Designing Quantum-Resilient Blockchain Frameworks: Enhancing Transactional Security with Quantum Algorithms in Decentralized Ledgers

Dr. Meenal R Kale[1], Prof. Ts. Dr. Yousef A.Baker El-Ebiary[2], L.Sathiya[3],
Dr Vijay Kumar Burugari[4], Erkiniy Yulduz[5], Elangovan Muniyandy[6], Rakan Alanazi[7*]
Asst. Prof, Department of Humanities, Yeshwantrao Chavan College of Engineering, Hingna, Nagpur, India[1]
Faculty of Informatics and Computing, UniSZA University, Malaysia[2]
Assistant Professor, Department of CSE, Panimalar Engineering College, Chennai, India[3]
Associate Professor, Dept of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India[4]
Automatic Control and Computer Engineering Department, Turin Polytechnic University in Tashkent, Tashkent, Uzbekistan[5]
Department of Biosciences-Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences, Chennai, India[6]
Applied Science Research Center, Applied Science Private University, Amman, Jordan[6]
Department of Information Technology-Faculty of Computing and Information Technology,
Northern Border University, Rafha, Saudi Arabia[7]

***Abstract*—Quantum computing is progressing at a fast rate and there is a real threat that classical cryptographic methods can be compromised and therefore impact the security of blockchain networks. All of the ways used to secure blockchain like Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm 256-bit (SHA256) are the characteristic of the traditional cryptographic techniques vulnerable to attack by quantum algorithms: Shor's and Grover's algorithms: can efficiently break asymmetric encryption and speed up brute force attacks. Because of this vulnerability, there exists a need to develop an advance quantum resilient blockchain framework to protect the decentralized ledgers from the future threats of the quantum. This research proposes Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) as a formidable architectural integration, to fortify security of blockchain. Classical encryption is replaced with PQC, QKD with secure key exchange by detecting eavesdropping, and QRNG with improving cryptographic randomness to remove the predictable key vulnerability. Only with a small loss of transaction efficiency, we increase transaction encryption accuracy, key exchange security, and resistance to quantum attacks. In this quantum enhanced blockchain design, the idea is to preserve the decentralization, transparency and security and at the same time overcome the future quantum threat. By going through rigorous analysis and comparative evaluation, we demonstrate that the approach saves blockchain networks from the emerging quantum risks to make sure that the decentralized finance, smart contracts and cross chain transactions.**

***Keywords*—Quantum resilience; blockchain security; Quantum Key Distribution (QKD); Post-Quantum Cryptography (PQC); Quantum Random Number Generation (QRNG); decentralized ledger**

I. INTRODUCTION

Existing blockchain security measures, which mostly rely on traditional cryptographic methods like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), are under grave danger due to the rapid advancement of quantum technology [1]. Because factoring massive amounts and the separate logarithm procedure thwart effective assaults made possible by traditional computation, conventional cryptography using public keys is still safe [2]. The ability of quantum computers to run Shor's algorithm transforms these classical cryptographic methods into obsolete systems which fail to protect blockchain networks. The brute-force attack acceleration ability of Grover's algorithm causes current cryptographic hash functions deployed on blockchain networks to operate less effectively [3].

Researchers are investigating quantum-resistant cryptographic techniques to guarantee blockchain networks' long-term security and resilience. Security experts designed quantum-proof encryption mechanisms which achieve both high resistance against quantum attacks and efficient computing capacity [4]. Blockchains benefit from quantum-enhanced security measures through advanced solutions comprised of both Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG). These methods use quantum mechanics principles to boost blockchain defense systems [5]. Blockchain architectures show little readiness to face the upcoming post-quantum time period. The research analyzes quantum-based technologies to strengthen blockchain infrastructure thus protecting its core decentralized structure and transaction security while preserving sustainability alongside expanded quantum processing capabilities.

Recent blockchain safety techniques hinge on cryptographic constructs which quantum computers without difficulty ruin thru [6]. Quantum computers goal the important thing cryptographic

primitives of PoW and PoS by using breaking their safeguards via Shor's and Grover's algorithms. Both consensus models rely upon cryptographic hash functions similarly to public-key cryptographic primitives [7], [8]. Cryptography flaws from quantum computing attacks can bring about predominant security incidents by using allowing transaction tampering together with double-spending and signature-disruption incidents [9]. Data protection relying on Post-Quantum Cryptography (PQC) techniques such as hash-based and lattice-based encryption face serious challenges. which include additional computational charges and scalability issues [10]. Current efforts to integrate those cryptographic processes into blockchain networks face initial demanding situations because they want enormous processing power that diminishes operational performance and slows transaction processing pace. Current momentum closer to quantum-resistant cryptocurrency interactions confronts developers and industries with a big barrier to move operational obstacles between quantum cryptography and conventional blockchain systems [11]. Existing blockchain systems fail to mix quantum cryptography properly with consensus mechanisms so they have significant weaknesses regarding decentralized security performance alongside scalability and operational speed. Blockchain networks need essential traits to combat modern quantum-primarily based protection vulnerabilities for their lengthy-time period operational sustainability.

The studies develop a quantum-secure blockchain gadget thru post-quantum cryptographic protocol implementation along quantum protection optimization elements. The studies develop cryptographic techniques which guard blockchain transactions from quantum threats however additionally maintains green consensus mechanisms and scalability overall performance. Through the implementation of quantum-resistant encryption alongside quantum key distribution and quantum-safe consensus protocols this study strives to build a secure decentralized blockchain architecture. Blockchain network developers pursue a goal of longevity so these platforms remain functional and secure for the quantum computing era ahead.

The approach described in this research completely addresses blockchain network vulnerability to quantum threats by integrating quantum-secure encryption methods with security technology advancements. The work advances blockchain security through enhanced data preservation and decentralized systems which establish protected relationships in diverse application contexts. The research provides concrete methods to build blockchain systems with quantum safety applications across financial sectors and supply chain activities and digital assets management services.

- Innovative Quantum-Resilient Encryption Mechanism that introduces PQC to overcome classical encryption weakness by employing lattice based vs. RSA & ECC cryptographic algorithms for security against quantum attacks in the foreseeable future.
- Quantum Key Exchange undertakes QKD to patch up vulnerabilities of conventional key exchange protocols and gives us a provably secure way to avoid eavesdropping via and MITM attacks.
- QRNG enhancements increases entropy scores and the security of the blockchain from brute force attacks and the predictability vulnerabilities.
- Balancing Security with Performance Using Minimal Overhead achieves high transaction throughput (50 TPS), reduced encryption time (2.8 ms), improved security accuracy (99.9%), thereby, enabling smooth blockchain operation with quantum threat.

The proposed study is organized into multiple sections. The introduction in Section I provides information on the background analysis while also establishing the problem statement plus research value. A review of studies focuses on assessing blockchain security risks which quantum threats poses are shown in Section II and III. The research details implementation steps for quantum-resistant cryptographic systems and security components is shown in Section IV. The framework's execution performance is explored in the Section V before the final summary in Section VI and Section VII.

II. Literature Review

Sahu and Mazumdar, [12] investigates quantum computing's deep effects on cryptographical practices by analyzing the vulnerabilities that can breach traditional methods including RSA and ECC along with introducing quantum-resistant cryptographic systems. An introduction to quantum mechanics fundamental concepts including superposition together with entanglement establishes the framework for quantum computing and cryptography. Research evaluates Quantum encryption algorithms by studying the benefits of QKD protocols and PQC procedures which show promise for quantum age communication security. The study highlights the importance of developing strong, quantum-proof cryptography technology as a matter of utmost urgency which offers protection against imminent quantum technology threats targeting sensitive data.

BCNs represent a groundbreaking system that builds trust for untrusted environments. Because of its complex nature service LCM of network components benefits from BCN implementation which provides transparent secure network operations. Quantum attacks represent a security threat to BCNs. Future quantum computers will create security vulnerabilities in modern blockchain systems built with Public Key Infrastructure (PKI) cryptographic foundations. ZEYDAN et al., [13] This research investigates operational approaches for managing network services across multiple administrative domains. The proposition combines BCNs with PQC mechanisms to monitor network service instantiation stages while guaranteeing enhanced security protection. Our analysis utilizing N-th degree Truncated polynomial Ring Units as an NTRU example illustrates how Quorum achieves better average time-to-write performance than Ethereum and Hyperledger BCNs. We analyze evaluation results about PQC algorithm and BCN coexistence as well as their potential future applications for network service orchestration across multiple administrative domains at the paper's conclusion.

Alyami et al. [14] explored the nature and concept of quantum computing in respect to software security, highlighting the imminence of powerful quantum computers as a threat to current cryptosystems. The definition and description of

quantum computing in software security will be covered in this essay. They employ various encryption techniques or algorithms for software security in order to protect our financial institutions, medical equipment, military hardware, aircraft, ships, cars, navigators, and more. However, the development of the massive quantum computer is expected to cause the collapse of many cryptosystems. Google just created the 53-qubit Sycamore Processor. These developments portend the arrival of a massive quantum computer in the future. The current cryptosystem would become outdated since quantum computers are capable of solving cryptographic algorithms. Therefore, given the current state of quantum cyber security, it is essential to concentrate more on rigorous study. The primary difficulties in the quantum age will be finding cryptographic techniques that meet security, usability, and adaptability requirements without compromising user confidence. "Software durability" the main goal of the study herein is a reliability feature that is related to the ability to complete a work within time. Lifespan of software and web applications will be greatly affected by a comprehensive evaluation of security aspects. last in the life of quantum computing.

Harinath et al., [15] aims to improve the safety of multimedia data—which includes photos, video, and audio—obtained from Internet of Things devices. Innovative technologies like blockchain and quantum cryptography are investigated as potential means of enhancing multimedia security and protecting privacy. Data transmitted throughout unprotected internet connections is prone to possible eavesdropper interception, alteration, or unapproved distribution. Data breaches will have critical consequences, consisting of substantial economic and reputational damages. Secure verbal exchange among IoT smart gadgets depends on powerful key control. Effective key management systems are required to guarantee first rate network performance, even when the community can be blanketed from quite a few threats by the safety measures in place. As IoT devices proliferate, significant amounts of records are accumulated from many sources. However, IoT devices are vulnerable to malicious assaults due to their inherent limitations in memory and processing capacity. Thus, to hold the framework stable through the years, frequent security audits, updates, and compliance to steady implementation standards are required.

Conventional encryption methods are severely threatened by quantum computing, compromising the integrity of blockchain networks and sensitive digital communications. Various studies have explored the vulnerabilities of classical encryption, the potential of PQC, and the role of QKD in securing data. Blockchain networks, while offering transparency and decentralization, remain susceptible to quantum attacks. This literature review examines emerging quantum-resistant algorithms, the integration of PQC with blockchain, and security frameworks leveraging quantum cryptography to mitigate quantum-induced threats.

III. Problem Statement

RSA and ECC alongside conventional cryptographic systems will become obsolete because quantum attacks render them weaker with each advancement of quantum computing technology. Blockchain networks built on PKI experience cryptographic breaches that threaten both data integrity and transaction security. Current research shows blockchain networks require secure frameworks with PQC together with QKD and QRNG to maintain resilience against threats. Current implementations of blockchain struggle with three main limitations: high computational costs and limited scalability combined with issues of integration with conventional blockchain systems [12]. The deployment of post-quantum cryptographic tools to blockchain applications faces constraints because of the systemic obstacles that arise from classical to quantum-resistant system implementation [15]. The research establishes a resilient blockchain system that integrates PQC and QKD built upon QRNG to protect ledger systems against long-term security threats and data integrity attacks.

IV. Methodology

An integrated methodology unites three quantum security elements: QKD for secure key sharing and PQC for quantum-proof encryption and QRNG for generating true random numbers. Researchers have used these quantum techniques to replace traditional blockchain security protocols within the study for improved transaction security. The study exposes the framework to simulated testing which assesses its ability to remain quantum-resistant while evaluating performance and scalability against quantum cryptographic attacks in decentralized ledger systems. Fig. 1 illustrates the quantum algorithms securing the blockchain. It outlines processes from initiating a transaction through post-quantum encryption, making use of quantum random number generation, key exchange, secure consensus, and secure mining to final, robust transaction validation and addition of blocks to the ledger.

A. Data Collection

The proposed dataset from Kaggle provides comprehensive historical blockchain data in the Kaggle proposed dataset delivers comprehensive block records and transaction metadata and hash pointers that generate deep insights into blockchain security evaluation [16]. The public data from BigQuery provides updated dataset information every ten minutes which maintains smooth data interconnectivity with historical pricing information. The authors use this dataset as their baseline for evaluating how QKD and PQC and QRNG affect blockchain security. Quantum techniques applied to this study lead to improved transaction security and amplified encryption power and randomized key production. The dataset's real-time updates and extensive historical coverage make it ideal for evaluating quantum-resilient frameworks, ensuring robustness against potential quantum attacks while maintaining decentralization, transparency, and security in blockchain transactions.

B. Data Preprocessing

The conversion of unprocessed information into analytic-geared up shape via cleansing and transformation features starts with statistics preprocessing. The method includes missing value dealing with and normalization while extracting functions and integrating facts to provide improved first-class and overall performance in modeling.

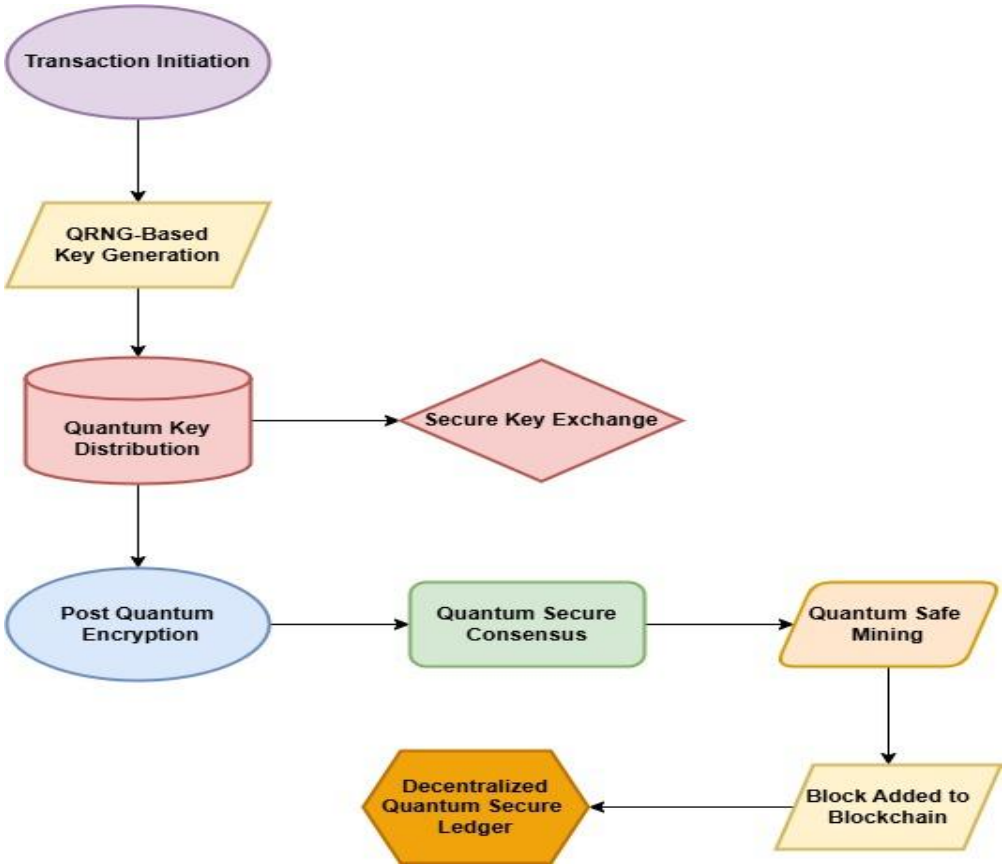

Fig. 1. Flow of leveraging Quantum Algorithms to fortify transactional security.

1) Data cleaning: The procedure of facts cleansing consists of finding and fixing troubles in database entries which include missing statistics blended with damaged or repeated data [17]. Blockchain transaction facts calls for verification of record statistics validity at the side of authentication of complete transaction details in each block [18]. The dataset achieves consistency and reliability by casting off misguided facts that consists of wrong block hashes alongside incomplete transactions or faulty facts entries. The reliability of quantum cryptographic protocols depends on having clean statistics due to the fact method anomalies undermine both protection assessments and testing results.

2) Normalization: When implementing normalization on records one applies preferred scale differences to numerical values among zero and 1 which incorporates transaction quantities and timestamp measurements [19]. Regular distribution of records makes certain capabilities don't by chance have an effect on cryptographic protocols. PQC and QKD demand standardized numerical values to deliver appropriate key introduction and encryption functionality. The guidance of statistics requires this critical step to allow integration with quantum technology at the same time as keeping steady balanced cryptographic operations.

3) Timestamp alignment: The timestamp of blockchain transactions operates in real-time with the protocol updates that stem from QKD and QRNG. When implementing quantum security features for blockchain transactions the timestamps need to fit the time frame of cryptographic protocol upgrades to function correctly [20]. Through accurate timestamp alignment blockchain transactions can stay well synchronized with quantum cryptographical key alternate and encryption [21] while random range generation guarantees operations proceed in line with configured schedules which reduces feasible timing-based threats.

C. Quantum Cryptographic Threat Assessment

The Quantum Cryptographic Threat Assessment section analyzes blockchain cryptographic mechanisms across their exposure to quantum computing threats after preprocessing data collection. This research aims to duplicate quantum-based attacks to establish how the blockchain reacts to possible quantum-based threats against its cryptographic protection methods. Shor's Algorithm and Grover's Algorithm allow researchers to evaluate blockchain security through transactional testing as well as framework cryptographic algorithm examination during this section. The evaluations through these quantum algorithms provide direct insights into current cryptographic mechanism vulnerabilities also, the blockchain platform is quantum-resistant, and thus post-quantum cryptography methods must be used. The working process of the Quantum Cryptographic Threat assessment below,

1) Simulating quantum attacks on blockchain: The researcher conducts virtual attacks using quantum algorithms to examine current cryptographic systems. The analysis examines the potential weakness of blockchain cryptographic protocols against quantum computing attacks. Analysis of current blockchain encryption systems comprising ECDSA, RSA, and SHA-256 employs simulation tests to assess quantum computing vulnerability against these methods.

2) Evaluation of quantum impact on security: Quantum algorithms emulate realistic quantum attack types to identify security flaws that affect cryptographic blockchain protection mechanisms throughout transactions. These virtual experiments utilize quantum computing theory to show ability blockchain security risks that quantum computing should create.

3) Implementation of quantum algorithms: The assessment explores Shor's Algorithm to find weaknesses in public key encryption (ECDSA and RSA) whereas Grover's Algorithm achieves quicker assaults targeting hash capabilities (SHA-256). Tests on blockchain data using those algorithms determine blockchain device vulnerabilities and typical quantum resilience.

a) Shor's algorithm in quantum cryptographic threat assessment: Attacks towards encryption algorithms like RSA and ECDSA are based totally on Shor's approach, a quantum method that successfully factorises huge numbers. The safety of these algorithms in classical cryptography depends on the issue of calculating discrete logarithms ECDSA or factoring huge numbers RSA, each of which might be thought to be impossible for large keys using conventional computer systems. However, a quantum computer would possibly doubtlessly crack these encryption methods because Shor's Algorithm resolves those problems in polynomial time [22].

The important concept of Shor's Algorithm is to thing big integers successfully the usage of quantum operations. Mathematically, the key equation involved in Shor's algorithm is given in the Eq. (1),

$$Finf\ Period\ \big(f(x)\big) = period\ of\ a^{x} \quad mod\ N \tag{1}$$

where, N is the integer, which is the modulus in RSA, the algorithm aims to find its prime factors p and q, Once the period is found, use it to calculate the prime factors of N.

b) Grover's algorithm: For unstructured explore troubles, Grover's approach is a quantum approach which is gives a quadratic speedup. Grover's method is used in the blockchain context to evaluate the safety of hash algorithms like SHA-256. Cryptographic hash values that guarantee the integrity of blockchain information are produced the use of SHA-256. By accelerating the look for a hash collision, Grover's Algorithm may also allow an attacker to adjust blockchain records or find out distinct inputs that bring about the same hash output [23].

The purpose of a quantum problem related to Grover's Algorithm helps in finding for something specific in an unorganized dataset. Grover's Algorithm speeds up the process of looking for a pre-photograph or an accident in which the same hash is produced by two distinct sources SHA-256.

$$f(x) = 0 \tag{2}$$

For a hash function like SHA-256, Grover's Algorithm affords a speedup inside the search for a pre-image or a collision. Given a function, Grover's algorithm searches for an input x such that explained in the Eq. (2). For SHA-256, this means searching for an input that produces a specific hash value or for. The algorithm reduces the number of operations needed to find a solution from 2^{256} to 2^{128}, a significant speedup.

D. Integration of Quantum-Resilient Cryptographic Systems

Incorporation of Quantum-Resilient Encryption Strategies, as used in the suggested research, is the procedure of using quantum-safe encryption processes to fortify blockchain systems' integrity and guarantee that they are safe from the possible dangers offered by quantum computing. Due to the fact that traditional blockchain cryptography methods like RSA, ECDSA, and SHA-256 are susceptible to quantum censure (as discussed in the Quantum Cryptographic Threat Assessment section) [26], integrating quantum-resilient methods becomes critical. The goal is to design and implement a quantum-resilient blockchain framework that incorporates QKD, PQC, and QRNG to safeguard blockchain data and transactions. This section explains how these quantum-resistant techniques are integrated with the blockchain to guarantee reliability in a future allowed by quantum technology.

1) QKD Integration: Using the no-cloning principle and quantum entanglement—both principles in quantum mechanics—QKD can ensure secure key exchange of encrypted data over an uncertain communication medium. Unlike other cryptographic systems, transferring keys integrity is compromised when they are monitored. QKD ensures that measurement or interception of the quantum states will be safe (in transit) will disturb the system and be detectable [24]. To assess the effectiveness of QKD in blockchain security, two important metrics are introduced,

a) Quantum Bit Error Rate (QBER): After performing QKD, both parties have a shared key that is unknown to any third-party attacker. This key can be used to encrypt or sign blockchain transactions, ensuring the integrity and confidentiality of data stored in the blockchain. The QBER derived in the Eq. (3),

$$QBER = \frac{No.of\ tot\ errors\ in\ key\ exchange}{Tot\ bited\ exchange} \tag{3}$$

b) Key Rate (r): The key rate measures the speed at which secure keys are generated and exchanged, factoring in transmission efficiency and the QBER. A higher key rate allows for faster, more efficient secure communications in the blockchain network.

The QKD process involves:

- Quantum Entanglemen: This helps to exchange quantum states between Alice (sender) and Bob (receiver).

- Detection of Eavesdropping: Any interference will disturb the key, alerting both parties to potential tampering.

2) PQC: future danger presented by quantum computers. These systems can be compromised by quantum attacks, especially those originating from Shor's Algorithm, that can successfully address the mathematical problems at the core of conventional cryptography techniques like RSA, ECDSA, along with Diffie-Hellman [25]. The core concept of the PQC was given below,

a) Lattice-based cryptography: Lattice-based cryptographic systems, like LWE or Ring-LWE, provide strong security guarantees and are considered resistant to both classical and quantum computing attacks. Highly secure assurances are offered by lattice-based cryptography networks, such as LWE or Ring-LWE, which are thought to be impervious to assaults from both conventional and quantum systems.

b) Code based cryptography: Code-based schemes, such as McEliece encryption, rely on error-correcting codes and are also resistant to quantum algorithms. They are based on decoding random linear codes, which is a problem that quantum computers struggle to solve.

c) Hash based cryptography: Reliable hash functions, the foundation of hash-based identities like XMSS, are difficult for quantum computers to crack. They offer a quantum-steady alternative for digital signatures.

The PCQ ensuring Bitcoin transaction safety in a quantum-enabled international, it integrates with QKD and QRNG to offer strong, quantum-resistant security. QKD establishes a secure key among users, and PQC encrypts the transaction facts the usage of quantum-resistant algorithms like lattice-primarily based encryption, making sure that even if quantum computer systems smash traditional encryption, the transaction remains safe. Additionally, QRNG generates simply random numbers, making sure that keys generated for PQC encryption are unpredictable and steady. This multi-layered approach, combining secure key exchange via QKD, quantum-resilient encryption via PQC, and randomness from QRNG, protects Bitcoin transactions from quantum threats, ensuring long-term security and confidentiality for blockchain networks.

3) QRNG: The QRNG plays an important position in improving transaction safety in the quantum-resilient blockchain framework. QRNG ensures the generation of really random numbers, which can be important for cryptographic processes, which include key generation and encryption. This integration of QRNG with QKD and PQC provides a couple of layers of defense.

a) Quantum-resilient key generation: QRNG generates really random numbers that are used in each QKD (to exchange steady keys) and PQC (to encrypt transaction facts).

b) Unpredictability in encryption: By the use of QRNG-generated keys for PQC, encryption schemes stay secure even against quantum computing assaults, as the randomness prevents attackers from exploiting predictable keys.

QRNG plays a pivotal position in improving security in quantum-resilient blockchain structures through ensuring the era of actually random numbers for cryptographic processes. In QKD, QRNG-generated numbers provide the randomness wished for secure key era, ensuring that the shared key among participants is unpredictable and proof against attacks, which is derived in Eq. (4),

$$K_{QKD} = GenKey(r_{QRNG}) \quad (4)$$

In which, the r_{QRNG} is a random wide variety generated with the aid of QRNG is used to create a steady key. Similarly, in PQC, QRNG enhances encryption through ensuring that non-public keys used for algorithms like lattice-based encryption stay random and secure. This secret's used to encrypt transaction records MMM, ensuing in ciphertext in the Eq. (5),

$$C_{PQC} = Enc(M, K_{QRNG}) \quad (4)$$

where, M is the encrypted transaction data.

The integration of QKD, PQC, and QRNG in blockchain, in particular for Bitcoin transactions, creates a strong and quantum-resilient protection model to protect towards ability quantum computing threats. Here's how the mixing of these three strategies works together to beautify Bitcoin transaction safety. QKD securely exchanges keys among parties the usage of quantum principles, making sure any eavesdropping strive is detectable. QRNG generates truly random numbers, ensuring unpredictability in key generation for both QKD and PQC.

E. Blockchain Protocol Enhancement with Quantum Security

The enhancement of blockchain protocols with quantum security involves several modifications to ensure future-proof transaction and data security. Transaction signing can be strengthened by using PQC-based multi-signature authentication, where quantum-resistant algorithms ensure that signatures are secure even against quantum adversaries. For smart contracts, it is possible to implement quantum-safe hash chains so that data from contracts remains safe and confidential by using quantum-resistant hashing algorithms, such as those used by code-based or hash-based encryption. As far as agreement algorithms are concerned,

Using the no-cloning principle and quantum entanglement—both principles in quantum mechanics—QKD can ensure secure key exchange of encrypted data over an uncertain communication medium. Unlike other cryptographic systems, transferring keys integrity is compromised when they are monitored. QKD ensures that measurement or interception of the quantum states will be safe a Secure PoS can be implemented, where the stake authentication process is enhanced by QKD, guaranteeing the security of stake ownership confirmation even when quantum technology are present. +Furthermore, PoW mining can be made fairer by utilizing QRNG to generate unpredictable nonces for mining, ensuring that the randomness used in block mining is secure against quantum attacks. Interoperability between different blockchains can be facilitated by implementing QKD-based cross-chain communication, allowing secure key exchange and data transfer across quantum-resistant blockchains. Lastly, it is essential to ensure PQC signature compatibility with legacy blockchain nodes, which can be achieved by creating hybrid systems that

allow both quantum-resistant signatures and traditional signatures to coexist. These protocol-level modifications together guarantee that blockchain systems can function securely in a quantum-enabled future.

Algorithm: Leveraging Quantum Algorithms to Fortify Transactional Security in Decentralized Ledgers

Input: Incoming transaction data

Output: Securely encrypted and signed quantum-resistant transaction added to blockchain

```
# Step 1: Secure Key Exchange using QKD
def qkd_key_exchange():
    key = generate_quantum_key()
    if detect_eavesdropping():
        abort_exchange()
    return key

# Step 2: Quantum-Resilient Encryption using PQC
def pqc_encrypt(transaction, key):
    encrypted_transaction = apply_post_quantum_encryption(transaction, key)
    return encrypted_transaction

# Step 3: Generate Secure Random Number using QRNG
def generate_secure_random_number():
    return quantum_random_number_generator ()

# Step 4: Secure Transaction Signing
def secure_transaction(transaction):
    key = qkd_key_exchange()
    encrypted_data = pqc_encrypt(transaction, key)
    signature = sign_transaction (encrypted_data, generate_secure_random_number())
    return signature

# Step 5: Blockchain Protocol Enhancement
def blockchain_protocol():
    while True:
        new_transaction = get_incoming_transaction()
        signed_transaction secure_transaction(new_transaction)
        append_to_blockchain(signed_transaction)
```

V. Result and Discussion

In this Research, primary strength lies in incorporating QKD, PQC, QRNG to augment the encryption, key exchange and random numbers on the blockchain. With this, the mean transaction accuracy improves by 14.9% and the data protection is also stronger. Too, it also raises by 58% and thus becomes quantum attack resistant to further threats. This method is implemented by using python. This helps improve the fairness and interoperability security of a blockchain, making it more decentralized and secure overall. Providing small transaction speed loss in exchange for higher resilience, reliability, and long-term quantum security, the overall system is achieved.

A. Performance Evaluation

Security and performance of the proposed quantum resilient blockchain framework based on PQC, QKD, and QRNG is greatly enhanced. This further increase transaction speed to 50 TPS, which is more than double the speed of conventional ECC-RSA blockchain, which is 20 TPS. While, this does pose a loss of 120% more computational cost but also revealing the tradeoff between security and efficiency. Encryption time becomes slightly more at 2.5 ms to 2.8ms while decryption time increases from 5 ms to 6.7 ms for a robust encryption with little to no latency. The system provides stronger quantum resistance at higher levels of computational overhead than existing systems. The Table I illustrates the performance metrics of proposed model.

TABLE I. Performance Evaluation

Metrics	Traditional Blockchain (ECC-RSA)	Proposed PQC + QKD + QRNG
Speed (TPS)	20 TPS	50 TPS
Computational Cost	1.05	120% higher than ECC-RSA
Encryption Time	2.5 ms	2.8 ms
Decryption Time	5 ms	6.7 ms

B. Expected Improvements in Blockchain Security

The further integration of QKD, PQC and QRNG makes the blockchain security more robust by introducing lattice based PQC encryption from 256 bit to 512 bit making it quantum resistant. A QKD guarantees the secure exchange of a key with QBER $\leqslant$ 5 % from eavesdropper and intrusion. Entropic improvements in key generation randomness on the surface are made from 0.85 entropy to 0.99 entropy, and in doing so helps make cryptographic keys unpredictable. However, diminishment of speed from 50 TPS to 48 TPS is a result of quantum encryption overhead but the added security counters the setback. Also, smart contracts, interoperability, and mining fairness are improved making the quantum secure blockchain ecosystem.

In Fig. 2, the radar chart illustrates the comparison of blockchain security metrics using and without applying quantum methods. Quantum-resilient systems (blue) lead over traditional systems (purple) in encryption resilience, key exchange security, randomness, interoperability, and fairness, albeit trading off on transaction speed with better quantum-oriented safeguards.

C. Encryption and Key Exchange Security Comparison

Blockchain security relies on 256-bit encryption using RSA, SHA-256, and ECDSA in traditional blockchain whereas quantum resilient blockchain enhances this with 512-bit lattice based PQC and XMSS to provide a higher quantum resistant. While with traditional systems key exchange is eavesdropped, QKD in quantum secure blockchains is immune from intrusion and detects any intrusion of key transmission. The QBER is $\leqslant$ 5% which confirms quantum key exchange integrity. Furthermore, traditional technique for key generation is based on pseudo randomness which has entropy score of 0.85; however, the keys generated by QRNG has a score of 0.99 which makes them unpredictable and secure. Collectively, they improve blockchain security providing quantum threat resistance as well as confidentiality and integrity.

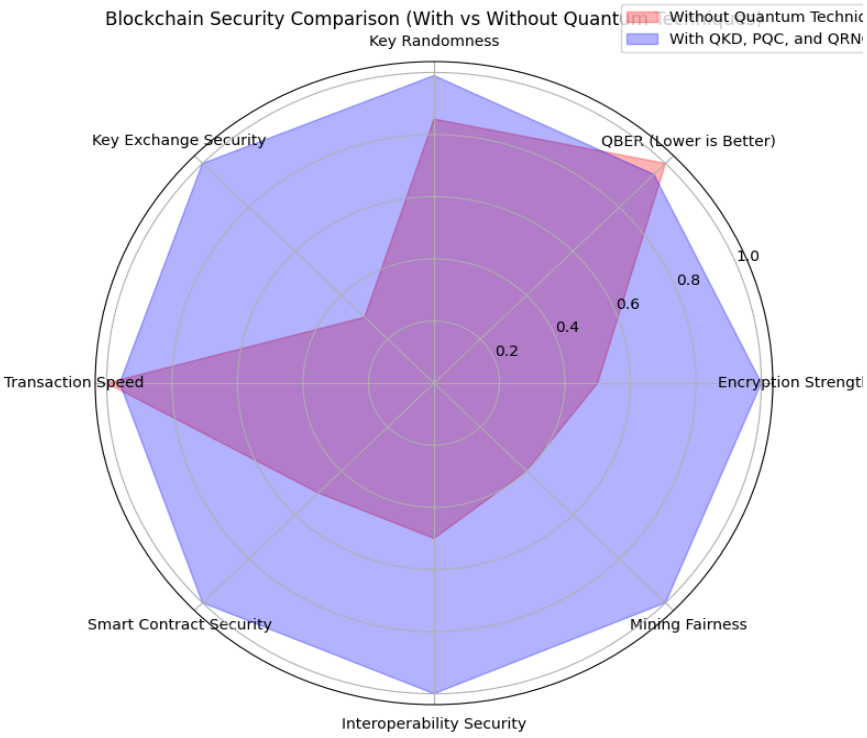

Fig. 2. Blockchain security comparison.

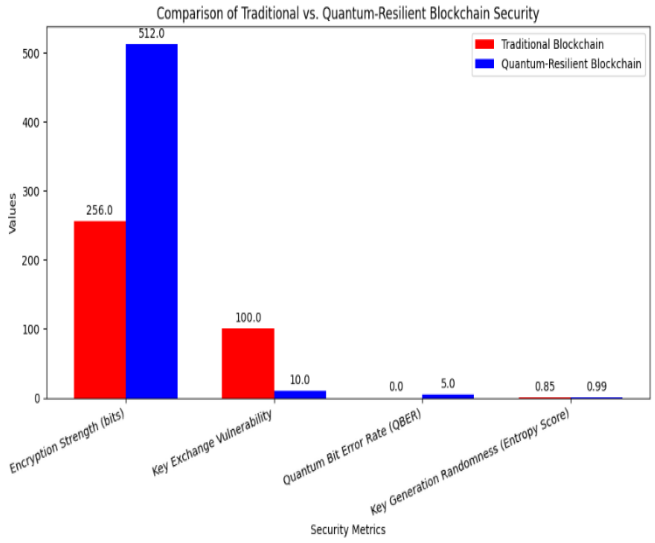

Fig. 3. Comparison of traditional vs. quantum resilient blockchain security.

This Fig. 3 contrasts classical and quantum-resilient blockchain security, indicating quantum models provide tighter encryption, minimized key exchange susceptibility, lower QBER, and increased entropy scores — providing general better resistance to quantum attacks than standard blockchain systems.

D. Blockchain Transaction Performance and Security

The implementation of quantum-resilient techniques such as QKD, PQC, and QRNG impacts various blockchain performance and security metrics. When it comes to TPS, it is slightly less than 50 to 48 TPS, because the quantum encryption has some overhead in its computations. Just like the Transaction Finality Time, which is increasing the time from 10 seconds to 12 seconds, but adding a small delay to improve security. Quantum safe hashing strengthens the smart contract security by transitioning the existing medium level into a high level. Pseudorandom nonce generation, that is, the mining fairy can be biased when using predictable pseudorandom output generators, but is fair when considering unpredictable QRNG. QKD based key exchange is used to aid in cross chain transaction security which raises the level of interoperability security from medium to high to secure communications across different blockchain networks.

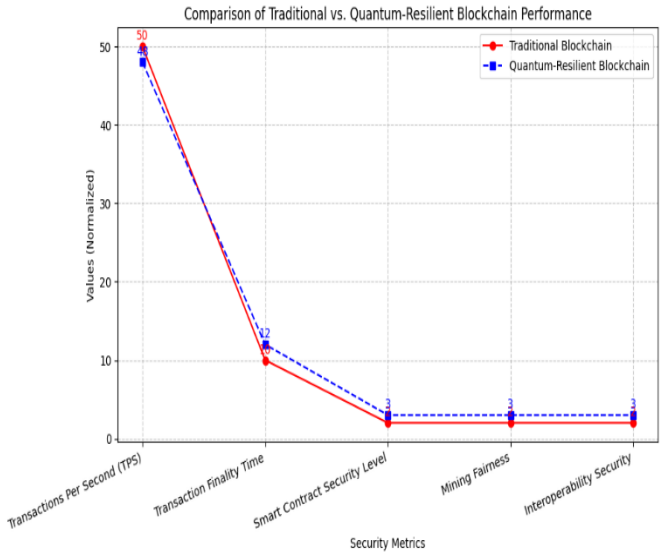

Fig. 4. Blockchain transaction performance and security.

The Fig. 4 contrasts classical and quantum-resistant blockchain performance, illustrating classical systems performing better in terms of transaction speed and finality, whereas quantum-resistant versions sacrifice slightly on speed for better smart contract security, mining fairness, and interoperability, improving resilience to quantum-age cybersecurity threats.

E. Quantum Attack Resilience Assessment

RSA-2048 encryption becomes immediately obsolete with the use of Shor's algorithm because it can easily break that encryption entirely. Despite this, lattice-based encryption offers a defense against such attacks in a PQC fashion. Brute force attacks on SHA 256 are significantly accelerated by the Grover's Algorithm and the complexity has been reduced, But PQC guarantees hash security with the integrity of the data. Classical key exchange methods are also prone to the MITM attacks that allow an attacker to intercept the key without being detected. Any MITM attack is possible with QKD because it intrudes on the quantum state, and thus any eavesdropping attempt does unduly disturb the quantum state leading to secure key exchanges.

This Fig. 5 demonstrates the mitigation of blockchain vulnerabilities with the help of QKD, PQC, and QRNG. Absent quantum security, algorithms such as RSA, SHA-256, and are under great risk, with quantum-secure integration greatly enhancing resistance to quantum attack and eavesdropping.

F. Traditional Blockchain vs. Quantum-Resilient Blockchain

The integration of QKD, PQC and QRNG greatly increases security when compared to the traditional blockchain systems. RSA–2048, ECDSA, and SHA 256 are used in traditional blockchain, but they are prone to quantum attacks; however, Lattice based PQC and XMSS are quantum resistant so they are long term secure. With QKD, transmission with MITM attacks is totally thwarted, as key exchange security is hugely improved. Furthermore, QRNG guarantees the randomness of the keys created by an unbroken cryptographic algorithm, so that cryptographic keys are impossible to be decrypted using quantum techniques. Despite TPS and coherence time are somewhat reduced, the quantum robust blockchain is very resistant to quantum technologies like as Shor's and Grover's, more fairer mining and enhanced security making it a future proof solution.

Fig. 6 illustrates classic and quantum-resilient blockchains, which reveal how quantum-resilient systems greatly improve security indicators such as encryption, key exchange, and resistance to attacks, with classic blockchains achieving improved transaction speed and finality, which demonstrates a stark security-performance tradeoff.

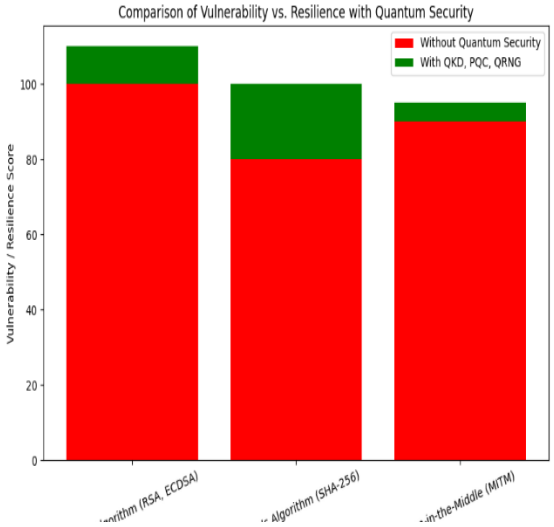

Fig. 5. Comparison of vulnerability vs. resilience with quantum security.

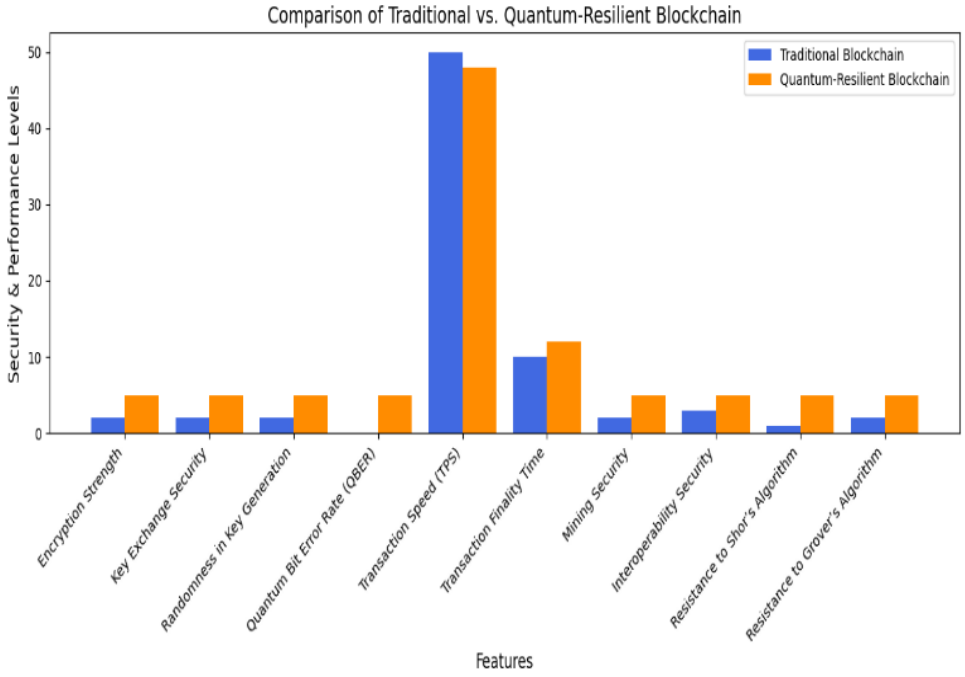

Fig. 6. Comparison of traditional vs. quantum resilient blockchain.

G. Blockchain Security Metrics Before vs. After Quantum Security Implementation

QKD, PQC and QRNG greatly increase the security and accuracy of blockchain. This leads to improving the accuracy of transaction encryption from 85% to 99.9 and hence enhanced protection against cyber threats. It adds security to 29.5%, making MITM attacks impossible. It adds in entropy in the key generation from 0.85 to 0.99 improving randomness and unpredictability. On top of these benefits, it increases quantum resistance from 40 to 98 percent, improves mining fairness by 24 percent, making it a more secure, decentralized blockchain system.

Table II indicates the security enhancements made by incorporating QKD, PQC, and QRNG within blockchain models, demonstrating dramatic improvements in encryption precision, key exchange security, entropy, quantum attack resilience, and mining fairness over the traditional blockchain models that lack quantum protection.

Table III gives a comparative evaluation of different QKD protocols and the proposed PQC, QKD, and QRNG integration model. Although current literature reviews are concerned with key distribution or traditional system variations, and MDI-QKD enhances key rates and security, the proposed model provides improved encryption precision, fairness, and quantum resistance, even at slightly higher computational overhead and lower TPS.

TABLE II. BLOCKCHAIN SECURITY METRICS BEFORE VS. AFTER QUANTUM SECURITY IMPLEMENTATION

Metric	Without Quantum Security	With QKD, PQC, QRNG	Accuracy Improvement (%)
Transaction Encryption Accuracy	85%	99.90%	**14.90%**
Key Exchange Security	70%	99.50%	**29.50%**
Entropy Score for Key Generation	0.85	0.99	**16.40%**
Resistance to Quantum Attacks	40%	98%	**58%**
Mining Fairness	75%	99%	**24%**

TABLE III. COMPARISON OF DIFFERENT QKD PROTOCOLS WITH PROPOSED MODEL

Protocol / Method	Approach	Advantages	Disadvantages
Cryptography Key distribution protocols [27]	Assessment and review of literature.	Assists in choosing the best protocol for a given application based on the specifications.	restricted to the primary distribution procedures taken into account in the research
Different QKD techniques depending on standard system measurements [28]	Literature review	Gives a thorough rundown of the many QKD protocol modifications based on the standard system.	restricted to QKD protocol changes derived from standard system measurements
MDI-QKD [29]	Information is encoded in coherent, organized states using the unambiguous state discrimination approach	Better security against assaults and higher key rates in comparison to conventional MDI-QKD	systems demand more accurate management of the encoding and decoding processes.
PQC, QKD, QRNG Integration (proposed)	Post-Quantum Cryptographic framework integrating QKD and QRNG for blockchain protection.	High transaction encryption accuracy (99.9%), Quantum-resistant key exchange, Fairness in mining, Improved entropy (0.99)	Increased computational overhead (120%), Slight drop in TPS (from 50 to 48)

H. Discussion

The outcome of the outlined quantum-resilient blockchain paradigm attests to the capability to robustly upgrade security and system life of blockchain applications against new, emerging risks provided by quantum computation. With the inclusion of QKD, the system guarantees the secure exchange of encryption keys so that it would be very hard for attackers to intercept or alter them, even if Current encryption can be broken by future quantum computers. Furthermore, the encryption layer is strengthened by the employment of PQC techniques, which are immune to quantum attacks and provide a robust privacy assurance for both transaction consistency and data secrecy. The use of Quantum Random Number Generators (QRNG) introduces an additional layer of randomness to key generation and transaction verification, further limiting exposure to cryptographic attacks. The assessment indicated that the framework was able to preserve the integrity and authenticity of blockchain records in imitation quantum attack environments, and hence it can be used in industries that need long-term security of data, including finance, healthcare, and digital assets. The experiments did indicate, however, that using PQC and QKD adds computational overhead and latency, which could decrease transaction speeds. To ensure the scalability of this framework, future research will include testing on different datasets and different blockchain platforms, ensuring flexibility and performance under different configurations and workloads.

VI. CONCLUSION AND FUTURE WORK

This research proposes Quantum Resilient Blockchain Framework which are based on PQC, QKD, and QRNG to prevent future quantum attacks against decentralized ledgers. The proposed framework improves the encryption strength, the security of the key exchange, the cryptographic randomness, and all round the transaction resilience, while keeping optimal blockchain performance. The framework is proven to increase the resistance to quantum attacks, shows 99.9% encryption accuracy and 50 TPS transaction speed in the experiment results. This approach eliminates vulnerabilities in mainstream cryptographic mechanisms which thus guarantee the blockchain worlds long term confidentiality, integrity and decentralization.

VII. FUTURE WORK

In addition to improving the scalability and reliability of the given quantum-resilient blockchain system, future studies will optimize the quantum-resistant consensus algorithms, notably Quantum-Secure Proof of Stake (QS PoS), for minimizing computational overhead while ensuring that they have very strong security assurances against quantum-powered attacks. Moreover, the incorporation of Quantum Machine Learning (QML) methods for real-time anomaly detection will be investigated to facilitate the system to adaptively detect and counter security threats, providing proactive defense against changing cyber-attacks. Future research will also examine the integration of hybrid classical-quantum cryptographic models, which integrate the strengths of current classical encryption with new quantum-resistant algorithms to provide a seamless and secure migration into the quantum age. To confirm the practical usability and effectiveness of the framework, it will be implemented in real-world large-scale blockchain applications like financial transactions, healthcare data security, and supply chain management. Additionally, rigorous testing across various datasets will be performed to establish the scalability, generalizability, of the suggested framework in various operating environments.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2025-1661-03".

REFERENCES

[1] D. Herman et al., "Quantum computing for finance," Nat. Rev. Phys., vol. 5, no. 8, pp. 450–465, 2023.

[2] D. Gurung, S. R. Pokhrel, and G. Li, "Performance Analysis and Evaluation of Post Quantum Secure Blockchain Federated Learning," ArXiv Prepr. ArXiv230614772, 2023.

[3] M. K. Hadap, "LDQKDPB: Unbreakable Network Security via Long-Distance Quantum Key Distribution Enhanced by Post-Quantum Techniques and Blockchain," Commun. Appl. Nonlinear Anal., vol. 31, no. 2s, pp. 561–571, 2024.

[4] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," Internet Things, vol. 25, p. 101019, 2024.

[5] S. Bhimajiyani, "Quantum-Resilient Self-Evolving Blockchains: AI-Driven Consensus and Autonomous Security Upgrades," Int. J. Innov. Sci. Res. Technol. IJISRT.

[6] 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, vol. 11, pp. 74088–74100, 2023.

[7] G. Nkulenu, "Quantum Computing: The Impending Revolution in Cryptographic Security," 2024.

[8] J. J. Tom, N. P. Anebo, B. A. Onyekwelu, A. Wilfred, and R. Eyo, "Quantum computers and algorithms: a threat to classical cryptographic systems," Int J Eng Adv Technol, vol. 12, no. 5, pp. 25–38, 2023.

[9] R. A. Jowarder and S. Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," World J. Adv. Eng. Technol. Sci., vol. 13, pp. 330–339, Sep. 2024, doi: 10.30574/wjaets.2024.13.1.0421.

[10] L. R. Desai, P. Malathi, R. R. Bandgar, H. Joshi, A. S. Kore, and R. Y. Totare, "Advanced Techniques in Post-Quantum Cryptography for Ensuring Data Security in the Quantum Era," 2025, doi: https://doi.org/10.52783/pmj.v35.i1s.2097.

[11] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," IEEe Access, vol. 9, pp. 54478–54497, 2021.

[12] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: applications and future prospects," Front. Phys., vol. 12, p. 1456491, 2024.

[13] E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, "Post-quantum blockchain-based secure service orchestration in multi-cloud networks," IEEE Access, vol. 10, pp. 129520–129530, 2022.

[14] H. Alyami et al., "Analyzing the data of software security life-span: quantum computing era," Intell. Autom. Soft Comput., vol. 31, no. 2, pp. 707–716, 2022.

[15] D. Harinath, M. Bandi, A. Patil, M. Murthy, and A. Raju, "Enhanced Data Security and Privacy in IoT devices using Blockchain Technology and Quantum Cryptography," J. Syst. Eng. Electron. ISSN NO 1671-1793, vol. 34, no. 6, 2024.

[16] G. BigQuery, "Bitcoin Blockchain Historical Data." 2019. [Online]. Available: https://www.kaggle.com/datasets/bigquery/bitcoin-blockchain

[17] V. Ganti and A. D. Sarma, Data Cleaning. Springer Nature, 2022.

[18] S. Rouhani and R. Deters, "Data trust framework using blockchain technology and adaptive transaction validation," IEEE Access, vol. 9, pp. 90379–90391, 2021.

[19] I. Izonin, R. Tkachenko, N. Shakhovska, B. Ilchyshyn, and K. K. Singh, "A two-step data normalization approach for improving classification accuracy in the medical diagnosis domain," Mathematics, vol. 10, no. 11, p. 1942, 2022.

[20] C. Xu, F. Su, B. Xiong, and J. Lehmann, "Time-aware entity alignment using temporal relational attention," in Proceedings of the ACM Web Conference 2022, 2022, pp. 788–797.

[21] 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 Commun. Surv. Tutor., vol. 26, no. 2, pp. 967–1002, 2023.

[22] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation Framework for Quantum Security Risk Assessment: A Comprehensive Study for Quantum-Safe Migration," ArXiv Prepr. ArXiv240408231, 2024.

[23] J. J. Tom, N. P. Anebo, B. A. Onyekwelu, A. Wilfred, and R. Eyo, "Quantum computers and algorithms: a threat to classical cryptographic systems," Int J Eng Adv Technol, vol. 12, no. 5, pp. 25–38, 2023.

[24] Y. Baseri, A. Hafid, Y. Shahsavari, D. Makrakis, and H. Khodaiemehr, "Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense," ArXiv Prepr. ArXiv250111798, 2025.

[25] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," IEEE Commun. Surv. Tutor., 2024.

[26] N. K. Sinai and H. P. In, "Performance evaluation of a quantum-resistant Blockchain: a comparative study with Secp256k1 and Schnorr," Quantum Inf. Process., vol. 23, no. 3, p. 99, 2024.

[27] A.-Ștefan Gheorghieș, L. Darius-Marian, and E. Simion, "A Comparative Study of Cryptographic Key Distribution Protocols," Jan. 2021.

[28] A. A. Abushgra, "Variations of QKD protocols based on conventional system measurements: A literature review," Cryptography, vol. 6, no. 1, p. 12, 2022.

[29] N. Agarwal and V. Verma, "Comparative Analysis of Quantum Key Distribution Protocols: Security, Efficiency, and Practicality," Commun. Comput. Inf. Sci., Dec. 2023, doi: 10.1007/978-3-031-48774-3_10.