Transition to Quantum-Resistant Solutions	<ul style="list-style-type: none"> <li>Tampering: Exploitation of legacy cryptographic systems during the transition phase.</li> <li>Elevation of Privilege: Attackers exploit unpatched vulnerabilities in transitioning protocols.</li> </ul>	Updating smart contracts and protocols to quantum-resistant algorithms is necessary but may introduce temporary security gaps [210].	Outdated cryptographic primitives, compatibility issues, and risks of incomplete migration.	Phased updates to quantum-resistant solutions, fallback mechanisms, testing in simulated environments, and collaboration with standardization bodies [210].
	Testing and Validation	<ul style="list-style-type: none"> <li>Info. Disclosure: Weaknesses in quantum-resistant algorithms could expose vulnerabilities.</li> <li>Tampering: Exploitation of untested or improperly validated quantum-resistant cryptographic schemes.</li> </ul>	Quantum-resistant algorithms require rigorous testing to ensure practicality, resilience, and scalability in BC environments.	Vulnerabilities due to improperly tested algorithms and reduced system performance during integration.	Rigorous testing in controlled environments, performance benchmarking, and phased deployment [210].
Node Operators	Quantum Hashing Attacks	<ul style="list-style-type: none"> <li>Tampering: Breaking traditional hashes enables modification of transaction history.</li> <li>Spoofing: Impersonation of valid nodes or miners using quantum-assisted hash manipulation.</li> </ul>	Grover's algorithm halves the effective security of hashing algorithms (e.g., SHA 256), reducing resistance to brute-force attacks [1].	Vulnerability to tampering with BC data, weakening of PoW consensus mechanisms, and potential double-spending risks.	Adoption of quantum-resistant hashing algorithms, such as sponge constructions and hash-based designs, and updates to PoW systems [36].
	Data Integrity Risks	<ul style="list-style-type: none"> <li>Info. Disclosure: Breaking encryption exposes sensitive data, including private keys.</li> <li>Tampering: Quantum attacks enable unauthorized modifications to BC or node data.</li> </ul>	Quantum attacks on encryption (e.g., RSA, ECC) can compromise stored and transmitted BC data, risking confidentiality and integrity [177].	Risks to private key security, data confidentiality, and historical transaction accuracy.	Adoption of lattice-based and hash-based cryptography for encryption, secure key management, and data storage protections [177].
	DoS Attacks	<ul style="list-style-type: none"> <li>DoS: Quantum-assisted attacks enable large-scale traffic flooding or resource exhaustion.</li> <li>Spoofing: Exploitation of compromised authentication to launch coordinated attacks.</li> </ul>	QC enhances the scalability and sophistication of DoS attacks by accelerating resource exhaustion techniques [212].	Disruption of node operations, reduced service availability, and potential node isolation.	Adoption of decentralized DoS mitigation systems, quantum-resistant authentication protocols, and enhanced network-layer protections [212].
	Unauthorized Access	<ul style="list-style-type: none"> <li>Elevation of Privilege: Breaking cryptographic protections to gain unauthorized access to nodes.</li> <li>Tampering: Compromised nodes enable manipulation of network data and configurations.</li> </ul>	Quantum decryption of private keys or authentication data may allow attackers to bypass security measures and gain control of node infrastructure [213].	Risks of unauthorized access, data breaches, manipulation of network state, and disruption of node operations.	Implementation of quantum-resistant authentication protocols, multi-factor authentication, regular security audits, and proactive infrastructure monitoring [213].

TABLE XII: (Cont.) Roles and Responsibilities in Mitigating Quantum Computing Impacts on BC

Role	Attack Vector	STRIDE Threats	Quantum Implications	Possible Vulnerabilities	Quantum-Resistance Measures
Regulators & Compliance Authorities	Encryption Vulnerabilities	<ul style="list-style-type: none"> <li>Info. Disclosure: Quantum attacks expose encrypted communications between regulators and stakeholders.</li> <li>Tampering: Compromised encryption allows alteration of regulatory data or directives.</li> <li>Repudiation: Attackers deny responsibility for breaches or altered communications.</li> </ul>	Quantum computers can break cryptographic standards like RSA and ECC, requiring regulators to transition to quantum-resistant encryption [214].	Risks to secure communications, data integrity, and enforcement of cryptographic compliance standards.	Adoption of post-quantum encryption standards, collaboration with global standardization bodies, and secure cryptographic audits [214].
	Data Security Risks	<ul style="list-style-type: none"> <li>Info. Disclosure: Breaking encryption exposes sensitive regulatory and compliance data, including Know Your Customer (KYC) records.</li> <li>Tampering: Quantum attacks enable unauthorized modification of stored or transmitted data.</li> <li>Spoofing: Impersonation of regulatory authorities to issue fraudulent compliance directives.</li> </ul>	Quantum attacks compromise encryption, creating vulnerabilities in regulatory systems and sensitive data [177].	Breaches of KYC records, manipulation of compliance records, and impersonation of regulatory entities, leading to compliance failures.	Implementation of quantum-resistant encryption, secure storage mechanisms, and periodic audits of regulatory systems [177].
	Legal Framework Updates	<ul style="list-style-type: none"> <li>Spoofing: Impersonation of regulators to issue fraudulent directives or policies.</li> <li>Tampering: Unauthorized changes to compliance or legal frameworks using quantum-enhanced tools.</li> <li>Elevation of Privilege: Exploiting outdated regulatory frameworks to bypass enforcement mechanisms.</li> </ul>	Quantum threats necessitate updates to cybersecurity and data protection laws to address cryptographic obsolescence and emerging quantum vulnerabilities [215].	Outdated legal frameworks that fail to mandate quantum-resistant systems and enforce compliance standards.	Regular updates to legal frameworks, phased mandates for quantum-resistant cryptographic systems, and post-quantum readiness audits [215].
	Privacy Mechanism Vulnerabilities	<ul style="list-style-type: none"> <li>Info. Disclosure: Quantum attacks expose anonymized or privacy-protected data.</li> <li>Spoofing: Impersonation of entities to exploit privacy-preserving tools.</li> <li>Repudiation: Attackers deny responsibility for breaches of privacy-preserving systems.</li> </ul>	Quantum capabilities weaken privacy-preserving mechanisms, such as zero-knowledge proofs and mixers, potentially undermining Anti-Money Laundering (AML) and KYC compliance [216].	Non-compliance of privacy tools with regulatory standards, exposure of sensitive user data, and challenges balancing privacy and AML requirements.	Enhanced oversight of privacy mechanisms, integration of quantum-resistant privacy tools, and regular technical audits to ensure compliance [216].
Auditors	Quantum-Accelerated Cryptanalysis	<ul style="list-style-type: none"> <li>Tampering: Manipulation of BC protocols or audit processes using quantum decryption.</li> <li>Info. Disclosure: Exposure of cryptographic weaknesses and sensitive audit findings.</li> </ul>	Quantum computers can break cryptographic primitives (e.g., RSA, ECC), requiring auditors to assess quantum-resistant solutions [217].	Ineffective detection of cryptographic vulnerabilities and outdated audit practices that fail to address quantum risks.	Development of quantum-aware audit frameworks, adoption of NIST post-quantum standards, and regular audits for cryptographic resilience [218].
	Transition Planning	<ul style="list-style-type: none"> <li>Spoofing: Impersonation of auditors to exploit migration vulnerabilities.</li> <li>Info. Disclosure: Quantum decryption exposes sensitive transition strategies.</li> <li>Tampering: Exploitation of unpatched or legacy systems during migration phases.</li> </ul>	Auditors guide BC projects through transitions to quantum-resistant cryptography, mitigating migration-specific risks [219].	Flawed migration plans, incomplete updates, and temporary compatibility issues during transitions.	Comprehensive evaluation of transition strategies, phased migration plans, and adoption of hybrid cryptographic systems to ensure smooth transitions [218].
	Post-Quantum Readiness Assessments	<ul style="list-style-type: none"> <li>Tampering: Exploitation of improperly deployed quantum-resistant implementations.</li> <li>Spoofing: Impersonation of auditors during readiness testing or compliance audits.</li> <li>Info. Disclosure: Exposure of vulnerabilities during assessments or simulated attacks.</li> </ul>	Auditors test quantum-resistant solutions for effectiveness and compliance with evolving standards [218].	Improperly deployed quantum-resistant systems and inadequate alignment with post-quantum standards.	Simulating quantum-based attacks, validating system alignment with regulatory frameworks, and conducting ongoing compliance audits [217].
	Collaborative Security Reviews	<ul style="list-style-type: none"> <li>Tampering: Misaligned collaboration leaves vulnerabilities unaddressed.</li> <li>Info. Disclosure: Exposure of sensitive findings during collaborative processes.</li> <li>Repudiation: Stakeholders deny responsibility for implementing quantum-resistant solutions.</li> </ul>	Collaboration ensures robust quantum-resistant designs and alignment with technical and regulatory standards [218].	Miscommunication, unaligned standards, or incomplete reviews can weaken system resilience.	Joint reviews with developers, cryptographers, and regulators to validate quantum-resistant designs and enforce global standards [218].
	Skill Development and Training	<ul style="list-style-type: none"> <li>Inadequate training leads to ineffective audits and overlooked vulnerabilities.</li> <li>Exploitation of outdated tools and methodologies by attackers.</li> </ul>	Auditors must acquire expertise in post-quantum cryptography, quantum-specific auditing tools, and advanced security frameworks [218].	Insufficient expertise compromises audits and weakens assessments of post-quantum readiness.	Continuous skill development through workshops, certifications, and training in quantum-resistant practices [218].
Governance Participants	Quantum-Supported Manipulation	<ul style="list-style-type: none"> <li>Spoofing: Forgery of governance participant identities to disrupt decision-making.</li> <li>Tampering: Manipulation of governance decisions or proposals.</li> </ul>	QC undermines cryptographic protections, enabling identity forgery and manipulation of decision-making processes [220].	Risk of unauthorized governance decisions, identity spoofing, and governance manipulation affecting system trust.	Adoption of quantum-resistant identity verification, secure quorum mechanisms, and tamper-proof governance protocols [220].
	Decentralized Governance Systems	<ul style="list-style-type: none"> <li>Spoofing: Quantum attackers forge participant identities to influence decision-making.</li> <li>Tampering: Alteration of governance-related data, outcomes, or rules.</li> <li>Repudiation: Denial of responsibility for fraudulent governance actions.</li> </ul>	Quantum threats could compromise decentralized governance systems, disrupting transparency, accountability, and trust [221].	Risk of governance manipulation, unauthorized access, and reduced confidence in decentralized systems.	Implementation of quantum-resistant cryptographic protocols, tamper-proof governance mechanisms, and enhanced audit trails [221].
	Voting Mechanisms	<ul style="list-style-type: none"> <li>Info. Disclosure: Quantum attacks expose confidential votes or voter identities.</li> <li>Tampering: Unauthorized alteration of cast votes or voting outcomes.</li> <li>Spoofing: Impersonation of voters to skew results or manipulate governance.</li> </ul>	QC compromises vote confidentiality and integrity, enabling manipulation of governance outcomes [222].	Privacy breaches, vote manipulation, vote-buying, coercion, and loss of confidence in governance outcomes.	Adoption of quantum-resistant cryptographic techniques and advanced privacy-preserving mechanisms like quantum-resistant zero-knowledge proofs [222].
	Smart Contract Execution	<ul style="list-style-type: none"> <li>Tampering: Quantum attackers disrupt governance-related transactions or smart contract execution.</li> <li>Elevation of Privilege: Unauthorized execution of governance-related actions.</li> </ul>	Quantum threats compromise governance-related smart contracts, enabling transaction manipulation, unauthorized actions, or financial tampering [223].	Risk of disrupted decision-making processes, treasury manipulation, and governance system failures.	Implementation of quantum-resistant smart contracts, formal verification practices, and secure governance transaction frameworks [223].
	Quorum Formation and Proposal Verification	<ul style="list-style-type: none"> <li>Spoofing: Forged identities disrupt quorum formation, enabling Sybil attacks.</li> <li>Tampering: Quantum attacks alter governance proposals or their verification.</li> </ul>	QC enables identity forgery and tampering, undermining quorum legitimacy and proposal verification [224].	Loss of governance integrity, fraudulent proposals, and weakened trust in decision-making structures.	Adoption of quantum-resistant identity verification systems, tamper-proof proposal mechanisms, and decentralized governance frameworks [224].
Oracles	Quantum Tampering	<ul style="list-style-type: none"> <li>Tampering: Manipulation of external data feeds from multiple sources.</li> <li>Info. Disclosure: Interception of sensitive oracle communications.</li> <li>Spoofing: Impersonation of legitimate oracles to deliver fraudulent data.</li> </ul>	Quantum attacks compromise cryptographic protections, enabling manipulation or interception of oracle data, undermining trust in smart contract operations [22], [220].	Risk of corrupted or falsified data feeds, compromised multi-oracle systems, and disrupted decision-making in oracle-driven applications.	Adoption of quantum-resistant cryptographic protocols, tamper-proof data verification mechanisms, and secure multi-source aggregation to prevent single-point failures [24], [186].
	Quantum Eavesdropping	<ul style="list-style-type: none"> <li>Info. Disclosure: Quantum-enabled interception of data during transmission.</li> </ul>	Secure communication channels between oracles and BC systems are vulnerable to quantum interception, exposing sensitive data or disrupting workflows [24].	Exposure of confidential data, leading to breaches of contract logic and manipulation of BC processes reliant on oracle inputs.	Transition to quantum-safe communication protocols and continuous monitoring of data flow integrity [186].
	Quantum-Compromised Smart Contracts	<ul style="list-style-type: none"> <li>Tampering: Manipulation of oracle-driven smart contract executions.</li> <li>Elevation of Privilege: Unauthorized execution of high-priority actions through compromised inputs.</li> </ul>	Quantum attacks undermine the cryptographic foundations of smart contracts that depend on oracle inputs, disrupting contract execution and financial operations [95], [211].	Disruption of contract reliability, unauthorized fund transfers, and manipulation of automated workflows in oracle-driven systems.	Implementing quantum-resistant smart contracts, regularly auditing oracle integrations, incorporating fail-safe mechanisms for data integrity, and fostering collaborative development with BC stakeholders [211].
Community Participants	Cryptographic Breaks	<ul style="list-style-type: none"> <li>Tampering: Manipulation of transactions or digital signatures.</li> <li>Spoofing: Forgery of participant identities.</li> </ul>	Quantum attacks on cryptography could enable identity forgery and transaction manipulation [28].	Loss of trust in BC systems, compromised digital signatures, and stolen participant identities or private keys.	Advocacy for the adoption of quantum-resistant cryptography by developers, active participation in governance discussions, and promotion of secure digital identity systems [32].
	Privacy Breaches	<ul style="list-style-type: none"> <li>Info. Disclosure: Exposure of transaction data and identities.</li> <li>Spoofing: Impersonation of users or community members.</li> </ul>	Quantum-enabled decryption threatens confidentiality of BC transactions [208].	Loss of user anonymity, exposure of sensitive data, and reduced trust in public BCs.	Promotion of privacy-preserving technologies like zero-knowledge proofs, secure multi-party computation, and community-driven awareness campaigns on privacy risks [225].
	Misinformation	<ul style="list-style-type: none"> <li>Tampering: Manipulation of educational materials or BC narratives.</li> <li>Spoofing: Creation of false sources to spread quantum-related misinformation.</li> </ul>	Misinformation about quantum vulnerabilities can cause panic and distrust in BC ecosystems [226].	Erosion of trust, spread of incorrect security measures, and delayed adoption of quantum-safe technologies.	Transparent communication, fact-checking initiatives, collaboration with trusted experts, and leveraging social media to dispel myths [226].
	Educational Gaps	<ul style="list-style-type: none"> <li>Info. Disclosure: Lack of knowledge delays the adoption of protective measures.</li> <li>Repudiation: Failure to provide accurate and accessible educational resources.</li> </ul>	Limited awareness of quantum risks leaves the community unprepared for emerging threats [227].	Vulnerabilities due to delayed adoption of quantum-safe practices, especially among non-technical participants.	Community-led educational initiatives like webinars, forums, outreach programs, and collaborative workshops to spread awareness [226].

Miners need to adapt their mining algorithms to incorporate quantum-resistant designs, effectively addressing the risks posed by quantum-accelerated mining and the potential for centralization. Service providers play a critical role in implementing quantum-resistant cryptography, securing smart contracts, and ensuring data confidentiality and integrity. End users should enhance wallet security, rigorously verify transactions, and adopt measures to mitigate quantum-assisted phishing attacks. Developers bear the responsibility of transitioning BC protocols and smart contracts to quantum-resistant cryptographic algorithms. They must conduct rigorous testing of these solutions and collaborate with cryptographic experts to ensure scalability, security, and resilience. Regulators need to update legal frameworks to address the implications of QC, enforce quantum-resistant standards, and monitor BC ecosystems for emerging vulnerabilities. Auditors play a vital role in assessing BC systems for quantum readiness. By evolving audit methodologies, conducting post-quantum readiness assessments, and guiding the transition to secure solutions, auditors help maintain system integrity. Community participants contribute by raising awareness, advocating for quantum-resistant practices, educating users, and supporting open-source development, conducting security audits, and promoting the adoption of best practices.

Table XII details the challenges and mitigation strategies associated with each role, emphasizing the necessity of quantum-resistant cryptography, advanced security protocols, and proactive risk management. By addressing these challenges and collaborating with standardization bodies such as NIST, the BC ecosystem can maintain its security and resilience in the face of QC advancements.

## VI. CHALLENGES AND STRATEGIES AFTER TRANSITIONING TO QUANTUM-RESISTANT BC SYSTEMS

While the integration of quantum-resistant algorithms seems like a natural solution, the transition itself introduces a new wave of challenges [228]. This section delves into the complexities organizations face after transitioning their BC systems to a quantum-resistant future. We will explore the multifaceted attack vectors that extend beyond just encryption vulnerabilities, and the strategic considerations required to navigate this critical shift. By examining key components like the BC network, mining pools, and user wallets, we will identify the challenges associated with adapting each element to quantum-resistant cryptography. We will also explore potential solutions that organizations can implement to ensure a smooth and secure transition, safeguarding the long-term viability of their BC deployments in the face of this evolving technological landscape.

### A. BC Network

The emergence of QC necessitates a paradigm shift in securing BC networks. While the integration of quantum-resistant algorithms offers a solution, it demands a comprehensive re-evaluation of the underlying network architecture. Unlike a straightforward cryptographic substitution, these new algorithms often necessitate larger

key sizes and impose significantly higher computational workloads. Consequently, adjustments to existing protocols, data structures, and even the fundamental infrastructure of the network become paramount [229]. Additionally, these changes can affect network latency and transaction throughput, further complicating the transition. This section explores the multifaceted challenges associated with this crucial transition, including potential incompatibilities with current systems, the need to accommodate larger keys and increased workloads, the imperative for network infrastructure upgrades, and the critical task of maintaining seamless interoperability during the migration process. By addressing these challenges and implementing effective solutions, organizations can ensure a smooth migration to a quantum-resistant BC network, safeguarding its long-term security and scalability within this evolving technological landscape. Here is a breakdown of the key challenges and potential solutions for BC networks in this context:

#### A.1. Compatibility with Existing Protocols and Data Structures

New cryptographic algorithms might not be readily compatible with existing BC protocols and data structures [230]. This could lead to issues with data validation, consensus mechanisms, and overall network functionality. Potential solutions include:

- Develop adaptations to existing protocols to accommodate the specific requirements of quantum-resistant algorithms.
- Explore alternative data structures inherently compatible with the new cryptography.
- Implement a phased migration approach, where certain functionalities transition to quantum-resistant algorithms first, followed by others.

#### A.2. Accommodating Larger Key Sizes and Increased Computational Demands

Post-quantum algorithms typically rely on larger key sizes compared to classical cryptography [8], [168], [231]. This can lead to increased storage requirements and computational demands for tasks like transaction verification and block validation, potentially impacting network latency and throughput. Potential solutions include:

- Analyze the trade-off between security level and key size, adopting a balance that ensures security without overly compromising efficiency.
- Upgrade hardware for BC nodes to handle the increased computational workload.
- Explore alternative consensus mechanisms with lower computational requirements that remain secure in a QC environment.

#### A.3. Network Infrastructure Upgrades

Upgrading the underlying infrastructure of the BC network is crucial for seamless operation with quantum-resistant algorithms. This includes software updates, hardware replacements, and ensuring compatibility with existing tools [232]–[234]. Potential solutions include:





Fig. 8: Challenges of Transitioning BC Components to Quantum-Resistant Cryptography

- Develop clear upgrade paths for BC nodes, providing detailed instructions and compatibility testing tools.
- Foster collaboration within the BC ecosystem to ensure smooth integration of new software versions across different network participants.
- Consider backward compatibility features during a transition period to minimize disruptions for users and applications reliant on older infrastructure.

#### A.4. Maintaining Interoperability

During the transition, some nodes might operate with old cryptography while others adopt new quantum-resistant algorithms [27], [31], [38]. This can potentially lead to network disruptions if interoperability is not maintained. Potential solutions include:

- Develop and implement robust communication protocols allowing nodes using different cryptographic schemes to interact seamlessly.
- Design a staged migration process with clear milestones and well-defined rollback mechanisms in case of unforeseen issues.
- Promote collaboration and communication within the BC community to ensure a smooth and coordinated transition for all participants.

By addressing these challenges and implementing effective solutions, organizations can successfully transition their BC networks to quantum-resistant algorithms. This ensures long-term security, scalability, and resilience against potential threats posed by quantum computers.

#### B. Mining Pool

Mining pools face significant challenges during the transition to quantum-secure cryptography. Increased computational

overheads associated with post-quantum algorithms can strain resources and potentially exacerbate centralization risks. Furthermore, new attack vectors, such as quantum-based DoS attacks or cryptanalysis of quantum-secure primitives, may emerge. To ensure continued success, mining pools must implement robust security measures, optimize resource utilization, and actively mitigate centralization risks [235]. The following explores these challenges and proposes strategies for successful operation in a quantum-secure environment.

##### B.1. Enhanced Security Measures

The transition to quantum-resistant algorithms introduces new attack vectors, such as quantum cryptanalysis and side-channel vulnerabilities, which can compromise mining operations. Robust security protocols are essential for mitigating these threats. Potential defense strategies include:

- Design and implement a key management system that operates with both current and quantum-resistant cryptographic keys for critical sectors.
- Deploy intrusion detection and prevention systems (IDS/IPS) to monitor for suspicious activities within the mining pool infrastructure [236].
- Conduct regular security audits to identify and address vulnerabilities in pool software, configurations, and network interfaces [217], [218].
- Implement stricter access controls and multi-factor authentication mechanisms to secure user accounts, mining resources, and administrative tools [237].

##### B.2. Resource Optimization

Quantum-resistant algorithms necessitate larger key sizes and increased computational power, significantly impacting energy consumption and resource demands [27], [31], [38]. Effective optimization strategies include:

- Utilize specialized hardware accelerators, such as GPUs,

FPGAs, or ASICs, designed for efficient execution of quantum-resistant cryptographic tasks.

- Implement dynamic resource allocation systems leveraging cloud computing to handle fluctuating mining demands.
- Investigate energy-efficient mining algorithms tailored to quantum-resistant cryptography and invest in renewable energy sources to mitigate environmental impacts.
- Quantify resource overheads, such as the percentage increase in energy consumption per transaction due to larger key sizes, and address thermal challenges with innovative cooling systems.

### B.3. Maintaining Competitiveness and Fairness

Increased hardware and operational costs may exacerbate centralization risks, as only well-funded mining pools can afford the necessary infrastructure [2], [8], [168]. To promote fairness and competitiveness:

- Encourage collaboration between mining pools to share computational resources and collectively strengthen network security.
- Advocate for the development of resource-efficient quantum-resistant algorithms to lower entry barriers for smaller participants.
- Foster transparency and fair competition within the mining ecosystem, ensuring equitable access to advanced technologies and software.
- Engage with policymakers to incentivize equitable mining practices and renewable energy adoption through subsidies, tax credits, or grants.

### B.4. Phased Transition and Continuous Adaptation

A phased roadmap ensures a smooth transition while maintaining security and functionality [8], [238]. Key considerations include:

- **Short-Term:** Conduct readiness assessments, upgrade critical hardware components, and implement baseline quantum-resistant algorithms for low-impact operations. Perform pilot testing to identify vulnerabilities.
- **Medium-Term:** Deploy advanced quantum-resistant algorithms for key-intensive processes, refine mining software for efficiency, and optimize energy consumption. Enhance interoperability with legacy BC nodes.
- **Long-Term:** Achieve full quantum resistance by adopting industry-standard post-quantum cryptographic mechanisms, aligning with emerging consensus protocols, and continuously adapting to advancements in QC.
- Use predictive analytics to anticipate and respond to changes in computational demand and environmental factors.

### B.5. Governance and Economic Considerations

The transition to quantum secure BC requires coordination and financial support to prevent smaller mining pools from being marginalized [239], [240].

- Establish a decentralized governance structure to coordinate upgrades across mining pools and ensure compliance with quantum-resistant standards.

- Implement shared resource models, such as pooled access to quantum-resistant hardware or cloud services, to reduce costs for smaller participants.
- Engage policymakers to provide financial incentives, such as grants or tax credits, for adopting quantum-resistant technologies and renewable energy sources.

By addressing these challenges and implementing robust solutions, mining pools can effectively navigate the complexities of operating in a quantum-secure environment. This ensures their continued contribution to the BC ecosystem's resilience, scalability, and security in the QC era.

## C. Transaction Verification Mechanism

The transition to quantum-resistant algorithms presents significant challenges for verifying transactions within BC networks. Careful consideration and adaptation are crucial to maintain network integrity and security. By proactively addressing these challenges, organizations can ensure a smooth transition and safeguard the enduring security and efficiency of their BC networks.

### C.1. Consensus Protocol Adaptation

Existing consensus mechanisms, which ensure network integrity by verifying transactions and reaching agreement on the BC state, might require adjustments to mitigate the risk of unauthorized control after the switch to quantum-resistant cryptography. Quantum-resistant algorithms can alter the computational power dynamics within the network (e.g., some algorithms might be more efficient for specific hardware), potentially creating vulnerabilities for malicious actors [197], [241]. Potential proactive approaches include:

- Analyze consensus mechanisms for potential vulnerabilities arising from the adoption of quantum-resistant algorithms.
- Modify parameters related to block validation, voting power, and dispute resolution mechanisms to address these vulnerabilities and maintain network security.
- Explore alternative consensus mechanisms specifically designed for quantum-resistant environments that offer inherent resistance to unauthorized control. Some existing proposals include post-quantum voting-based variants.

### C.2. Increased Computational Overheads

The complex nature of quantum-resistant cryptographic operations might introduce performance slowdowns [8], [168], [231] due to increased computational demands for transaction verification. This could lead to longer processing times and potentially affect the scalability of the BC network. Potential proactive strategies to mitigate this challenge include:

- Optimize the implementation of quantum-resistant algorithms within the transaction verification process. This could involve code refactoring and leveraging hardware acceleration techniques.
- Explore alternative cryptographic schemes that offer a balance between security and computational efficiency in the context of transaction verification.

- Consider sharding, increasing block size or other scalability solutions to distribute the workload of transaction verification across multiple nodes within the network.
- Leveraging interoperability protocols facilitating network communication between different BCs, allowing load distribution.
- Utilize quantum-resistant off-chain scaling solutions, encompassing methodologies such as state channels, sidechains, Plasma, and rollups, which facilitate the execution and processing of transactions externally to the primary BC. This approach augments scalability by ensuring that only crucial state changes are finalized on-chain. Additionally, this necessitates the development of efficient and quantum-resistant ZKPs.

### C.3. Implementation Complexity

Integrating quantum-resistant cryptography adds complexity to existing systems, potentially introducing new security vulnerabilities [11], [228]. This complexity can affect transaction verification mechanisms within the BC. Potential proactive measures include:

- Ensure thorough analysis and testing of the integration process to identify and address potential security vulnerabilities introduced by implementation complexity.
- Implement secure coding practices and adhere to established cryptographic standards to mitigate the risk of exploitation due to implementation complexity.
- Provide specialized training and resources for developers to effectively manage the intricacies of integrating PQC into transaction verification mechanisms.
- Collaborate with experts in quantum-resistant cryptography to ensure the robustness and integrity of the embedded solutions.

### C.4. Maintaining Decentralization

The increased computational demands of quantum-resistant algorithms might inadvertently lead to centralization within the network. Only entities with access to powerful hardware might be able to efficiently participate in transaction verification [36]. Potential Solutions include:

- Encourage the development of more resource-efficient quantum-resistant algorithms that are accessible to a wider range of hardware capabilities.
- Explore alternative consensus mechanisms that promote decentralization and participation even with computationally intensive verification processes.
- Implement incentive structures that reward efficient verification and participation, regardless of the computational resources available to individual nodes.

By addressing these challenges and implementing appropriate solutions, organizations can ensure a smooth transition for transaction verification mechanisms in BC networks. This will maintain network integrity, efficiency, and decentralization even in the face of potential threats from quantum computers.

## D. Smart Contract

The shift to quantum-resistant algorithms within BC networks introduces a unique set of challenges for smart contracts. These challenges include potential security vulnerabilities arising from interactions with new algorithms, compatibility issues with existing smart contracts, and the need for user education regarding the transition. Addressing these challenges is crucial for ensuring the seamless integration and continued functionality of smart contracts in a quantum-secure environment.

### D.1. Compatibility with Existing Smart Contracts

Upgrading existing smart contracts to utilize quantum-resistant algorithms might not be straightforward. This could lead to a situation where some contracts operate with the old cryptography while others adopt the new, potentially hindering interoperability and causing disruptions. Potential mitigation strategies include:

- Develop migration tools and frameworks to facilitate a smooth transition of existing smart contracts to utilize quantum-resistant algorithms [242].
- Explore the creation of standardized wrappers or compatibility layers that allow older smart contracts to interact seamlessly with newer ones using quantum-resistant cryptography (consider potential overhead of wrappers) [243].
- Encourage developers to design smart contracts with modularity and future-proofing in mind, making them easier to adapt to evolving cryptographic standards [95].

### D.2. User Education and Awareness

Users interacting with smart contracts need to be aware of the transition to quantum-resistant algorithms and the potential risks involved if they do not upgrade their tools and interact with outdated, vulnerable smart contracts. Proactive strategies include:

- Develop educational resources and awareness campaigns to inform users about the importance of upgrading their wallets and tools to interact with quantum-resistant smart contracts [35].
- Implement clear warnings and notifications within BC applications to highlight the risks of interacting with outdated smart contracts [35].
- Promote best practices for secure smart contract interaction, including proper key management and verification of contract details before execution [244].

### D.3. Unforeseen Vulnerabilities

The interaction between existing smart contract code and the new quantum-resistant cryptography might introduce unforeseen vulnerabilities. These vulnerabilities could potentially allow unauthorized access to funds or manipulation of smart contract execution [245], [246]. Possible mitigation strategies for these vulnerabilities include:

- Conduct thorough audits and validation processes specifically designed to identify vulnerabilities arising from the interaction between smart contracts and quantum-resistant algorithms.

- Encourage the development and use of formal verification techniques to mathematically prove the security of smart contracts in a quantum-resistant environment.
- Promote best practices for smart contract development that prioritize security and minimize potential attack vectors, especially when interacting with quantum-resistant cryptography.

#### D.4. Performance Implications

Integrating quantum-resistant algorithms may impact the performance of smart contracts due to increased computational requirements. This can lead to higher execution costs and longer processing times [247], [248]. Potential solutions include:

- Review and optimize the smart contract code to reduce complexity and enhance execution efficiency. This may involve minimizing redundant computations and optimizing data structures.
- Aggregate multiple transactions into a single batch to minimize the number of on-chain operations and reduce congestion.
- Optimize quantum-resistant algorithms to reduce computational overhead and improve efficiency.
- Implement off-chain computations where feasible to minimize on-chain processing demands.
- Explore mechanisms for modular implementation and asynchronous execution of smart contracts, allowing certain tasks to run independently, thus improving throughput.
- Regularly benchmark and monitor smart contract performance to identify and address bottlenecks.

#### D.5. Regulatory Considerations

The transition to quantum-resistant cryptography may be subject to regulatory requirements and standards. Organizations must ensure compliance with evolving guidelines to avoid legal and operational risks [243], [249]. Steps to consider:

- Stay informed about regulatory developments related to quantum-resistant cryptography and BC technologies.
- Engage with policymakers and industry groups to contribute to the development of practical and effective regulations.
- Implement compliance frameworks that align with current and anticipated regulatory standards.

By addressing these challenges and implementing effective solutions, organizations can ensure the continued security and functionality of smart contracts in a quantum-resistant future.

#### E. User Wallet

The transition to quantum-resistant BC presents specific challenges for user wallets, which are critical interfaces for users to access and manage their digital assets. Ensuring a seamless and secure transition is paramount to maintain user trust and the integrity of the BC ecosystem. In the following, we examine the primary challenges and propose solutions to facilitate this transition.

##### E.1. Wallet Compatibility and Security Upgrades

Existing user wallets might not be compatible with the new quantum-resistant cryptography. This leaves users vulnerable to potential attacks that exploit weaknesses in older cryptographic algorithms [1], [2], [197]. Potential Solutions include:

- Develop and disseminate clear upgrade paths and comprehensive instructions to assist users in transitioning to wallet versions that implement quantum-resistant algorithms.
- Implement backward-compatible solutions where feasible to ensure continuity of service during the transition period.
- Encourage wallet developers to adopt standardized quantum-resistant cryptographic protocols to maintain interoperability across the BC network.
- Implement multi-signature wallets to enhance security. This requires multiple keys to authorize a transaction, adding another layer of protection.

##### E.2. User Education and Awareness

In the context of user adoption [250], individuals might be hesitant or unaware of the need to upgrade their wallets, potentially leaving them vulnerable even after the transition to quantum-resistant algorithms. Potential Solutions include:

- Launch educational campaigns to inform users about the importance of upgrading to quantum-resistant wallets and the associated security benefits.
- Integrate intuitive prompts and automated update features within wallet applications to facilitate seamless user transitions.
- Provide accessible resources, such as tutorials and FAQs, to assist users in understanding and navigating the upgrade process.

##### E.3. Maintaining User Experience

Upgrading wallets and potentially adopting new functionalities related to quantum-resistant cryptography might introduce complexities that could hinder user experience [251]. Potential Solutions include:

- Design wallet interfaces that incorporate new security features without compromising simplicity and user-friendliness.
- Conduct user testing to identify and address potential usability issues arising from the integration of quantum-resistant features.
- Ensure that security enhancements are implemented in a manner that is transparent to users, minimizing disruptions to their typical interactions with the wallet.

By proactively addressing these challenges through strategic upgrades, user education, and thoughtful design, organizations can ensure that user wallets remain secure and user-friendly in the quantum-resistant era of BC technology.

## VII. HYBRID BC ARCHITECTURES

Given the limitations of quantum-resistant BC, developing effective transition strategies is crucial for mitigating quantum threats to a BC system. A comprehensive security approach

requires a hybrid strategy that integrates PQC with meticulous system design and continuous monitoring [11]–[13]. This hybrid approach combines classical and post-quantum cryptography, ensuring a smoother transition while maintaining operational integrity and reducing risks during and after migration [1], [2]. Key advantages of this approach include: (a) interoperability between classical and post-quantum BCs, (b) backward compatibility with existing systems, (c) enhanced security during the transition, (d) layered cryptographic protection against both classical and quantum threats, and (e) scalability through selective application of post-quantum algorithms. Additionally, it addresses challenges such as increased key sizes, network fragmentation, and performance overheads associated with a full PQC transition [17]–[19].

To address these challenges and facilitate a smooth transition, two primary hybrid BC architectures are proposed: *Non-Composite* and *Composite*. These architectures integrate classical cryptography (for backward compatibility) and post-quantum cryptography (for future security), enabling BC systems to gradually adopt quantum-resistant algorithms while maintaining uninterrupted operations. By combining classical and quantum-resistant cryptographic approaches, these architectures establish a multi-layered security framework to mitigate quantum-related vulnerabilities [252].

#### A. Non-Composite Architecture

The Non-Composite BC Architecture adopts a dual-ledger strategy, maintaining separate ledgers with distinct cryptographic functionalities. A public ledger secured with classical cryptography handles routine transactions, while a private ledger secured with post-quantum cryptography is used for high-security transactions. This separation provides a clear migration path to quantum resistance. Figure 9 illustrates this architecture.

- **Public Ledger (Classical Cryptography):** Handles routine transactions using existing cryptographic standards, offering compatibility with current systems but becoming vulnerable to quantum attacks as QC advances.
- **Permissioned Private Ledger (Post-Quantum Cryptography):** Dedicated to highly sensitive transactions, leveraging post-quantum cryptographic algorithms with stricter access controls to resist quantum threats.

While this architecture provides robust security for sensitive transactions, it faces several challenges:

- **Integration Complexity:** Managing separate ledgers within one BC ecosystem introduces significant implementation and operational complexity.
- **Interoperability Issues:** Seamless interaction between ledgers secured with different cryptographic frameworks is difficult to achieve.
- **Infrastructure Overhead:** Maintaining two parallel ledgers requires additional computational and storage resources, increasing operational costs.

#### B. Composite Architecture

The Composite BC Architecture integrates classical and post-quantum cryptographic functionalities within a single

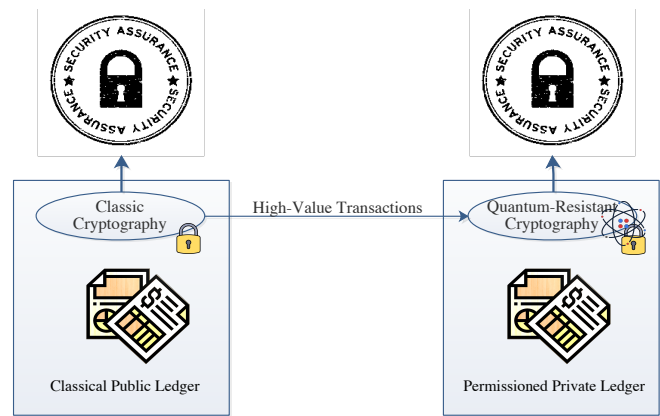


Fig. 9: Non-Composite BC Architecture

ledger. Each block contains sections dedicated to both cryptographic approaches, facilitating gradual migration and maintaining a unified ledger structure. Figure 10 illustrates this architecture.

- **Integrated Sections:** Each block includes sections for classical and post-quantum cryptography, enabling a seamless transition to quantum resistance without maintaining separate ledgers.
- **Dual Cryptographic Operations:** Transactions requiring high security use post-quantum cryptography, while less critical operations utilize classical cryptography for performance optimization.

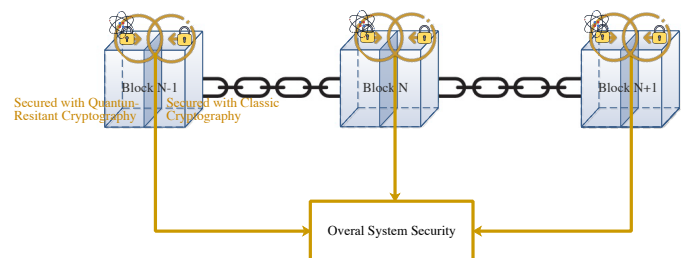


Fig. 10: Composite BC Architecture

The Composite Architecture simplifies integration but introduces its own challenges:

- **Increased Block Size:** Dual cryptographic operations increase block size, potentially affecting scalability and transaction throughput [15].
- **Reliance on Standardization:** Dependence on standardized post-quantum cryptographic algorithms, which are still under development, adds uncertainty [58].
- **Protocol Modifications:** Significant changes to existing BC protocols are needed to support dual cryptographic functionalities [253].

#### C. Choosing the Right Architecture

The selection of an appropriate architecture depends on the specific needs of the BC application, with the following key considerations:

- **Security Needs:** The Non-Composite approach is ideal for applications requiring stringent security for sensitive transactions.
- **Integration Simplicity:** The Composite approach minimizes structural changes, making it more suitable for general use cases.
- **Performance Optimization:** The Composite Architecture balances security and scalability, enabling efficient handling of less critical transactions.

Table XIII provides a detailed comparison of the two architectures, highlighting their strengths and weaknesses across various dimensions.

TABLE XIII: Comparison of Composite and Non-Composite BC Architectures

Feature	Composite BC Architecture	Non-Composite BC Architecture
Cryptographic Strategy	Both classical and post-quantum cryptographic methods coexist in the same block, enabling selective use based on transaction requirements.	Separate ledgers: one with classical cryptography, another with post-quantum cryptography.
Transition Approach	Gradual migration to post-quantum cryptography, allowing classical cryptography to remain for less critical transactions.	Clear separation of classical and post-quantum cryptography with distinct ledgers for different purposes. Classical transactions must migrate to the post-quantum ledger for full security.
Compatibility	Maintains compatibility with existing BC infrastructure and participants, minimizing disruption.	Requires significant infrastructure changes, potentially disrupting existing systems.
Performance Impact	Minimizes performance issues by using classical cryptography for less critical transactions. The increased block size may affect scalability.	Post-quantum cryptography is only used in the permissioned private ledger, potentially offering better performance for routine transactions.
Security	Security relies on the most robust cryptographic primitive (post-quantum) in the block. Redundancy ensures that if classical cryptography is compromised, the post-quantum layer maintains security.	Ensures maximum security for sensitive transactions, as they are fully isolated on a post-quantum secured ledger. Routine transactions on the classical ledger remain vulnerable to quantum attacks.
Scalability	Potential increase in block size due to the inclusion of both classical and post-quantum cryptographic methods.	Scalability is less impacted for routine transactions, but managing separate ledgers adds complexity and operational overhead.
Implementation Complexity	Moderate complexity, as existing blocks need to accommodate both cryptographic methods within a unified ledger.	High complexity due to the need for maintaining and managing separate ledgers with distinct cryptographic frameworks.
Flexibility	High flexibility: Allows different cryptographic sections for different transaction needs within a single ledger.	Limited flexibility: Transactions are strictly assigned to either the classical or post-quantum ledger, restricting dynamic use.
Integration Complexity	Requires protocol modifications to support dual cryptographic functionalities but maintains a unified structure.	Managing two separate ledgers introduces significant operational and implementation challenges, including interoperability issues.
Security Transition	Enables a gradual and seamless transition to quantum-resistant cryptography, providing time for testing post-quantum algorithms in the ecosystem.	More disruptive transition: Classical transactions must migrate to the post-quantum ledger, increasing risk during the migration period.
Risk Mitigation	Redundancy ensures that if classical cryptography is compromised, the post-quantum cryptography within the same block can still ensure security.	Risk mitigation depends on isolating sensitive transactions within the post-quantum secured private ledger. Routine transactions remain vulnerable.
Ease of Adoption	Easier adoption for existing BC networks, as it minimizes changes to core infrastructure and ensures backward compatibility.	Harder to adopt, requiring more significant changes and careful management of two distinct ledgers.
Future-Proofing	Allows for future adjustments and the introduction of more efficient post-quantum algorithms as standards evolve (e.g., NIST PQC).	Ensures the highest security for critical transactions but may face challenges in upgrading cryptographic standards due to the segregated ledger design.
Use Case Suitability	Suitable for a phased transition with minimal disruption to regular operations.	Best suited for use cases requiring isolated, high-security transactions with clear cryptographic separation.
Standardization Reliance	Relies on the development and standardization of post-quantum cryptographic algorithms (e.g., NIST PQC).	Similarly relies on standardized post-quantum cryptography but within a separate, more secure ledger structure.

#### D. Hybrid Strategies for Cryptographic Primitives of BC

Hybrid BC architectures rely on robust cryptographic primitives to secure key functionalities such as key exchange, encryption, and digital signatures. These hybrid strategies combine classical and post-quantum cryptography to facilitate

a secure transition to quantum-resistant systems. By enabling “crypto-agility,” hybrid strategies allow BC systems to adapt seamlessly to evolving cryptographic standards [88], [254].

Two critical approaches are integral to these strategies: the Hybrid KEM/ENC Strategy and the Hybrid Signature Strategy. Both play a pivotal role in enhancing the robustness of Non-Composite and Composite BC architectures.

TABLE XIV: Hybrid KEM/ENC Strategy

Combiners	Pros	Cons
Concatenation [255]	• Supports lightweight operations, simple logic, and easy implementation.	• Requires inclusion of PQ key, potentially altering FIPS 140 validation. • Lack of integrity protection for concatenated shared secret key components. • Limited security proofs to classical adversaries [256].
Concat-KDF [253], [257]–[260]	• Combines key exchange outputs through a single KDF, reducing brute-force effectiveness.	• Requires inclusion of PQ key in code, potentially altering FIPS 140 validation. • Security depends on the models and assumptions about KEM/ENC and KDF.
Cascade-KDF [253]	• Produces shared secret using cascade of KDF iterations, maintaining efficiency. • Reduces brute-force effectiveness.	• Requires inclusion of PQ key in code, potentially altering FIPS 140 validation. • Security guaranteed only under specific models and assumptions about KDF.
Dual-PRF [15], [261]	• Maintains IND-CCA security if one KEM/ENC and Pseudorandom Function (PRF) components are secure. • Provides security proofs for classical and quantum adversaries.	• Requires extra preprocessing for the first key.
Nested-Dual-PRF [15]	• Preserves IND-CCA security with secure KEM/ENC and PRF components. • Offers security proofs for classical and quantum adversaries.	• Requires additional preprocessing for the first key.
Split-key-PRF [262]	• Maintains IND-CCA security with split-key pseudorandom combiner. • Trade-off between security and efficiency in parallel combiners.	• Provides security proofs only for classical adversaries.
XOR [262]–[264]	• Supports lightweight operations and easy implementation.	• XOR’s reversibility can compromise sub-keys, leading to potential master key recovery and vulnerability to related-key attacks, compromising cipher security. It maintains solely IND-CPA security as discussed in [262], supports one-way authenticated key exchange (1W-AKE) as per [263], and offers breakdown-resilient authenticated key exchange (AKE) as outlined in [264]. Security proofs are provided only for classical adversaries [262], [263].
XOR-then-MAC [15]	• Prevents mix-and-match attacks, maintains IND-CCA security, and provides security against classical, partial, and fully quantum adversaries, while also protecting ciphertext from modification and relying on the security of one combined KEM/ENC and the Message Authentication Code (MAC) scheme’s unforgeability.	• Vulnerable to message content modification depending on MAC security.
XOR-then-PRF [262]	• Simply replaces XOR for providing integrity protection on ciphertexts.	• Vulnerable to intentional message content modification and related-key attacks due to PRF security issues. • Does not retain CCA security and provides security proofs only for classical adversaries.

1) *Hybrid KEM/ENC Strategy:* Although BC systems primarily depend on digital signatures for transaction authentication and verification, Hybrid KEM/ENC strategies are highly relevant in the broader BC ecosystem. These strategies play a vital role in several contexts, including secure off-chain communication, wallet security, Layer-2 and cross-chain applications, confidential transactions, and key management in IoT and smart contract ecosystems. By integrating Hybrid KEM/ENC strategies, BC systems can address quantum-related vulnerabilities comprehensively, ensuring security across all layers of the ecosystem and preparing for emerging use cases requiring secure, quantum-resistant key exchange.

In the realm of KEM/ENC, the hybrid approach amalgamates multiple KEM/ENC algorithms by using specific combiners. This process yields hybrid algorithms whose security levels match those of their strongest

components. Combiners such as Concatenation [255], Concat-Key Derivation Function (KDF) [253], [257]–[259], Cascade-KDF [253], Dual-PRF [15], [261], Nested-Dual-PRF [15], Split-key-PRF [262], XOR [262]–[264], XOR-then-MAC [15], and XOR-then-PRF [262] offer distinctive advantages ranging from simplicity and resilience against brute-force attacks to seamless integration with existing infrastructure. Careful consideration of the advantages and disadvantages of each combiner is essential to wisely choose the best strategy for managing the migration of BC systems.

TABLE XV: Hybrid Signature Strategy

Combiners	Pros	Cons
Concatenation [265]	<ul style="list-style-type: none"> <li>Supports lightweight operations, simple logic, and easy implementation.</li> <li>Retains unforgeability when both signature algorithms are unforgeable.</li> </ul>	<ul style="list-style-type: none"> <li>Does not support non-separability property for both signature algorithms.</li> </ul>
Weak Nesting [265]	<ul style="list-style-type: none"> <li>Preserves unforgeability when the first signature algorithm is unforgeable.</li> <li>Supports non-separability property for the second signature algorithm.</li> </ul>	<ul style="list-style-type: none"> <li>Unforgeability of weak nesting depends crucially on the unforgeability of the first signature scheme.</li> </ul>
Strong Nesting [16], [265]	<ul style="list-style-type: none"> <li>Retains unforgeability when both signature algorithms are unforgeable.</li> <li>Preserves non-separability property for the second signature algorithm.</li> </ul>	<ul style="list-style-type: none"> <li>Caution needed with Strong Nesting due to potential signature leaks from one of its underlying schemes.</li> </ul>
Dual Nesting [265]	<ul style="list-style-type: none"> <li>Preserves unforgeability of each message under its corresponding signature scheme.</li> <li>Retains unforgeability of both messages when the outer signature scheme is unforgeable.</li> </ul>	<ul style="list-style-type: none"> <li>Not designed to provide the unforgeability of both messages under either signature scheme.</li> </ul>

2) *Hybrid Signature Strategy*: Similarly, the hybrid signature strategy endeavors to amalgamate multiple independent signatures, ensuring the integrity and unforgeability of resultant signatures against chosen message attack scenarios. Embracing a diverse range of combiners including Concatenation [265], Weak Nesting [265], Strong Nesting [16], [265], and Dual Nesting [265], this strategy equips organizations with a comprehensive array of cryptographic tools meticulously designed to counteract potential adversaries, while safeguarding the integrity of signatory intent. A thorough evaluation of each combiner’s strengths, weaknesses, and susceptibility to quantum vulnerabilities is essential for crafting a resilient cryptographic framework capable of withstanding the challenges of the quantum era.

3) *Integration with BC Architectures*: Both the KEM/ENC and Signature strategies align seamlessly with Non-Composite and Composite BC architectures. In Non-Composite architectures, they provide tailored cryptographic solutions for each ledger, ensuring security based on sensitivity. In Composite architectures, they enable dual cryptographic sections within each block, allowing transactions to select the most appropriate mechanism based on security and performance requirements.

The integration of hybrid strategies for cryptographic primitives fortifies BC architectures against emerging quantum threats. By leveraging robust combiners for KEM/ENC and digital signatures, BC systems can achieve a high degree of security, flexibility, and resilience. These strategies lay the foundation for a secure and scalable transition to quantum-resistant systems.

#### E. Advantages of Hybrid BCs

Hybrid BCs represent a strategic response to the dynamic landscape of cryptography and the impending challenges

posed by QC, providing a synthesis of security, adaptability, and future readiness tailored to the varied requirements of BC participants. They offer numerous compelling advantages:

- **Smooth Transition and Future-Proofing**: Enables a phased approach to transitioning to quantum-resistant cryptography while mitigating risks and ensuring ongoing security.
- **Reduced Fragmentation and Enhanced Ecosystem Compatibility**: Minimizes potential fragmentation within the BC ecosystem by combining classical and quantum-resistant functionalities, fostering interoperability.
- **Ongoing Research and Continuous Improvement**: Facilitates seamless integration of evolving quantum-resistant cryptography, ensuring continued resilience against potential QC threats.

#### F. Risk Assessment and Security Posture

The hybrid approach leverages the strength of its most robust cryptographic primitive to safeguard the overall system’s security even if other algorithms are rendered vulnerable by future quantum attacks (see Figure 11). This selective focus ensures minimal disruption during migration by maintaining a well-defined security baseline built upon the strongest primitive. By adopting this strategy, BC stakeholders can proactively address the challenges of QC and achieve a seamless transition to quantum-resistant cryptography with confidence.

The security posture differs slightly between the two hybrid approaches:

- **Non-Composite Approach**: Here, the permissioned private ledger, which is secured with quantum-resistant algorithms, acts as the primary shield. Even if the classical cryptography on the public ledger gets compromised, the system can still function securely for highly sensitive transactions as long as the private ledger remains secure.
- **Composite Approach**: This approach integrates classical and quantum-resistant algorithms within the same ledger structure. However, the overall security hinges on the strength of the most robust primitive (ideally the quantum-resistant one). If this remains secure, it protects the entire system.

		Risk (Primitive 2)		
		Low	Medium	High
Risk (Primitive 1)	Low	Low	Low	Low
	Medium	Low	Medium	Medium
	High	Low	Medium	High

Fig. 11: Combined Risk of Hybrid Approach from Underlying Primitives

#### G. Final Discussion: Adapting Hybrid BCs for Quantum Resistance

Hybrid BC architectures balance security, scalability, and compatibility, offering a strategic response to QC threats. While challenges in integration and infrastructure remain, the

TABLE XVI: Impact of Quantum Computing on Different BC Platforms

Platform	Vulnerable Components	Potential Impacts	STRIDE Threats	L	I	R	Mitigation Strategies
Bitcoin	<ul style="list-style-type: none"> <li>ECDSA: Used for digital signatures.</li> <li>SHA-256: Used for hashing blocks.</li> </ul>	<ul style="list-style-type: none"> <li>Forgery of digital signatures, enabling unauthorized spending.</li> <li>Breaking collision resistance of SHA-256, disrupting mining and block verification.</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Impersonation through compromised signatures</li> <li>Tampering: Alteration of transaction data or blocks</li> <li>Repudiation: Disputes arising from forged transactions</li> <li>DoS: Mining and consensus disruption</li> <li>Elevation of Privilege: Unauthorized network control through compromised keys</li> </ul>	H	H	H	<ul style="list-style-type: none"> <li>Transition to quantum-resistant signature schemes</li> <li>Transition to a stronger hash function</li> <li>Develop quantum-resistant PoW or use alternative approaches such as proof-of-space or memory-hard PoW to mitigate quantum mining advantages.</li> </ul>
Ethereum	<ul style="list-style-type: none"> <li>ECDSA: Used for digital signatures.</li> <li>Keccak-256: Used for hashing transactions and blocks.</li> <li>Elliptic Curve Integrated Encryption Scheme (ECIES): Encrypts communication (less common).</li> </ul>	<ul style="list-style-type: none"> <li>Signature forgery and potential disruption of consensus mechanism.</li> <li>Breach of encrypted communication.</li> <li>Tampering with smart contract states or inputs.</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Identity impersonation via ECDSA compromise</li> <li>Tampering: Block manipulation by breaking Keccak-256</li> <li>Repudiation: Disputes from forged or altered transactions</li> <li>Information Disclosure: Leaked data through broken ECIES encryption</li> <li>DoS: Quantum attacks degrading network operations</li> <li>Elevation of Privilege: Unauthorized access to smart contracts</li> </ul>	H	H	H	<ul style="list-style-type: none"> <li>Migration to quantum-resistant signature schemes</li> <li>Replace ECIES with a post-quantum KEM</li> <li>Use a higher-security hash function in block hashing</li> <li>Formal verification of smart contracts to eliminate vulnerabilities</li> <li>Develop quantum-resistant smart contract libraries and frameworks</li> </ul>
Ripple	<ul style="list-style-type: none"> <li>ECDSA: Used for digital signatures.</li> <li>SHA-256: Used for hashing transactions.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized manipulation of transactions and account balances.</li> <li>Limited relevance for Information Disclosure due to Ripple's simpler metadata structure.</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Forged transactions through signature compromise</li> <li>Tampering: Manipulation of transaction data</li> <li>Repudiation: Disputes arising from altered balances</li> <li>DoS: Attacks exploiting consensus mechanisms</li> <li>Elevation of Privilege: Misuse of validator roles via key compromise</li> </ul>	H	H	H	<ul style="list-style-type: none"> <li>Similar mitigation strategies as Bitcoin and Ethereum</li> <li>Explore alternative consensus mechanisms less vulnerable to quantum attacks (e.g., voting-based consensus algorithms)</li> <li>Strengthen validator key management to prevent privilege escalation.</li> </ul>
Litecoin	<ul style="list-style-type: none"> <li>Scrypt: Memory-intensive PoW hashing algorithm (more ASIC-resistant than SHA-256).</li> <li>ECDSA: Used for digital signatures.</li> </ul>	<ul style="list-style-type: none"> <li>Scrypt provides some resistance, but QC can break it.</li> <li>ECDSA is vulnerable to signature forgery.</li> <li>Enhanced quantum mining could enable 51% attacks.</li> <li>Mining disruptions may cause DoS on the network.</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Identity theft through signature compromise</li> <li>Tampering: Block alterations exploiting quantum vulnerabilities</li> <li>Repudiation: Forged transactions leading to disputes</li> <li>DoS: Mining disruption due to compromised algorithms</li> <li>Elevation of Privilege: Unauthorized control of mining resources</li> </ul>	H	H	H	<ul style="list-style-type: none"> <li>Research on memory-hard hashing functions secure against classical and quantum attacks</li> <li>Adopt quantum-resistant signature schemes to replace ECDSA.</li> <li>Explore quantum resistant alternative for PoW mechanisms such as proof-of-space or memory-hard PoW models to enhance resistance.</li> <li>Evaluate Scrypt's quantum resilience and improve hashing where necessary.</li> </ul>
Zcash (Privacy Coin)	<ul style="list-style-type: none"> <li>Standard Transactions: <ul style="list-style-type: none"> <li>ECDSA/SHA-256: Used for signatures and hashing, similar to Bitcoin.</li> </ul> </li> <li>Shielded Transactions: <ul style="list-style-type: none"> <li>Groth16 zk-SNARKs* (Elliptic curve and pairing-based cryptography): Used for private transactions.</li> <li>ECC-based key generation: Supports Groth16 and transaction privacy.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Vulnerable to signature forgery and block tampering.</li> <li>Loss of anonymity if Groth16 is broken by quantum attacks.</li> <li>Potential manipulation of shielded transactions if proofs or keys are compromised.</li> <li>Disruption of shielded transaction validation due to computational overload.</li> </ul>	<ul style="list-style-type: none"> <li>Spoofing: Signature forgery enabling identity theft</li> <li>Tampering: Modification of transaction data</li> <li>Repudiation: Disputes from altered or forged transactions</li> <li>DoS: Disruption of standard transaction processing</li> <li>Information Disclosure: Loss of privacy due to ZKP compromise</li> <li>Tampering: Unauthorized modification of shielded transactions</li> <li>Repudiation: Disputes from forged proofs</li> <li>DoS: Disruption of shielded transaction processing</li> <li>Elevation of Privilege: Exploiting ZKP weaknesses to gain unauthorized control</li> </ul>	H	H	H	<ul style="list-style-type: none"> <li>Transition from ECDSA to post-quantum signature schemes (e.g., lattice-based cryptography)</li> <li>Replace SHA-256 with SHA-512 or alternatives such as SHA-3</li> <li>Research and implement post-quantum zk-SNARKs (e.g., Virgo [266], Ligero [267] and Aurora [268]) and post-quantum signatures.</li> <li>Develop fallback mechanisms to handle computational overload or proof failures</li> <li>Enhance network-wide transition plans to quantum-resistant cryptography</li> </ul>

\*In May 2022, Zcash introduced the Orchard shielded payment protocol with Network Upgrade 5 (NU5), using the Halo 2 zero-knowledge proving system. Halo 2 removes the trusted setup and supports scalable private payments. While it improves efficiency over previous zk-SNARKs like Groth16, its security depends on assumptions not proven secure against quantum attacks.

long-term benefits of enhanced security and future-proof design make these architectures a critical step towards quantum-resistant BCs.

### VIII. SECURITY EVALUATION OF MAJOR BC PLATFORMS

This section presents a detailed analysis of the potential impact of QC on major BC platforms, including Bitcoin [269], Ethereum [270], Ripple [271], Litecoin [272], and Zcash [273], a privacy-focused cryptocurrency. The analysis examines their vulnerable components, assesses potential impacts, analyzes associated STRIDE threats, and provides an evaluation of likelihood, impact, and overall risk levels under the assumption of a sufficiently advanced QC environment. Table XVI offers a consolidated reference for understanding these implications.

It is important to emphasize that the likelihood ratings assigned in the Table represent a scenario in which large-scale quantum computers are available and capable of breaking or weakening current cryptographic primitives. Our earlier analysis (Figure 4) indicates that the expected likelihood of such powerful quantum threats remains relatively low in the short term (within the next 10 years), increases to a medium level by around 15 years, and becomes high beyond a 20-year horizon. Thus, the *High* likelihood ratings in Table XVI should be interpreted as long-term projections rather than immediate

certainties. In the near term, due to the limited maturity of QC, these threats are far less likely to materialize.

The evaluation reveals that all these BC platforms, despite architectural differences, could face severe consequences once quantum attacks become feasible. Bitcoin and Ethereum, heavily reliant on ECDSA signatures and their respective cryptographic hash functions, would be susceptible to unauthorized transactions and mining disruptions. Ripple, while somewhat centralized, still depends on ECDSA and SHA-256, making it vulnerable to signature forgery and ledger manipulation. Litecoin's use of Scrypt may provide partial near-term mitigation, but as quantum capabilities advance, its reliance on ECDSA remains a critical vulnerability. Despite Zcash's use of complex privacy mechanisms like Groth16 zk-SNARKs or Halo 2 recursive proofs, which enable fast, private transactions through elliptic curve cryptography, it could still suffer anonymity breaches and compromised transaction integrity under a quantum-capable adversary.

While the immediate risks remain low, given the current state of quantum technology, the potential long-term impact is undeniably high. Unauthorized spending, tampering with transaction data, erosion of trust, and systemic collapse are all plausible outcomes once robust quantum machines emerge. This underscores the crucial importance of transitioning to post-quantum cryptographic primitives well before the threats mature. Adopting quantum-resistant signatures,



TABLE XVII: Post-Quantum BC Platforms: Features, Applications, and STRIDE Threats with Corrected Risk Assessment

Platform	Structure	BC Type	Consensus Mechanism	Crypto Type	Signature Alg.	Application	STRIDE Threats	L	I	R
QRL [274]	BC	Permissionless Public	PoS (QRL PoS)	Hash	XMSS	Digital asset safety	<ul style="list-style-type: none"> <li>• Spoofing: Strong resistance via XMSS but risks arise from weak supporting infrastructure.</li> <li>• DoS: Resource exhaustion from computational overhead of PQC algorithms.</li> </ul>	M	H	H
Komodo [275]	BC	Permissionless Public	PoW	Lattice	Dilithium	Multi-chain smart contracts	<ul style="list-style-type: none"> <li>• Spoofing: Challenges in integrating Dilithium signatures may introduce vulnerabilities.</li> <li>• Tampering: Risks during cryptographic transitions.</li> <li>• DoS: Overhead of PQC algorithms.</li> </ul>	M	M	M
Nexus [276]	BC	Permissionless Public	PoW, PoS	Lattice	FALCON	Decentralized routing	<ul style="list-style-type: none"> <li>• Tampering: Integrity risks due to decentralized routing.</li> <li>• DoS: Overhead from FALCON scheme may lead to overload.</li> </ul>	M	H	H
Tidecoin [277]	BC	Permissionless Public	PoW	Lattice	FALCON-512	Cryptocurrency	<ul style="list-style-type: none"> <li>• Spoofing: FALCON-512 integration challenges may lead to vulnerabilities.</li> <li>• Tampering: Cryptographic update processes may expose integrity risks.</li> <li>• DoS: Performance constraints from PQC implementations.</li> </ul>	M	H	H
Abelian [278]	BC	Permissionless Public	PoW	Lattice	Dilithium	Privacy-focused cryptocurrency	<ul style="list-style-type: none"> <li>• Information Disclosure: Potential for privacy leaks during PQC transitions.</li> <li>• DoS: High resource demand may be exploited.</li> </ul>	M	H	H
LACChain [279]	BC	Permissioned Public*	Proof of Authority (PoA)	Lattice	FALCON-512	Latin American adoption	<ul style="list-style-type: none"> <li>• Repudiation: Insufficient cryptographic logging during key exchanges may arise.</li> <li>• DoS: Medium likelihood due to potential insider threats and governance vulnerabilities, despite a controlled environment.</li> </ul>	M	M	M
QAN [280]	BC	Hybrid	Proof of Randomness (PoR)	Lattice	Dilithium	Smart contracts, DApps	<ul style="list-style-type: none"> <li>• Tampering: Cryptographic transition risks during hybrid operations.</li> <li>• Elevation of Privilege: Weak hybrid integration could enable unauthorized access.</li> </ul>	M	H	H
HCASH [281]	BC, DAG	Public	PoW, PoS	Lattice	BLISS	Cross-ecosystem data flow	<ul style="list-style-type: none"> <li>• Information Disclosure: Vulnerabilities in data flow management across ecosystems.</li> <li>• DoS: High likelihood from resource-intensive dual structures.</li> </ul>	M	H	H
IOTA [282]	DAG	Permissionless Public	PoS - OTV (On-Tangle-Voting)	Hash	W-OTS**	IoT micro-transactions	<ul style="list-style-type: none"> <li>• Spoofing: Transition to EdDSA signatures may increase impersonation risks.</li> <li>• Tampering: Vulnerabilities in the Tangle's data integrity mechanisms.</li> <li>• DoS: Scalability features may be targeted.</li> </ul>	H	H	H

\* Permissioned Public: Publicly accessible for reading/interacting, but validator roles require authorization by a governing body.

\*\* In April 2021, they transitioned to using EdDSA as their digital signature, replacing W-OTS.

exploring new hashing schemes, and developing post-quantum zero-knowledge proofs will be essential strategies for ensuring the long-term security and viability of these BC platforms in the quantum era.

## IX. POST-QUANTUM BCs: CURRENT AVAILABILITY AND THEIR ROLE

As the threat of QC grows, BC projects have begun integrating PQC to future-proof their systems. These platforms aim to address challenges such as quantum-safe cryptographic integration, performance trade-offs, and interoperability with existing systems, aligning with the broader themes discussed in this section.

Post-quantum BCs employ cryptographic algorithms deemed secure against quantum attacks, including lattice-based, hash-based, multivariate polynomial, and isogeny-based cryptography. As the threat of QC intensifies, BC projects have initiated the integration of PQC to enhance the future resilience of their systems. These platforms aim to achieve quantum-safe cryptographic integration, manage performance trade-offs, and ensure interoperability with existing frameworks. These platforms and their respective features, applications, and risk evaluations are summarized in Table XVII. Examples include QRL [274], Komodo [275], Nexus [276], Tidecoin [277], Abelian [278], LACChain [279], QAN [280], HCASH [281], and IOTA [282]. QRL employs the XMSS hash-based signature scheme to ensure the security of digital assets, offering forward secrecy but with a trade-off in larger signature sizes (e.g., approximately 2 KB compared

to 64 bytes for ECDSA). Komodo leverages the Dilithium lattice-based cryptographic approach for secure multi-chain smart contracts, balancing efficiency and post-quantum security. Nexus utilizes the FALCON signature scheme for decentralized routing, noted for its smaller signature sizes (e.g., 666 bytes for FALCON-512) but requiring robust key management. Tidecoin integrates FALCON-512 signatures with a CPU-friendly PoW consensus mechanism to ensure compatibility with existing devices while addressing quantum threats. Abelian employs the Dilithium signature scheme to enhance privacy in its cryptocurrency platform. LACChain, as shown in Table XVII, leverages post-quantum X.509 certificates and quantum-secure TLS protocols for secure communication in a permissioned-public framework, allowing public read access while restricting validator roles to authorized entities. Platforms such as QAN, a hybrid BC, combine lattice-based Dilithium signatures with PoR consensus for smart contracts and DApps, introducing flexibility but also risks during transitions between classical and post-quantum mechanisms. HCASH, which combines BC and DAG architectures, integrates the BLISS lattice-based signature scheme to facilitate cross-ecosystem data flow. For IOTA, the initial implementation utilized a probabilistic consensus algorithm involving random walks on a DAGs and W-OTS, a hash-based signature scheme, tailored for micro-transactions within IoT environments. However, as indicated in Table XVII, their shift to EdDSA in April 2021 presents significant vulnerabilities considering the impending advent of QC.

Despite these advancements, the adoption of post-quantum BCs faces significant challenges. Performance overheads are a primary concern, as larger key sizes and signatures in PQC algorithms (e.g., XMSS, BLISS) increase computational demands, affecting transaction throughput and straining resource-constrained devices. For instance, XMSS signatures can exceed 2 KB, significantly larger than classical alternatives. Interoperability is another major challenge, as hybrid cryptographic systems combining classical and quantum-resistant methods introduce complexity and potential vulnerabilities during transitions. Platforms like QAN highlight the need for robust synchronization mechanisms to address conflicting cryptographic assumptions. Regulatory uncertainty further compounds these issues, as formal guidelines for integrating PQC into BC applications remain underdeveloped, even as NIST progresses with standardization efforts for algorithms like CRYSTALS-Dilithium and FALCON.

The likelihood and impact of security threats vary significantly across post-quantum BC platforms. For the post-quantum platforms analyzed in Table XVII, QRL, Komodo, Nexus, Tidecoin, Abelian, LACChain, QAN, and HCASH exhibit a "Medium" likelihood of attack, reflecting partial but not trivial vulnerabilities. More specifically, QRL and Tidecoin use resource-intensive PQC algorithms (XMSS and FALCON-512), which can enable DoS attacks but are mitigated by rate-limiting and smaller user bases. Nexus's multi-layer consensus and decentralized routing add complexity yet provide partial resilience. Komodo employs multi-chain smart contracts, introducing bridging and transition risks, though its mature codebase and network segmentation help contain these threats. Abelian's Dilithium-based privacy features may expose metadata if parameters are mishandled, but robust privacy protocols mitigate simple exploits. LACChain's permissioned model reduces external threats but remains vulnerable to insider attacks and governance flaws. QAN's hybrid classical and post-quantum approach can face tampering during cryptographic transitions, yet its niche adoption limits widespread exploitation. HCASH integrates BC and DAG elements, complicating data flow but benefiting from a modest user base and ecosystem isolation. Collectively, these factors place these platforms in a medium likelihood category, recognizing known vulnerabilities while acknowledging partial protections. In contrast, IOTA's transition from W-OTS to EdDSA enhances practical aspects like efficiency and usability, but the reliance on elliptic curve cryptography makes EdDSA inherently vulnerable to quantum attacks. This vulnerability, combined with IOTA's wide deployment in IoT environments, places it at a "High" likelihood of future exploitation by quantum adversaries.

Regarding impact (as per criteria mentioned in Table IV), Komodo and LACChain face a "Medium" level of disruption because their multi-chain design (Komodo) or controlled, permissioned environment (LACChain) helps contain or recover from breaches more readily. Meanwhile, for other post-quantum BC platforms mentioned in Table XVII (i.e., QRL, Tidecoin, Nexus, and IOTA) successful exploits can yield a "High" impact, encompassing severe operational downtime, compromised cryptographic integrity, and significant repu-

tational harm. Ultimately, risk emerges from the interplay of these factors: even a moderately likely exploit can have dire consequences if its impact is sufficiently severe. These scenarios underscore the importance of continuous audits, robust governance, and proactive security measures to safeguard quantum-safe BC ecosystems against evolving threats.

## X. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

The convergence of BC technology with emerging fields such as Web3, quantum Artificial Intelligence (AI), and Machine Learning (ML) represents a paradigm shift, offering opportunities to enhance transparency, security, and scalability in decentralized systems. However, the rapid advancement of QC has introduced existential threats to the cryptographic foundations of BC, necessitating urgent adaptations to preserve the integrity and resilience of these systems. While progress has been made in post-quantum cryptography and hybrid BC architectures, critical challenges remain unresolved, requiring focused research and innovation to ensure BC ecosystems' long-term sustainability.

One critical area is the development of quantum-resilient AI models. As current ML systems often rely on encryption methods vulnerable to quantum attacks, adapting AI algorithms to utilize quantum-resistant cryptographic techniques is necessary to ensure data integrity and confidentiality. Additionally, enhanced security protocols must be implemented as AI integrates into BC systems. The potential for adversarial attacks, where AI models can be manipulated to produce erroneous results, increases in a quantum context. Therefore, research should aim to develop safeguards against both traditional adversarial threats and those posed by quantum capabilities. Interoperability challenges also arise with the integration of AI into DApps on Web3, particularly as transitions to quantum-safe systems occur. Establishing frameworks for seamless interaction between AI models, blockchain networks, and quantum-resistant protocols is vital to prevent fragmentation and ensure comprehensive functionality. Moreover, leveraging AI for real-time monitoring and threat detection within BC environments can enhance security. AI algorithms can be trained to identify unusual patterns and potential vulnerabilities, yet they must also adapt to the evolving landscape of quantum threats. Research should focus on creating AI systems that can dynamically update their threat assessment mechanisms in response to emerging quantum capabilities.

Governance and decision-making processes in decentralized networks may be impacted by the integration of AI technologies. Ensuring secure and transparent governance requires exploration of the implications of QC on consensus mechanisms. Enhanced AI-driven governance frameworks could facilitate more robust decision-making while mitigating risks related to quantum vulnerabilities. Ethical considerations and trust also need to be emphasized. As AI and BC converge, issues surrounding data privacy, bias, and transparency gain importance. The complexities brought forth by the quantum era necessitate the development of comprehensive ethical guidelines and regulatory frameworks tailored to AI in Web3.

Finally, the evolution of advanced ZKPs and other privacy-preserving mechanisms is crucial. As quantum capabilities

advance, research into quantum-resistant ZKPs that integrate with AI applications will be essential for securing privacy-centric platforms within the blockchain ecosystem.

In summary, the convergence of AI, Web3, and BC offers transformative opportunities but also presents unique threats in QC landscape. Targeted research and innovation are vital for developing resilient and secure systems that can thrive in this new era.

## XI. CONCLUSION

The convergence of BC technology and QC presents both unprecedented challenges and remarkable opportunities. While the emergence of QC poses a significant threat to BC security, proactive measures and strategic risk assessment can effectively mitigate these risks and ensure the continued evolution of BC technology in the quantum era.

Across various components of the BC ecosystem – encompassing the network, mining pools, transaction verification mechanisms, smart contracts, and user wallets – the need for quantum-resistant solutions is paramount. Major BC platforms, including Bitcoin, Ethereum, Ripple, Litecoin, and Zcash, require a multifaceted approach to address their vulnerabilities. This involves transitioning to quantum-resistant signature schemes, leveraging formal verification methodologies for smart contracts, and exploring consensus mechanisms inherently resistant to quantum attacks, all essential for bolstering platform resilience.

Safeguarding BC systems from quantum threats necessitates a collaborative effort from all stakeholders within the ecosystem – developers, wallet providers, researchers, and users alike. Maintaining vigilance regarding advancements in QC and proactively implementing robust security measures are crucial for preserving trust, integrity, and resilience in BC technology amidst evolving threats. By fostering collaboration, innovating in the development of quantum-resistant solutions, and adopting a proactive mindset, we can effectively navigate the complex landscape of BC security in the quantum era.

In conclusion, while the challenges posed by QC are formidable, they also catalyze innovation and collaboration. Continued research and development in quantum-resistant cryptography are vital for staying ahead of emerging threats and ensuring the long-term viability of BC technology in an increasingly quantum world. Through proactive risk assessment and strategic defense measures, we can pave the way for a secure and resilient BC ecosystem that thrives in the quantum era.

## REFERENCES

- [1] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, p. 100065, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2590005621000138>
- [2] M. Allende, D. L. León, S. Cerón, A. Pareja, E. Pacheco, A. Leal, M. Da Silva, A. Pardo, D. Jones, D. J. Worrall *et al.*, "Quantum-resistance in blockchain networks," *Scientific Reports*, vol. 13, no. 1, p. 5664, 2023.
- [3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.
- [4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.
- [5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.
- [6] V. Grozer *et al.*, "An efficient brute force attack handling techniques for server virtualization," in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.
- [7] G. Brassard, P. Hoyer, and A. Tapp, "Quantum algorithm for the collision problem," *arXiv preprint quant-ph/9705002*, 1997.
- [8] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation framework for quantum security risk assessment: A comprehensive study for quantum-safe migration," *Available at SSRN 4750609*.
- [9] Y. K. Wong, Y. Zhou, X. Zhou, Y. S. Liang, and Z. Y. Li, "Web 3.0 and quantum security: Long-distance free-space qsd for global web 3.0 networks," *arXiv preprint arXiv:2402.09108*, 2024.
- [10] D. G. Mamatha, N. Dimri, and R. Sinha, "Post-quantum cryptography: Securing digital communication in the quantum era," *arXiv preprint arXiv:2403.11741*, 2024.
- [11] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022.
- [12] K. F. Hasan, L. Simpson, M. A. R. Bae, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, 2024.
- [13] D. Ott, C. Peikert *et al.*, "Identifying research challenges in post quantum cryptography migration and cryptographic agility," *arXiv preprint arXiv:1909.07353*, 2019.
- [14] H.-Y. Kwon, I. Bajuna, and M.-K. Lee, "Compact hybrid signature for secure transition to post-quantum era," *IEEE Access*, 2024.
- [15] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, and D. Stebila, "Hybrid key encapsulation mechanisms and authenticated key exchange," in *International Conference on Post-Quantum Cryptography*. Springer, 2019, pp. 206–226.
- [16] D. Ghinea, F. Kaczmarczyk, J. Pullman, J. Cretin, R. Misoczki, S. Kölbl, L. Invernizzi, E. Bursztein, and J.-M. Picod, "Hybrid post-quantum signatures in hardware security keys," 2022.
- [17] M. Conti, G. Kumar, P. Nerurkar, R. Saha, and L. Vigneri, "A survey on security challenges and solutions in the iot," *Journal of Network and Computer Applications*, vol. 203, p. 103383, 2022.
- [18] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "Scada vulnerabilities and attacks: A review of the state-of-the-art and open issues," *Computers & security*, vol. 125, p. 103028, 2023.
- [19] F. Lázaro, R. Raulefs, H. Bartz, and T. Jerkovits, "Vdes r-mode: Vulnerability analysis and mitigation concepts," *International Journal of Satellite Communications and Networking*, vol. 41, no. 2, pp. 178–194, 2023.
- [20] Nature, "Keeping secrets in a quantum world," *Nature*, 2023.
- [21] Cybersecurity and I. S. Agency, "Post-quantum cryptography initiative," <https://www.cisa.gov>, CISA, Tech. Rep., 2023.
- [22] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2490–2510, 2020.
- [23] H. W. Lim and N. J. Buselli, "managing risks and opportunities for quantum safe development," 2024.
- [24] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5g-enabled iot: Challenges, opportunities and solutions," *Internet of Things*, p. 100950, 2023.
- [25] M. Georgescu, H. Hazeyama, T. Okuda, Y. Kadobayashi, and S. Yamaguchi, "The stride towards ipv6: A comprehensive threat model for ipv6 transition technologies," in *ICISSP*, 2016, pp. 243–254.
- [26] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja, "Stride to a secure smart grid in a hybrid cloud," in *Computer Security*. Springer, 2017, pp. 77–90.
- [27] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. Di Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys & Tutorials*, 2024.
- [28] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the internet of things: Survey and research directions," *IEEE Communications Surveys & Tutorials*, 2024.
- [29] A. Karakaya and A. Ulu, "A survey on post-quantum based approaches for edge computing security," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 16, no. 1, p. e1644, 2024.

- [30] K. Kaushik and A. Kumar, "Demystifying quantum blockchain for healthcare," *Security and Privacy*, vol. 6, no. 3, p. e284, 2023.
- [31] A. Liu, X.-B. Chen, S. Xu, Z. Wang, Z. Li, L. Xu, Y. Zhang, and Y. Chen, "A secure scheme based on a hybrid of classical-quantum communications protocols for managing classical blockchains," *Entropy*, vol. 25, no. 5, p. 811, 2023.
- [32] H. Khodaieemehr, K. Bagheri, and C. Feng, "Navigating the quantum computing threat landscape for blockchains: A comprehensive survey," *Authorea Preprints*, 2023.
- [33] P. Swathi and B. Dragan, "A survey on quantum-safe blockchain system," in *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, 2022.
- [34] A. R. Faridi, F. Masood, A. H. T. Shamsan, M. Luqman, and M. Y. Salmony, "Blockchain in the quantum world," *arXiv preprint arXiv:2202.00224*, 2022.
- [35] R. Naz and D. A. Kumar, "Surveying quantum-proof blockchain security: The era of exotic signatures," in *Proceedings of the 25th International Conference on Distributed Computing and Networking*, 2024, pp. 412–417.
- [36] Z. Yang, T. Salman, R. Jain, and R. Di Pietro, "Decentralization using quantum blockchain: A theoretical analysis," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–16, 2022.
- [37] A. Kumar, S. Bhatia, K. Kaushik, S. M. Gandhi, S. G. Devi, A. D. J. Diego, and A. Mashat, "Survey of promising technologies for quantum drones and networks," *Ieee Access*, vol. 9, pp. 125 868–125 911, 2021.
- [38] M. Edwards, A. Mashatan, and S. Ghose, "A review of quantum and hybrid quantum/classical blockchain protocols," *Quantum Information Processing*, vol. 19, pp. 1–22, 2020.
- [39] G. Iovane, "Murequa chain: Multiscale relativistic quantum blockchain," *IEEE Access*, vol. 9, pp. 39 827–39 838, 2021.
- [40] R. M. Blank, "Nist special publication (sp) 800-30 revision 1, guide for conducting risk assessments," 2011.
- [41] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions in stride security threat modeling," *Software and Systems Modeling*, pp. 1–18, 2021.
- [42] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-30, Revision 1," <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, U.S. Department of Commerce, Special Publication 800-30, 2012.
- [43] M. Mosca and M. Piani, "2022 quantum threat timeline report," *Global Risk Insitute*, 2022.
- [44] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization," [https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-\(evaluation-criteria\)](https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)), 2024.
- [45] S. Turner and D. Brown, "Use of elliptic curve cryptography (ecc) algorithms in cryptographic message syntax (cms)," Tech. Rep., 2010.
- [46] D. Gillmor, "Negotiated finite field diffie-hellman ephemeral parameters for transport layer security (tls)," Tech. Rep., 2016.
- [47] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, "Pkcs# 1: Rsa cryptography specifications version 2.2," Tech. Rep., 2016.
- [48] J. Schaad, "Use of the advanced encryption standard (aes) encryption algorithm in cryptographic message syntax (cms)," Tech. Rep., 2003.
- [49] D. Eastlake 3rd and T. Hansen, "Us secure hash algorithms (sha and sha-based hmac and hkdf)," Tech. Rep., 2011.
- [50] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: a cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.
- [51] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238–268, 2018.
- [52] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, "Falcon: Fast-fourier lattice-based compact signatures over ntru," *Submission to the NIST's post-quantum cryptography standardization process*, vol. 36, no. 5, 2018.
- [53] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier *et al.*, "Classic mceliece: conservative code-based cryptography," *NIST submissions*, 2017.
- [54] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and I. Bourges, "Hamming quasi-cyclic (hq)," *NIST PQC Round*, vol. 2, pp. 4–13, 2018.
- [55] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Güneysu, C. A. Melchor *et al.*, "Bike: bit flipping key encapsulation," 2017.
- [56] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The sphincs+ signature framework," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2129–2146.
- [57] D. Jao and L. D. Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *International Workshop on Post-Quantum Cryptography*. Springer, 2011, pp. 19–34.
- [58] National Institute of Standards and Technology (NIST). (2022) NIST Post-Quantum Cryptographic Candidates to Be Standardized: Round 4. [Online]. Available: <https://csrc.nist.gov/News/2022/pqc-candidate-s-to-be-standardized-and-round-4>
- [59] N. I. of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard," U.S. Department of Commerce, Federal Information Processing Standards (FIPS) 203, 2023. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf>
- [60] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Digital Signature Standard," U.S. Department of Commerce, Federal Information Processing Standards (FIPS) FIPS 204, 2023. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf>
- [61] National Institute of Standards and Technology, "Secure hash standard (shs)," <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.ipd.pdf>, U.S. Department of Commerce, Federal Information Processing Standards (FIPS) 205, 2002.
- [62] N. I. of Standards and Technology, "Post-quantum cryptography fips approved," August 2024. [Online]. Available: <https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved>
- [63] P. Ravi, D. B. Roy, S. Bhasin, A. Chattopadhyay, and D. Mukhopadhyay, "Number "not used" once-practical fault attack on pqm4 implementations of nist candidates," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2019, pp. 232–250.
- [64] T. Oder, T. Schneider, T. Pöppelmann, and T. Güneysu, "Practical cca2-secure and masked ring-lwe implementation," *Cryptology ePrint Archive*, 2016.
- [65] P. Ravi, S. Bhasin, S. S. Roy, and A. Chattopadhyay, "Drop by drop you break the rock-exploiting generic vulnerabilities in lattice-based pke/kems using em-based physical attacks," *Cryptology ePrint Archive*, 2020.
- [66] M. Hamburg, J. Hermelink, R. Primas, S. Samardjiska, T. Schamberger, S. Streit, E. Strieder, and C. van Vredendaal, "Chosen ciphertext k-trace attacks on masked cca2 secure kyber," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 88–113, 2021.
- [67] P. Pessl and R. Primas, "More practical single-trace attacks on the number theoretic transform," in *International Conference on Cryptology and Information Security in Latin America*. Springer, 2019, pp. 130–149.
- [68] T. Kamucheka, M. Fahr, T. Teague, A. Nelson, D. Andrews, and M. Huang, "Power-based side channel attack analysis on pqc algorithms," *Cryptology ePrint Archive*, 2021.
- [69] E. Dubrova, K. Ngo, and J. Gärtner, "Breaking a fifth-order masked implementation of crystals-kyber by copy-paste," *Cryptology ePrint Archive*, 2022.
- [70] P. Ravi, S. S. Roy, A. Chattopadhyay, and S. Bhasin, "Generic side-channel attacks on cca-secure lattice-based pke and kems," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2020, no. 3, pp. 307–335, 2020.
- [71] Z. Xu, O. Pemberton, S. S. Roy, D. Oswald, W. Yao, and Z. Zheng, "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: the case study of kyber," *IEEE Transactions on Computers*, vol. 71, no. 9, pp. 2163–2176, 2021.
- [72] P. Ravi, S. Bhasin, S. S. Roy, and A. Chattopadhyay, "On exploiting message leakage in (few) nist pqc candidates for practical message recovery attacks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 684–699, 2021.
- [73] M. R. Albrecht, A. Deo, and K. G. Paterson, "Cold boot attacks on ring and module lwe keys under the ntt," *Cryptology ePrint Archive*, 2018.
- [74] L. G. Bruinderink and P. Pessl, "Differential fault attacks on deterministic lattice signatures," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 21–43, 2018.
- [75] V. Migliore, B. Gérard, M. Tibouchi, and P.-A. Fouque, "Masking dilithium," in *International Conference on Applied Cryptography and Network Security*. Springer, 2019, pp. 344–362.

- [76] S. Marzougui, V. Ulitzsch, M. Tibouchi, and J.-P. Seifert, "Profiling side-channel attacks on dilithium: A small bit-fiddling leak breaks it all," *Cryptology ePrint Archive*, 2022.
- [77] P. Ravi, M. P. Jhanwar, J. Howe, A. Chattopadhyay, and S. Bhasin, "Exploiting determinism in lattice-based signatures: practical fault attacks on pqm4 implementations of nist candidates," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, pp. 427–440.
- [78] R. Singh, S. Islam, B. Sunar, and P. Schaumont, "An end-to-end analysis of emfi on bit-sliced post-quantum implementations," *arXiv preprint arXiv:2204.06153*, 2022.
- [79] A. Berzati, A. C. Viera, M. Chartouni, S. Madec, D. Vergnaud, and D. Vigilant, "A practical template attack on crystals-dilithium," *Cryptology ePrint Archive*, Paper 2023/050, 2023.
- [80] L. Castelnovi, A. Martinelli, and T. Prest, "Grafting trees: a fault attack against the sphincs framework," in *International Conference on Post-Quantum Cryptography*. Springer, 2018, pp. 165–184.
- [81] A. Genêt, M. J. Kannwischer, H. Pelletier, and A. McLaughlan, "Practical fault injection attacks on sphincs," *Cryptology ePrint Archive*, 2018.
- [82] M. J. Kannwischer, A. Genêt, D. Butin, J. Krämer, and J. Buchmann, "Differential power analysis of xmss and sphincs," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2018, pp. 168–188.
- [83] S. McCarthy, J. Howe, N. Smyth, S. Brannigan, and M. O'Neill, "Bearz attack falcon: implementation attacks with countermeasures on the falcon signature scheme," *Cryptology ePrint Archive*, 2019.
- [84] M. Guerreau, A. Martinelli, T. Ricosset, and M. Rossi, "The hidden parallelepiped is back again: Power analysis attacks on falcon," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 141–164, 2022.
- [85] E. Karabulut and A. Aysu, "Falcon down: Breaking falcon post-quantum signature scheme through side-channel attacks," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*. IEEE, 2021, pp. 691–696.
- [86] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *Journal of Banking and Financial Technology*, vol. 3, pp. 1–17, 2019.
- [87] N. I. of Standards and T. (NIST), "Transition to post-quantum cryptography standards," National Institute of Standards and Technology, Interagency Report NIST IR 8547 IPD, November 2024, accessed: 2024-11-19. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8547.ipd>
- [88] K. Petrenko, A. Mashatan, and F. Shirazi, "Assessing the quantum-resistant cryptographic agility of routing and switching it network infrastructure in a large-size financial organization," *Journal of Information Security and Applications*, vol. 46, pp. 151–163, 2019.
- [89] K. H. Shakib, M. Rahman, and M. Islam, "Quantum cyber-attack on blockchain-based vanet," *arXiv preprint arXiv:2304.04411*, 2023.
- [90] N. I. of Standards and T. (NIST), "Post-quantum cryptography," <https://csrc.nist.gov/projects/post-quantum-cryptography>, 2023.
- [91] NIST, "Status report on the third round of the nist post-quantum cryptography standardization process," <https://csrc.nist.gov/publications/detail/nistir/8413/final>, 2022, [Online; accessed 28-07-2022].
- [92] A. Feraudo, N. Romandini, C. Mazzocca, R. Montanari, and P. Bellavista, "Diva: A did-based reputation system for secure transmission in vanets using iota," *Computer Networks*, p. 110332, 2024.
- [93] A. Smahi, H. Li, W. Han, A. A. Fateh, and C. C. Chan, "Vfl-chain: Bulletproofing federated learning in the v2x environments," *Future Generation Computer Systems*, 2024.
- [94] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied sciences*, vol. 9, no. 9, p. 1788, 2019.
- [95] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE access*, vol. 8, pp. 21 091–21 116, 2020.
- [96] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for cryptocurrencies," *Journal of Network and Computer Applications*, vol. 182, p. 103035, 2021.
- [97] Q. R. L. (QRL), "Qrl proof-of-stake algorithm," <https://github.com/theQRL/PoS/blob/master/pos-qrl.pdf>, jul 2017, info@theqrl.org.
- [98] M. Y. Shalaginov and M. Dubrovsky, "Quantum proof of work with parametrized quantum circuits," 2022.
- [99] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-peer Networking and Applications*, vol. 9, pp. 397–413, 2016.
- [100] A. Judmayer, A. Zamyatin, N. Stifter, A. G. Voyiatzis, and E. Weippl, "Merged mining: Curse or cure?" in *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings*. Springer, 2017, pp. 316–333.
- [101] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.
- [102] G. of Canada, "Defending against distributed denial of service (ddos) attacks," 2024. [Online]. Available: <https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110>
- [103] B. Riskhan, H. A. J. Safuan, K. Hussain, A. A. H. Elnour, A. Abdelmaboud, F. Khan, and M. Kundi, "An adaptive distributed denial of service attack prevention technique in a distributed environment," *Sensors*, vol. 23, no. 14, p. 6574, 2023.
- [104] C. Deng and C. Wen, "Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and dos attacks," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 3, pp. 1308–1318, 2020.
- [105] P. Kumari and P. Kaur, "A survey of fault tolerance in cloud computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 10, pp. 1159–1176, 2021.
- [106] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, p. 103232, 2021.
- [107] M. Conklin, B. Elzweig, and L. J. Trautman, "Legal recourse for victims of blockchain and cyber breach attacks," *UC Davis Bus. LJ*, vol. 23, p. 135, 2023.
- [108] U. S. Aditya, R. Singh, P. K. Singh, and A. Kalla, "A survey on blockchain in robotics: Issues, opportunities, challenges and future directions," *Journal of Network and Computer Applications*, vol. 196, p. 103245, 2021.
- [109] G. Fuchsbaauer, M. Orrù, and Y. Seurin, "Aggregate cash systems: A cryptographic investigation of mumblewimble," in *Advances in Cryptology—EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part I 38*. Springer, 2019, pp. 657–689.
- [110] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, 2024.
- [111] H. Xu, Y. Zhou, J. Ming, and M. Lyu, "Layered obfuscation: a taxonomy of software obfuscation techniques for layered security," *Cybersecurity*, vol. 3, pp. 1–18, 2020.
- [112] G. Alagic and B. Fefferman, "On quantum obfuscation," *arXiv preprint arXiv:1602.01771*, 2016.
- [113] C. Liu, H. Guo, M. Xu, S. Wang, D. Yu, J. Yu, and X. Cheng, "Extending on-chain trust to off-chain—trustworthy blockchain data collection using trusted execution environment (tee)," *IEEE Transactions on Computers*, vol. 71, no. 12, pp. 3268–3280, 2022.
- [114] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.
- [115] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE communications surveys & tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.
- [116] Strivemindz, "Quantum threat: How will blockchain adapt to quantum computing?" *LinkedIn*, 2023. [Online]. Available: <https://www.linkedin.com/pulse/quantum-threat-how-blockchain-adapt-computing-strivemindz/>
- [117] D. Malkhi, K. Nayak, and L. Ren, "Flexible byzantine fault tolerance," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 1041–1053.
- [118] W. Zhong, C. Yang, W. Liang, J. Cai, L. Chen, J. Liao, and N. Xiong, "Byzantine fault-tolerant consensus algorithms: a survey," *Electronics*, vol. 12, no. 18, p. 3801, 2023.
- [119] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on applications of game theory in blockchain," *arXiv preprint arXiv:1902.10865*, 2019.
- [120] Z. Noorian and M. Ulieru, "The state of the art in trust and reputation systems: a framework for comparison," *Journal of theoretical and applied electronic commerce research*, vol. 5, no. 2, pp. 97–117, 2010.

- [121] B. Rodrigues, M. Franco, C. Killer, E. J. Scheid, and B. Stiller, "On trust, blockchain, and reputation systems," in *Handbook on blockchain*. Springer, 2022, pp. 299–337.
- [122] T. Weingärtner, D. Batista, S. Köchli, and G. Voutat, "Prototyping a smart contract based public procurement to fight corruption," *Computers*, vol. 10, no. 7, p. 85, 2021.
- [123] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th symposium on operating systems principles*, 2017, pp. 51–68.
- [124] V. Gandotra, F.-É. Racicot, and A. Rahimzadeh, "Cryptocurrency mining," in *Cryptofinance and Mechanisms of Exchange: The Making of Virtual Currency*. Springer, 2020, pp. 51–67.
- [125] R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," *Cryptology ePrint Archive*, 2016.
- [126] C. R. García, S. Rommel, S. Takarabt, J. J. V. Olmos, S. Guilley, P. Nguyen, and I. T. Monroy, "Quantum-resistant transport layer security," *Computer Communications*, vol. 213, pp. 345–358, 2024.
- [127] K. M. Khan, J. Arshad, and M. M. Khan, "Empirical analysis of transaction malleability within blockchain-based e-voting," *Computers & Security*, vol. 100, p. 102081, 2021.
- [128] K. Nicolas, Y. Wang, G. C. Giakos, B. Wei, and H. Shen, "Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach," *IEEE Access*, vol. 9, pp. 3838–3857, 2020.
- [129] N. I. of Standards and Technology, "Nist to standardize encryption algorithms that can resist attack by quantum computers," <https://www.nist.gov>, NIST, Tech. Rep., 2023.
- [130] B. Bünz, J. Campen, and O. Günther, "Improving the privacy, scalability, and ecological impact of blockchains," Ph.D. dissertation, 2018. [Online]. Available: <https://cs.nyu.edu/~bb/papers/thesis.pdf>
- [131] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proceedings of the 2019 international conference on management of data*, 2019, pp. 123–140.
- [132] D. Boneh, J. Boneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Annual international cryptology conference*. Springer, 2018, pp. 757–788.
- [133] S. Chauhan, V. P. Ojha, S. Yarahmadian, and D. Carvalho, "Towards building quantum resistant blockchain," in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. IEEE, 2023, pp. 1–9.
- [134] T. Ramanandran, A. Delignat-Lavaud, C. Fournet, N. Swamy, T. Chajed, N. Kobeissi, and J. Protzenko, "{EverParse}: Verified secure {Zero-Copy} parsers for authenticated message formats," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1465–1482.
- [135] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and mtgox," in *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19*. Springer, 2014, pp. 313–326.
- [136] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6g security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.
- [137] A. Singh, R. M. Parizi, M. Han, A. Dehghantaha, H. Karimipour, and K.-K. R. Choo, "Public blockchains scalability: An examination of sharding and segregated witness," *Blockchain cybersecurity, trust and privacy*, pp. 203–232, 2020.
- [138] P. Ruan, D. Loghin, Q.-T. Ta, M. Zhang, G. Chen, and B. C. Ooi, "A transactional perspective on execute-order-validate blockchains," in *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data*, 2020, pp. 543–557.
- [139] E. Zaghoul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and blockchain: Security and privacy," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 288–10 313, 2020.
- [140] T. Yanagita, S. Chakraborty, K. Sadakane, and S. R. Satti, "Space-efficient data structure for posets with applications," in *18th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.
- [141] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.
- [142] D. Chefrou, "Evolution of network time synchronization towards nanoseconds accuracy: A survey," *Computer Communications*, vol. 191, pp. 26–35, 2022.
- [143] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-based uav path planning for healthcare 4.0: Current challenges and the way ahead," *IEEE Network*, vol. 35, no. 1, pp. 20–29, 2021.
- [144] C. Wu, L. Ke, and Y. Du, "Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain," *Information Sciences*, vol. 548, pp. 438–449, 2021.
- [145] P. Ananth, Z. Hu, and H. Yuen, "On the (im) plausibility of public-key quantum money from collision-resistant hash functions," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2023, pp. 39–72.
- [146] D. Basile, V. Goretta, C. Di Ciccio, and S. Kirrane, "Enhancing blockchain-based processes with decentralized oracles," in *International Conference on Business Process Management*. Springer, 2021, pp. 102–118.
- [147] J. Dong, C. Song, Y. Sun, and T. Zhang, "Daon: A decentralized autonomous oracle network to provide secure data for smart contracts," *IEEE Transactions on Information Forensics and Security*, 2023.
- [148] A. M. Lewis, M. Travagnin *et al.*, "A secure quantum communications infrastructure for europe: Technical background for a policy vision," *Publications Office of the European Union: Luxembourg*, 2022.
- [149] Y. Zhao, X. Kang, T. Li, C.-K. Chu, and H. Wang, "Toward trustworthy defi oracles: past, present, and future," *IEEE Access*, vol. 10, pp. 60 914–60 928, 2022.
- [150] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng, and N. Guizani, "Smart contract vulnerability analysis and security audit," *IEEE Network*, vol. 34, no. 5, pp. 276–282, 2020.
- [151] Y. Chen, C. Xu, J. S. He, and S. Xiao, "A cross language code security audit framework based on normalized representation," *Journal of Quantum Computing*, vol. 4, no. 2, 2022.
- [152] M. Lewis, S. Soudjani, and P. Zuliani, "Formal verification of quantum programs: Theory, tools, and challenges," *ACM Transactions on Quantum Computing*, vol. 5, no. 1, pp. 1–35, 2023.
- [153] C. Chareton, S. Bardin, D. Lee, B. Valiron, R. Vilmart, and Z. Xu, "Formal methods for quantum programs: A survey," *arXiv preprint arXiv:2109.06493*, 2021.
- [154] A. Ghaleb and K. Pattabiraman, "How effective are smart contract analysis tools? evaluating smart contract static analysis tools using bug injection," in *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2020, pp. 415–427.
- [155] R. Fontein, "Comparison of static analysis tooling for smart contracts on the evm," in *28th Twente Student conference on IT*, 2018.
- [156] J. Khor, M. A. Masama, M. Sidorov, W. Leong, and J. Lim, "An improved gas efficient library for securing iot smart contracts against arithmetic vulnerabilities," in *Proceedings of the 2020 9th International Conference on Software and Computer Applications*, 2020, pp. 326–330.
- [157] K. Al Harthy and A. Agarwal, "Defi cybersecurity technical and non-technical risks," in *Decentralized Finance: The Impact of Blockchain-Based Financial Innovations on Entrepreneurship*. Springer, 2024, pp. 133–149.
- [158] P. Tolmach, "Securing smart contracts with formal verification and automated program repair," 2023.
- [159] K. Hameed, M. Barika, S. Garg, M. B. Amin, and B. Kang, "A taxonomy study on securing blockchain-based industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues," *Journal of Industrial Information Integration*, vol. 26, p. 100312, 2022.
- [160] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer Networks*, vol. 184, p. 107679, 2021.
- [161] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, E. Lee, and I. Ashraf, "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges," *IEEE Access*, vol. 10, pp. 96 538–96 555, 2022.
- [162] W. Zou, D. Lo, P. S. Kochhar, X.-B. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE transactions on software engineering*, vol. 47, no. 10, pp. 2084–2106, 2019.
- [163] M. Scherer, "Performance and scalability of blockchain networks and smart contracts," 2017.
- [164] P. Das, L. Eckey, T. Frassetto, D. Gens, K. Hostáková, P. Jauernig, S. Faust, and A.-R. Sadeghi, "{FastKitten}: Practical smart contracts on bitcoin," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 801–818.
- [165] Y. Wang, K. Li, Y. Tang, J. Chen, Q. Zhang, X. Luo, and T. Chen, "Towards saving blockchain fees via secure and cost-effective batching of smart-contract invocations," *IEEE Transactions on Software Engineering*, vol. 49, no. 4, pp. 2980–2995, 2023.

- [166] N. K. Parida, C. Jatoth, V. D. Reddy, M. M. Hussain, and J. Faizi, "Post-quantum distributed ledger technology: a systematic survey," *Scientific Reports*, vol. 13, no. 1, p. 20729, 2023.
- [167] X. Ren, M. Xu, D. Niyato, J. Kang, Z. Xiong, C. Qiu, and X. Wang, "Building resilient web 3.0 with quantum information technologies and blockchain: An ambilateral view," *arXiv preprint arXiv:2303.13050*, 2023.
- [168] Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols."
- [169] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, 2020.
- [170] M. R. Hasan, A. Alazab, S. B. Joy, M. N. Uddin, M. A. Uddin, A. Khraisat, I. Gondal, W. F. Urmi, and M. A. Talukder, "Smart contract-based access control framework for internet of things devices," *Computers*, vol. 12, no. 11, p. 240, 2023.
- [171] B. Bellaj, A. Ouaddah, N. Crespi, A. Mezrioui, and E. Bertin, "A transpilation-based approach to writing secure access control smart contracts," in *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2023, pp. 1–7.
- [172] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan, and A. Jaradat, "Internet of things and blockchain integration: security, privacy, technical, and design challenges," *Future Internet*, vol. 14, no. 7, p. 216, 2022.
- [173] C. Joshi, C. Bhole, and N. Vaswani, "A scrutiny review of cps 4.0-based blockchain with quantum resistance," in *Advancements in quantum blockchain with real-time applications*. IGI Global, 2022, pp. 131–157.
- [174] H. Zhang, L.-H. Merino, Z. Qu, M. Bastankhah, V. Estrada-Galiñanes, and B. Ford, "F3b: A low-overhead blockchain architecture with per-transaction front-running protection," *arXiv preprint arXiv:2205.08529*, 2022.
- [175] J. Burdges and L. De Feo, "Delay encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2021, pp. 302–326.
- [176] P. Thanalakshmi, A. Rishikesh, J. Marion Marceline, G. P. Joshi, and W. Cho, "A quantum-resistant blockchain system: A comparative analysis," *Mathematics*, vol. 11, no. 18, p. 3947, 2023.
- [177] D. R. Sahu, H. Tiwari, D. S. Tomar, and R. Pateriya, "Quantum-resistant cryptography to prevent from phishing attack exploiting blockchain wallet," in *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications*. Springer, 2024, pp. 171–191.
- [178] S. Goldfeder, J. Bonneau, J. Kroll, and E. Felten, "Securing bitcoin wallets via threshold signatures," 2014.
- [179] J.-P. Aumasson and O. Shlomovits, "Attacking threshold wallets," *Cryptology ePrint Archive*, 2020.
- [180] V. Mannalatha, S. Mishra, and A. Pathak, "A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness," *Quantum Information Processing*, vol. 22, no. 12, p. 439, 2023.
- [181] M. M. Jacak, P. Józwiak, J. Niemczuk, and J. E. Jacak, "Quantum generators of random numbers," *Scientific Reports*, vol. 11, no. 1, p. 16108, 2021.
- [182] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, "Device-independent quantum random-number generation," *Nature*, vol. 562, no. 7728, pp. 548–551, 2018.
- [183] M. Berta, O. Fawzi, and V. B. Scholz, "Quantum-proof randomness extractors via operator space theory," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2480–2503, 2017.
- [184] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," *Physical review letters*, vol. 118, no. 6, p. 060503, 2017.
- [185] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 87, no. 6, p. 062327, 2013.
- [186] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE transactions on dependable and secure computing*, vol. 19, no. 3, pp. 1885–1899, 2020.
- [187] M. Dürmuth, M. Golla, P. Markert, A. May, and L. Schlieper, "Towards quantum large-scale password guessing on real-world distributions," in *International Conference on Cryptology and Network Security*. Springer, 2021, pp. 412–431.
- [188] A. Biryukov, D. Dinu, D. Khovratovich, and S. Josefsson, "Rfc 9106: Argon2 memory-hard function for password hashing and proof-of-work applications," 2021.
- [189] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," 2024. [Online]. Available: <https://arxiv.org/abs/2404.10659>
- [190] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perner, and D. Smith-Tone, "Report on post-quantum cryptography," US Department of Commerce, National Institute of Standards and Technology, 2016.
- [191] N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, "Strengthening the blockchain-based internet of value with trust," in *2018 IEEE international conference on communications (ICC)*. IEEE, 2018, pp. 1–7.
- [192] Microsoft, "Post-quantum tls," <https://www.microsoft.com/en-us/research/project/post-quantum-tls>, accessed: 2023-10-05.
- [193] D. A. Bard, J. J. Kearney, and C. A. Perez-Delgado, "Quantum advantage on proof of work," *Array*, vol. 15, p. 100225, 2022.
- [194] K. Schärer and M. Comuzzi, "The quantum threat to blockchain: summary and timeline analysis," *Quantum Machine Intelligence*, vol. 5, no. 1, p. 19, 2023.
- [195] H. Shekhawat and D. S. Gupta, "Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure," *Pervasive and Mobile Computing*, vol. 100, p. 101919, 2024.
- [196] J. Gomes, S. Khan, and D. Svetinovic, "Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience," *IEEE Access*, 2023.
- [197] N. K. Sinai and H. P. In, "Performance evaluation of a quantum-resistant blockchain: a comparative study with secp256k1 and schnorr," *Quantum Information Processing*, vol. 23, no. 3, p. 99, 2024.
- [198] J. Chen, W. Gan, M. Hu, and C.-M. Chen, "On the construction of a post-quantum blockchain for smart city," *Journal of information security and applications*, vol. 58, p. 102780, 2021.
- [199] S. Akhail and V. Kumar, "Quantum resilience and distributed trust: The promise of blockchain and quantum computing in defense," in *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications*. Springer, 2024, pp. 125–153.
- [200] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. M. Sam, and G. A. N. Samy, "Effect of quantum computing on blockchain-based electronic health record systems," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*. IEEE, 2022, pp. 179–184.
- [201] S. Siddiqui, S. Hameed, S. A. Shah, A. K. Khan, and A. Aneiba, "Smart contract-based security architecture for collaborative services in municipal smart cities," *Journal of Systems Architecture*, vol. 135, p. 102802, 2023.
- [202] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.
- [203] Y. Kethepalli, R. Joseph, S. R. Vajjala, J. Vemula, and N. S. Naik, "Reinforcing security and usability of crypto-wallet with post-quantum cryptography and zero-knowledge proof," *arXiv preprint arXiv:2308.07309*, 2023.
- [204] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: research and applications*, vol. 3, no. 2, p. 100067, 2022.
- [205] Z. A. Khan and A. S. Namin, "Ethereum smart contracts: Vulnerabilities and their classifications," in *2020 IEEE International Conference on Big Data (Big Data)*. IEEE, 2020, pp. 1–10.
- [206] S. Mohanty, S. Sharma, P. K. Pattnaik, and A. Hol, "A comprehensive review on cyber security and online banking security frameworks," *Risk Detection and Cyber Security for the Success of Contemporary Computing*, pp. 1–22, 2023.
- [207] F. A. Fahim *et al.*, "Comparative analysis between security models for enhancement of network security in 6g technology," Ph.D. dissertation, Department of Electronic and Telecommunication Engineering, 2022.
- [208] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevičius, A.-A. O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021.
- [209] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.
- [210] V. Vasani, K. Prateek, R. Amin, S. Maity, and A. D. Dwivedi, "Embracing the quantum frontier: Investigating quantum communication,

- cryptography, applications and future directions,” *Journal of Industrial Information Integration*, p. 100594, 2024.
- [211] A. H. Karbasi and S. Shahpasand, “A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks,” *Peer-to-peer networking and applications*, vol. 13, pp. 1423–1441, 2020.
- [212] C. Mangla, S. Rani, N. M. F. Qureshi, and A. Singh, “Mitigating 5g security challenges for next-gen industry using quantum computing,” *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 6, p. 101334, 2023.
- [213] B. Putz, F. Menges, and G. Pernul, “A secure and auditable logging infrastructure based on a permissioned blockchain,” *Computers & Security*, vol. 87, p. 101602, 2019.
- [214] Y. Li, W. Susilo, G. Yang, Y. Yu, X. Du, D. Liu, and N. Guizani, “Toward privacy and regulation in blockchain-based cryptocurrencies,” *IEEE Network*, vol. 33, no. 5, pp. 111–117, 2019.
- [215] I. Kong, M. Janssen, and N. Bharosa, “Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions,” *Government Information Quarterly*, vol. 41, no. 1, p. 101884, 2024.
- [216] K. DeRose, “Establishing the legal framework to regulate quantum computing technology,” *Cath. UJL & Tech*, vol. 31, p. 145, 2022.
- [217] B. S. White, C. G. King, and J. Holladay, “Blockchain security risk assessment and the auditor,” *Journal of Corporate Accounting & Finance*, vol. 31, no. 2, pp. 47–53, 2020.
- [218] S. B. Kahyaoglu, “An evaluation of accounting and auditing framework within the quantum perspective,” *Southern African Journal of Accountability and Auditing Research*, vol. 25, no. 1, pp. 1–5, 2023.
- [219] A.-T. Ciulei, M.-C. Crețu, and E. Simion, “Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective,” *Cryptology ePrint Archive*, Paper 2022/026, 2022, <https://eprint.iacr.org/2022/026>. [Online]. Available: <https://eprint.iacr.org/2022/026>
- [220] W. G. Johnson, “Governance tools for the second quantum revolution,” *Jurimetrics*, vol. 59, no. 4, pp. 487–522, 2019.
- [221] V. Malik, R. Mittal, D. Mavaluru, B. R. Narapureddy, S. Goyal, R. J. Martin, K. Srinivasan, and A. Mittal, “Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks,” *IEEE Access*, 2023.
- [222] M. Aurangzeb, Y. Wang, S. Iqbal, A. Naveed, Z. Ahmed, M. Alenezi, and M. Shouran, “Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage,” *Energy Reports*, vol. 11, pp. 2493–2515, 2024.
- [223] Y. Ma, S. Goyal, A. S. Rajawat, P. Bedi, and S. Yasmeen, “Blockchain-based human intelligent systems for smart city safety,” *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 2, p. e4939, 2024.
- [224] M. Kassen, “Blockchain and digital governance: Decentralization of decision making policy,” *Review of Policy Research*, 2023.
- [225] K. Ikeda, “Chapter seven - security and privacy of blockchain and quantum computation,” in *Blockchain Technology: Platforms, Tools and Use Cases*, ser. Advances in Computers, P. Raj and G. C. Deka, Eds. Elsevier, 2018, vol. 111, pp. 199–228. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0065245818300160>
- [226] P. Radanliev, “Cyber diplomacy: defining the opportunities for cybersecurity and risks from artificial intelligence, iot, blockchains, and quantum computing,” *Journal of Cyber Security Technology*, pp. 1–51, 2024.
- [227] K. R. Ku-Mahamud, M. Omar, N. A. A. Bakar, and I. D. Muraina, “Awareness, trust, and adoption of blockchain technology and cryptocurrency among blockchain communities in malaysia,” *International Journal on Advanced Science, Engineering & Information Technology*, vol. 9, no. 4, pp. 1217–1222, 2019.
- [228] A. Mashatan and D. Heintzman, “The complex path to quantum resistance,” *Communications of the ACM*, vol. 64, no. 9, pp. 46–53, 2021.
- [229] “Quantum technologies at aws,” <https://aws.amazon.com/products/quantum/>, 2023, accessed: 2023-11-27.
- [230] S. Banaeian Far and M. Rajabzadeh Asaar, “A blockchain-based quantum-secure reporting protocol,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2992–3011, 2021.
- [231] O. Q. Safe, “Oqs algorithm performance visualizations,” Open Quantum Safe Project. [Online]. Available: <https://openquantumsafe.org/benchmarking/>
- [232] A. Seira, J. Allen, C. Watsky, and R. Alley, “Governance of permissionless blockchain networks,” 2024.
- [233] G. Segal, Y. Martsiano, A. Markinson, A. Mayer, A. Halperin, and E. Zimlichman, “A blockchain-based computerized network infrastructure for the transparent, immutable calculation and dissemination of quantitative, measurable parameters of academic and medical research publications,” *Digital Health*, vol. 9, p. 20552076231194851, 2023.
- [234] D. Marchsreiter, “Towards quantum-safe blockchain: Exploration of pqc and public-key recovery on embedded systems,” *Cryptology ePrint Archive*, 2024.
- [235] H. Chen, M. Pendleton, L. Njilla, and S. Xu, “A survey on ethereum systems security: Vulnerabilities, attacks, and defenses,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.
- [236] P. Prajapati, B. Bhatt, G. Zalavadiya, M. Ajwalia, and P. Shah, “A review on recent intrusion detection systems and intrusion prevention systems in iot,” in *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2021, pp. 588–593.
- [237] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, “A survey on multi-factor authentication for online banking in the wild,” *Computers & Security*, vol. 95, p. 101745, 2020.
- [238] A. K. Bishwas and M. Sen, “Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat,” *arXiv preprint arXiv:2411.09995*, 2024.
- [239] Z. Chen, X. Sun, X. Shan, and J. Zhang, “Decentralized mining pool games in blockchain,” in *2020 IEEE International Conference on Knowledge Graph (ICKG)*, 2020, pp. 426–432.
- [240] R. Tyler, “Battle begins to stop quantum computers smashing cyber defences,” *The Times*, 2023. [Online]. Available: <https://www.thetimes.co.uk/article/battle-begins-to-stop-quantum-computers-smashing-cyber-defences-rzmlwqw7f>
- [241] G. Zhang, F. Pan, Y. Mao, S. Tjjanic, M. Dang’ana, S. Motepalli, S. Zhang, and H.-A. Jacobsen, “Reaching consensus in the byzantine empire: A comprehensive review of bft consensus algorithms,” *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–41, 2024.
- [242] Cybersecurity, I. S. Agency, N. S. Agency, N. I. of Standards, and Technology, “Quantum-readiness: Migration to post-quantum cryptography,” August 2023. [Online]. Available: [https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf)
- [243] W. Newhouse, M. Souppaya, W. Barker, C. Brown, P. Kampanakis, J. Goodman, J. Prat, R. Larrieu, J. Gray, M. Ounsworth, C. Viana, H. L. V. Gong, K. Kwiatkowski, A. Hu, R. Burns, C. Paquin, J. Gilbert, G. Scinta, E. Kim, and V. Krummel, “Migration to post-quantum cryptography: Quantum readiness: Testing draft standards,” National Institute of Standards and Technology, Special Publication 1800-38C, December 2023, preliminary Draft. [Online]. Available: <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf>
- [244] P. Tsankov, A. Dan, D. Drachler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, “Securify: Practical security analysis of smart contracts,” in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 2018, pp. 67–82.
- [245] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, “A survey of smart contract formal specification and verification,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, pp. 1–38, 2021.
- [246] E. Foundation, “Formal verification of smart contracts,” <https://ethereum.org/en/developers/docs/smart-contracts/formal-verification/>.
- [247] K. Schierbauer, “Performance measurement of quantum-resistant algorithms in blockchain networks,” Ph.D. dissertation, University of Applied Sciences, 2024.
- [248] E. Dekker and P. Spaans, “Performance comparison of vpn implementations wireguard, strongswan, and openvpn in a 1 gbit/s environment.”
- [249] U. G. A. Office, “Blockchain in finance: Legislative and regulatory actions are needed to ensure comprehensive oversight of crypto assets,” Jun. 2023. [Online]. Available: <https://www.gao.gov/assets/gao-23-105346.pdf>
- [250] N. Alnahawi, A. Wiesmaier, T. Grasmeyer, J. Geißler, A. Zeier, P. Bauspieß, and A. Heinemann, “On the state of post-quantum cryptography migration,” 2021.
- [251] M. De Stefano, F. Pecorelli, D. Di Nucci, F. Palomba, and A. De Lucia, “Software engineering for quantum programming: How far are we?” *Journal of Systems and Software*, vol. 190, p. 111326, 2022.
- [252] F. D., “Terminology for Post-Quantum Traditional Hybrid Schemes,” <https://www.ietf.org/archive/id/draft-ietf-pquip-pqt-hybrid-terminology-04.html>, Internet Engineering Task Force, Internet-Draft draft-driscoll-pqt-hybrid-terminology-02, 2024, work in Progress.
- [253] M. Campagna and A. Petcher, “Security of hybrid key encapsulation,” *Cryptology ePrint Archive*, 2020.



- [254] N. Alnahawi, N. Schmitt, A. Wiesmaier, A. Heinemann, and T. Grasmeyer, "On the state of crypto-agility," *Cryptology ePrint Archive*, 2023.
- [255] E. Barker, L. Chen, S. Keller, A. Roginsky, A. Vassilev, and R. Davis, "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography," National Institute of Standards and Technology, Tech. Rep., 2018.
- [256] A. A. Giron, R. Custódio, and F. Rodríguez-Henríquez, "Post-quantum hybrid key exchange: a systematic mapping study," *Journal of Cryptographic Engineering*, pp. 1–18, 2022.
- [257] W. Whyte, Z. Zhang, S. Fluhrer, and O. Garcia-Morchon, "Quantum-safe hybrid (qsh) key exchange for transport layer security (tls) version 1.3," *IETF Draft*, 2017.
- [258] F. Kiefer and K. Kwiatkowski, "Hybrid ecdhe-sidh key exchange for tls," 2018.
- [259] J. M. Schanck, W. Whyte, and Z. Zhang, "Circuit-extension handshakes for tor achieving forward secrecy in a quantum world," *Cryptology ePrint Archive*, 2015.
- [260] D. Steblia, S. Fluhrer, and S. Gueron, "Hybrid key exchange in tls 1.3," *Internet Engineering Task Force, Internet-Draft draft-ietf-tls-hybrid-design-01*, 2020.
- [261] B. Dowling, T. B. Hansen, and K. G. Paterson, "Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange," in *International Conference on Post-Quantum Cryptography*. Springer, 2020, pp. 483–502.
- [262] F. Giacon, F. Heuer, and B. Poettering, "Kem combiners," in *IACR International Workshop on Public Key Cryptography*. Springer, 2018, pp. 190–218.
- [263] S. Ghosh and A. Kate, "Post-quantum forward-secure onion routing," in *International Conference on Applied Cryptography and Network Security*. Springer, 2015, pp. 263–286.
- [264] J. Brendel, M. Fischlin, and F. Günther, "Breakdown resilience of key exchange protocols: Newhope, tls 1.3, and hybrids," in *European Symposium on Research in Computer Security*. Springer, 2019, pp. 521–541.
- [265] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *International Workshop on Post-Quantum Cryptography*. Springer, 2017, pp. 384–405.
- [266] J. Zhang, T. Xie, Y. Zhang, and D. Song, "Transparent polynomial delegation and its applications to zero knowledge proof," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, May 2020, pp. 859–876.
- [267] S. Ames, C. Hazay, Y. Ishai, and M. Venkatasubramanian, "Ligero," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. New York, NY, USA: Association for Computing Machinery, October 2017, pp. 2087–2104.
- [268] E. Ben-Sasson, A. Chiesa, M. Riabzev, N. Spooner, M. Virza, and N. P. Ward, "Aurora: Transparent succinct arguments for r1cs," in *Advances in Cryptology – EUROCRYPT 2019*, ser. Lecture Notes in Computer Science, Y. Ishai and V. Rijmen, Eds. Springer International Publishing, 2019, vol. 11476, pp. 103–128.
- [269] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [270] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.
- [271] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings 8*. Springer, 2015, pp. 163–180.
- [272] M. L. F. Jumaili and S. M. Karim, "Comparison of tow two cryptocurrencies: Bitcoin and litecoin," in *Journal of Physics: Conference Series*, vol. 1963, no. 1. IOP Publishing, 2021, p. 012143.
- [273] D. Hopwood, S. Bowe, T. Hornby, N. Wilcox *et al.*, "Zcash protocol specification," *GitHub: San Francisco, CA, USA*, vol. 4, no. 220, p. 32, 2016.
- [274] "The Quantum Resistant Ledger (QRL)," <https://www.theqrl.org/>.
- [275] Komodo Platform, "Dilithium: A Quantum-Secure Blockchain Solution," <https://komodoplatfrom.com/en/blog/dilithium-quantum-secure-blockchain/>.
- [276] "Nexus: Connecting a decentralized world," <https://nexus.io>.
- [277] "Tidecoin: Quantum Resistant Cryptocurrency," <https://tidecoin.co/>.
- [278] "Abelian: Quantum Resistant Blockchain," <https://www.abelian.info/home/>.
- [279] "Quantum Resistance Overview: LACNet," <https://lacnet.lacchain.net/quantum-resistance-overview/>.
- [280] "QANplatform: Quantum-Resistant Hybrid Blockchain," <https://www.qanplatform.com/en>.
- [281] "HCash: Quantum-Resistant Cryptocurrency," <https://h.cash/>.
- [282] "IOTA Foundation," <https://www.iota.org/>.