Enhancing Security using Quantum Blockchain in Consumer IoT Networks

Mritunjay Shall Peelam, Vinay Chamola*, *Senior Member, IEEE and*
Biplab Sikdar Senior Member, IEEE

***Abstract*—Blockchain technology, renowned for its ability to securely store data, hashes, and signatures permanently, faces unprecedented challenges in secure Consumer IoT (CIoT) networks with the advent of quantum computing. This paper proposes a set of robust quantum-based protocols and techniques to address these challenges by enhancing the security, scalability, and reliability of CIoT systems in the face of quantum threats. Updating the blockchain infrastructure is imperative to ensure ongoing security, which involves forks or protocol adjustments to establish new post-quantum chains and addresses, requiring rapid data and asset migration by users. Blockchain guarantees data integrity through an immutable ledger of transactions distributed via cryptographic hashes. The proposed quantum protocols and techniques enhance scalability and reliability and address the unique security needs of both commercial and governmental applications in secure CIoT networks through immersive embedded cyber-physical systems. These include Quantum Currency Security Protocols, Distributed Ledger Data Blocks, Quantum Ledger Verification, Quantum Solutions for Middleman Attacks, and the integration of Elliptic Curve Cryptography (ECC)-based security measures. By integrating these methods, the proposed approach ensures robust protection against emerging quantum threats, thereby securing sensitive information and transactions.**

***Index Terms*—Quantum Computing, Quantum Key Distribution (QKD), Blockchain, CIoT, Consumer IoT, Consumer Electronics Network.**

I. INTRODUCTION

QUANTUM computing solves the mathematical challenges underlying most forms of encryption today [1]. Quantum computers present a significant challenge to the effectiveness of current asymmetric encryption methods [2]. Asymmetric cryptography involves generating a pair of keys, one private and one public, that are mathematically related [3]. The private key must remain confidential, while the public key is openly shared. Digital signatures created using this method can be verified by anyone possessing the corresponding public key, a crucial feature used extensively in the financial industry to validate transactions [4]. The security of asymmetric cryptography relies on the mathematical concept of a "Message Digest", which ensures that while it's computationally feasible to derive the public key from the private key, the reverse process is computationally infeasible [5, 6]. This fundamental principle is the foundation for protecting electronic transactions and communications within consumer networks to enhance IoT security through immersive embedded cyber-physical systems. Fig. 1 shows the different layers of a blockchain system and the types of attacks it faces. It starts with block data, networking protocols, consensus algorithms, smart contracts, and decentralized applications. Each layer is susceptible to specific attacks like network attacks, consensus manipulation, and contract tampering, which can compromise data security and system integrity [6–8]. Quantum blockchain technology enhances security in Consumer IoT through advanced quantum techniques. Quantum-resistant encryption, such as lattice-based cryptography or multivariate cryptography, protects sensitive data, ensuring confidentiality and thwarting breaches of the CIA triad [9]. Robust quantum cryptographic protocols, like Quantum Key Distribution (QKD), defend against network attacks such as eavesdropping and man-in-the-middle attacks [10, 11]. Quantum-resistant consensus algorithms prevent manipulation and maintain transaction integrity, including Quantum-Resistant Proof of Work (QR-PoW) or Quantum-Resistant Proof of Stake (QR-PoS).

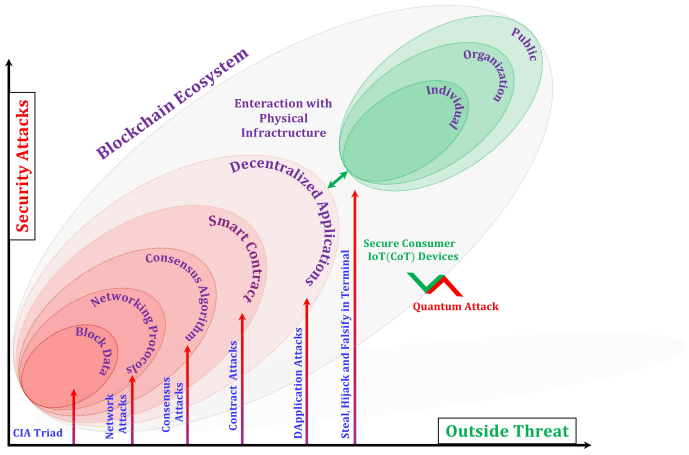

Fig. 1: Layered representation of a blockchain system highlighting potential attack vectors.

Integration with Hardware Security Modules (HSMs) employing quantum-resistant algorithms, such as quantum-safe digital signatures or quantum-safe hash functions, secure against physical attacks like theft, hijacking,

*Corresponding author.
Mritunjay Shall Peelam and Vinay Chamola are with the Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India 333031. Vinay Chamola is also with APPCAIR. (e-mail: {mritunjay.peelam, vinay.chamola}@pilani.bits-pilani.ac.in.)
Biplab Sikdar is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 119077 (e-mail: bsikdar@nus.edu.sg).

and tampering of device interactions with blockchain networks [12]. This comprehensive approach ensures that consumer IoT networks remain secure against emerging threats posed by quantum computing and physical security risks.

A. Significance of Quantum Blockchain

Blockchain is a distributed ledger technology that facilitates consensus building across a large, potentially dishonest user base due to its high Byzantine Fault Tolerance (BFT) [6, 22]. Key features of blockchain technology, such as accountability and transaction transparency, make it appealing for a wide range of uses, from smart contracts to manufacturing [23]. On a modern blockchain network, any user may record a new transaction in the distributed ledger. This specification allows for the transfer of digital assets between parties and stipulates that the digital signature of the initiator must sign each transaction. Each user's transaction history is stored as a blockchain on their local computer [24]. Securing these networks, especially against emerging quantum threats, remains a challenge. Fig 2 shows the

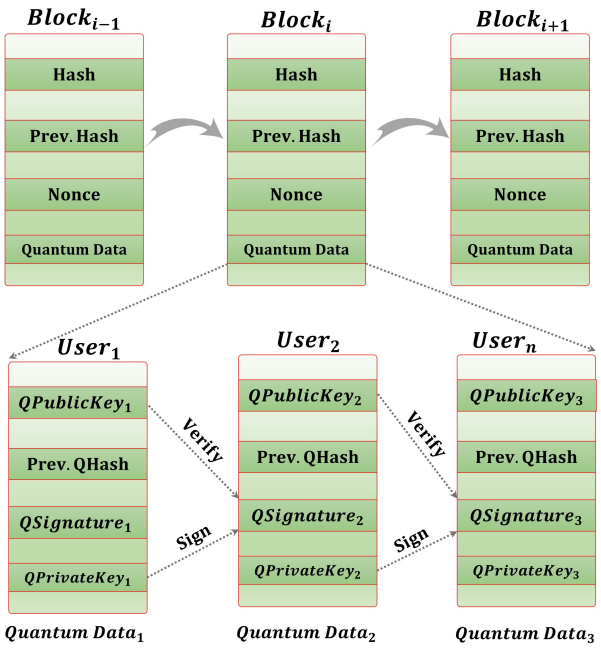

Fig. 2: Quantum blockchain data organization in secure Consumer IoT networks.

quantum blockchain data organization designed to address the challenges of secure Consumer IoT networks. The structure comprises sequential blocks ($Block_{i-1}$, $Block_i$, and $Block_{i+1}$) containing essential elements such as Hash, Previous Hash, Nonce, and Quantum Data. Each block is cryptographically linked to its predecessor, ensuring data integrity. Users ($User_1, User_2, ...User_n$) interact with this system through quantum keys ($QPublicKey, QPrivateKey$) and signatures ($QSignature$), providing a robust verification mechanism. This quantum-enhanced blockchain framework aims to enhance security, protect against quantum attacks, and ensure reliable data handling across consumer IoT networks. It is an ideal solution for safeguarding sensitive information and transactions [8, 25]. The blockchain is a decentralized database constructed through a series of interconnected blocks, each encompassing four crucial elements: Hash of the preceding block, Quantum computing-related data content, Nonce, utilized to shape the hash into a predetermined form, and Hash of the block itself. Quantum computing introduces unique computational capabilities that require specialized handling of quantum data [26]. Integrating these attributes into secure Consumer IoT networks makes it possible to ensure the integrity, confidentiality, and reliability of quantum information within these networks. This enables secure consumer IoT networks to effectively serve as robust and trustworthy platforms for managing quantum data, contributing to the advancement and adoption of quantum technologies [26]. The advent of universal quantum computers poses significant threats to traditional security methods in secure consumer IoT networks [27]. Table I compares traditional cryptographic methods like RSA and ECC and quantum-resistant methods like lattice-based and hash-based cryptography. It highlights key differences in areas like quantum vulnerability, key sizes, computational efficiency, and long-term security, emphasizing the potential impact of quantum threats on consumer IoT networks. Quantum computing threatens encryption methods like RSA and ECC, which are commonly used in blockchain, by making it possible to break their security through algorithms like Shor's. Quantum-resistant encryption methods, such as lattice-based or hash-based cryptography, are being developed to counter this [20]. Blockchain systems can integrate these quantum-resistant algorithms to ensure long-term security. Early adoption of these approaches is crucial to secure against future quantum attacks on current encryption standards [28]. Shor's quantum algorithm, capable of factoring large numbers and discrete logarithms in polynomial time, undermines the security of such algorithms [25, 29]. The essence of Shor's algorithm can be encapsulated by the equation for period finding:

$$r = \min\{r > 0 : a^r \equiv 1 \pmod{N}\}, \tag{1}$$

Where N is the large integer to be factored, a is a randomly chosen number less than N, and r is the order of a modulo N. Successfully determining r enables the efficient factorization of N. Shor's algorithm, encapsulated by the equation 1 demonstrates how large numbers used in encryption, such as RSA, can be factored efficiently [30]. This process is particularly relevant in smart consumer electronics devices within CioT networks. For example, in a network of smart home devices such as cameras, smart locks, and thermostats, which use RSA encryption for secure communication, Shor's algorithm aids in finding the period r, where $a^r \equiv 1 \pmod{N}$, to solve the factoring problem [31]. Once this period is found, the system can streamline secure key exchanges and improve the efficiency of cryptographic operations. This example illustrates how the equation 1 encapsulates the core function of Shor's algorithm and its application to enhancing encryption and communication in CIoT networks. Grover's search method introduces vulnerabilities by providing a quadratic speedup in determining the inverse hash function [29]. The

TABLE I: Comparison between Quantum-Resistant Cryptographic and Traditional Cryptographic methods.

Parameter	Traditional Cryptographic Methods (RSA, ECC)	Quantum-Resistant Cryptographic Methods (Lattice-based, Hash-based)
Quantum Vulnerability [13]	Highly vulnerable (broken by Shor's algorithm)	Resistant to quantum attacks (e.g., 2^{128} quantum complexity for lattice problems)
Underlying Problem [14]	Integer factorization (RSA) or discrete logarithms (ECC)	Hard lattice problems (NTRU), hash functions, multivariate equations
Key Sizes [14]	RSA-2048 bits, ECC-256 bits for 128-bit security	Lattice-based: 1000–2000 bits, Hash-based: 256 bits for 128-bit security
Computation Efficiency [15]	RSA-2048: 1ms, ECC-256: 0.1ms per operation	Lattice-based: 5-10ms, Hash-based: 1-2ms per operation
Security Against Classical Attacks [16]	Strong (RSA-1024 broken), ECC-256 strong	Strong (based on NP-hard problems), hash-based also strong
Maturity and Adoption [17, 18]	Well-established, widely adopted (TLS, SSL, blockchain)	Still under research, some early adoption (e.g., NTRU)
Adaptability to Blockchain [19]	Integrates into current protocols	Requires key management adjustments and protocol updates
Long-Term Security [14]	Insecure in the quantum era (broken in minutes by large quantum computers)	Secure against classical and quantum attacks (128-256-bit quantum security)
Performance Overhead [20, 21]	Low (RSA-2048 encryption: 1MB/s)	Higher (Lattice-based: 200KB/s, Hash-based: 500KB/s)

foundational equation of Grover's algorithm, which outlines the number of iterations k needed to find a target item with high probability, is given by:

$$k = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor \tag{2}$$

Where N is the number of items in the database, this equation demonstrates Grover's algorithm's quadratic speedup over classical search methods. Computationally intensive post-quantum digital signatures alone may not suffice against assaults that manipulate the network's hash rate using a quantum computer [32]. While alternative approaches, such as blockchains based on mining procedures, exist to sustain distributed ledgers, they still rely on pairwise authenticated channels or digital signatures, leaving them vulnerable to quantum computer attacks. Pairwise authentic channels can ensure message integrity during transit but fail to address the transferability problem [33]. Post-quantum signatures are critical for securing blockchain in Consumer IoT networks as they address vulnerabilities posed by quantum computing [19]. Current advancements, like NIST's quantum-resistant algorithms (e.g., CRYSTALS-Dilithium, Falcon), are being integrated into blockchain frameworks to ensure resilient authentication and transaction validation [34]. These signatures are particularly practical in IoT settings due to their lightweight cryptographic nature, enabling secure end-to-end encryption for resource-constrained devices [35]. By securing data integrity and decentralizing trust, post-quantum signatures ensure tamper-resistant, future-proof protection against emerging quantum threats, making them vital for the security of smart consumer electronics [36].

B. Impact of Quantum Computing on Blockchain

Quantum computing rapidly moves from labs to mainstream use, promising efficiency in computational tasks beyond classical computers. It threatens the security of current cryptographic methods, posing challenges for technologies like IoT, blockchain, and AI [37, 38]. This shift has significant implications for consumer electronic networks, particularly ensuring secure operations. Ensuring secure Consumer IoT networks will require adapting to these quantum challenges. Blockchain and other Distributed Ledger Technologies (DLTs) provide transparency and security through public-key cryptography and hash functions. Quantum computing threatens these methods, necessitating the development of post-quantum cryptosystems [20]. This shift is crucial for maintaining secure operations in Consumer IoT networks. Quantum computers utilize qubits, allowing them to be in superposition states as:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{3}$$

with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively, where $|\alpha|^2 + |\beta|^2 = 1$. This property enables quantum parallelism, as an n-qubit system represents 2^n possible states simultaneously. Quantum algorithms, like Grover's algorithm, can search unsorted databases in $O(\sqrt{N})$ time, offering a quadratic speed-up over classical algorithms [39]. The impact of quantum blockchain on consumer IoT networks includes enhanced encryption and faster data processing, leading to more secure and efficient communication systems. This poses a risk to cryptographic codes protecting digital signatures and transaction histories, which is crucial as up to 10% of global GDP will be stored on blockchains by 2025 [40]. Quantum technology necessitates new cryptographic protocols to secure data, profoundly impacting Consumer IoT networks by altering industry data security practices. Table II shows the impact of quantum computing on various blockchain parameters, comparing classical blockchain performance with quantum-enhanced capabilities. Data for this analysis were collected from recent advancements and theoretical models in quantum computing and blockchain technology. This information benefits consumer IoT networks by highlighting potential transaction speed, security, and energy efficiency improvements, which are critical for developing more robust and efficient systems. Integrating quantum cryptography in Consumer IoT networks represents a significant advancement in blockchain security. Fig. 3 combines quantum computing with traditional blockchain methods. Using the unpredictable properties of quantum mechanics enhances security measures,

TABLE II: Influences of Quantum Computing on Blockchain Performance Metrics.

Blockchain Parameter	Classical Blockchain	Impact of Quantum Computing	Equivalent Signature (Classical)	Equivalent Signature (Quantum)
Hash Rate	10^{10} hashes/second	10^{30} hashes/second	SHA-256	SHA-512
Key Length	256 bits	512 bits or more	RSA-2048	Post-Quantum RSA-4096
Transaction Throughput	10 transactions/second	1000 transactions/second	ECDSA	Post-Quantum ECDSA
Latency	10 seconds	0.1 seconds	ECDSA	Post-Quantum ECDSA
Consensus Mechanism Efficiency	70%	90%	PoW	Quantum-Optimized PoW
Block Size (B)	1 MB	10 MB	SHA-256	Post-Quantum Block Compression
Block Creation Time (BCT)	10 minutes	1 minute	PoW	Quantum-Optimized PoW
Encryption Breaking Time	10^{12} years	10^{-3} years	RSA-2048	Quantum-Resistant Encryption
Signature Verification Speed	1000 verifications/second	10^{6} verifications/second	ECDSA	Post-Quantum ECDSA
Data Integrity Check Speed	500 checks/second	10^{4} checks/second	SHA-256	Post-Quantum Hashing
Smart Contract Execution Time	1 second	0.01 second	ECDSA	Post-Quantum Smart Contracts
Block Propagation Delay	5 seconds	0.5 seconds	SHA-256	Quantum-Optimized Propagation
Transaction Finality (TF)	1 hour	5 minutes	ECDSA	Post-Quantum ECDSA
Double Spend Attack Resistance	Medium	High	ECDSA	Post-Quantum Double Spend Resistance
Privacy Preservation (PP)	Medium	High	SHA-256	Quantum-Enhanced Privacy Protocols
Consensus Time	5 minutes	10 seconds	PoW	Quantum-Optimized Consensus Mechanisms

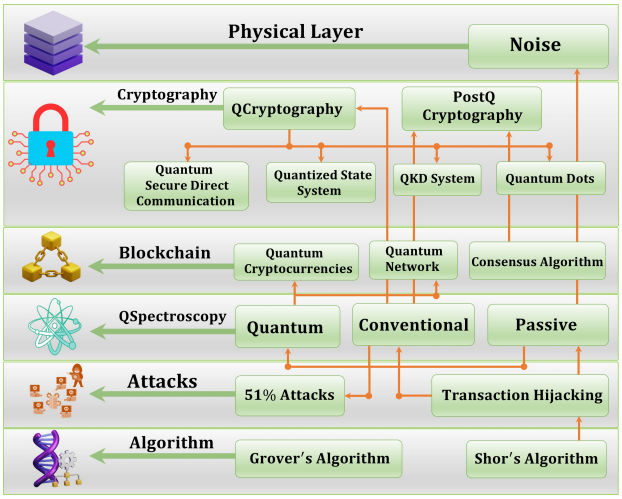

Fig. 3: Layered Integration Approach: Quantum Leap in Blockchain Security and the Impact of Quantum Computing on Blockchain.

making blockchain systems more resilient against potential breaches. This step secures our digital future and marks a major consumer IoT network technology advancement.

C. Role of Immersive Embedded Cyber-Physical Systems (IE-CPS) in Securing CIoT with Quantum Blockchain

The rapid growth of the CIoT has led to a significant increase in connected devices, raising concerns over data security, privacy, and system reliability [41]. IE-CPS and Quantum Blockchain offer an advanced secure communication and data management solution to address these challenges. The integration of these technologies enhances security and scalability while addressing the complexity of modern CIoT environments. IE-CPS involves the integration of computational capabilities into physical processes, enabling real-time interaction with the surrounding environment [42]. They are particularly valuable in CIoT, where they enhance interconnected devices' situational awareness and adaptability. The IE-CPS can be expressed as:

$$\text{IE-CPS} = \{(S, A, E) \mid S \subseteq S, A \subseteq A, E \subseteq E\} \quad (4)$$

Where:

- S represents the set of physical sensors that collect data ($S_i \in S$).
- A is the set of actuators that execute actions ($A_i \in A$).
- E represents the embedded computational environment ($E_i \in E$).

The system's control algorithms govern the real-time data flow and interaction between sensors and actuators, which can be represented using a control function [43].

$$u(t) = f(S, A, E, t) \quad (5)$$

Where $u(t)$ is the control signal at time t, and f is the function that dictates the behavior of the embedded system. The following are the roles of IE-CPS:

1) Enhanced Data Integrity through Quantum-Resistant Consensus: Quantum Blockchain ensures data integrity by utilizing QKD alongside a quantum-resistant consensus mechanism [44]. Using quantum keys QK_{AB} between two nodes A and B helps secure the communication channel.

$$QK_{AB} = \{q_i \mid q_i \in \{0, 1\}, i = 1, 2, \ldots, n\} \quad (6)$$

The consensus mechanism is resistant to quantum attacks, enabling secure transaction validation. Each block in the blockchain is encrypted using a quantum key QK_{AB}, making it difficult for adversaries to alter the contents of a block without detection:

$$B_i = (H(B_{i-1}), QK_{AB}, D_i, t_i) \quad (7)$$

2) Real-time Intrusion Detection with IE-CPS Monitoring: IE-CPS provides continuous monitoring of the physical environment and can detect anomalies in real-time, improving the security posture of CIoT devices [45]. This can be modeled as:

$$\mathcal{A}(t) = \{S_i(t), A_i(t) \mid i = 1, 2, \ldots, m\} \tag{8}$$

By integrating IE-CPS, any anomaly δ detected in sensor readings can be flagged as:

$$\delta = \begin{cases} 1 & \text{if } S_i(t) \neq \hat{S}_i(t) \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

Where $\hat{S}_i(t)$ represents the expected sensor readings, quantum-secured communication ensures that such alerts are transmitted securely to control centers, preventing tampering during transmission.

3) Scalable Secure Communication via Quantum Blockchain: Using quantum cryptography in blockchain networks allows for scalable and secure communication between numerous CIoT devices [46]. As the number of devices n increases, traditional encryption methods struggle with key management. Quantum key distribution simplifies this with the following:

$$\text{Key Length} \propto \log_2(n) \tag{10}$$

This relationship indicates that the length of the quantum key increases logarithmically with the number of devices, allowing secure key management even as the CIoT network scales. This ensures that each device in the IE-CPS framework can communicate securely without compromising performance.

4) Tamper-Proof Data Storage Using Quantum Ledger: The tamper-proof nature of Quantum Blockchain provides a secure ledger for storing CIoT data, ensuring that any unauthorized access or modification attempts are detectable [47]. If an adversary tries to clone a quantum state $|\psi\rangle$, the *no-cloning theorem* ensures:

$$|\psi\rangle \otimes |0\rangle \nrightarrow |\psi\rangle \otimes |\psi\rangle \tag{11}$$

This property is used to secure data in the blockchain, making it impossible to duplicate data blocks without detection. Thus, combining IE-CPS and Quantum Blockchain enables a tamper-resistant data storage mechanism where quantum keys secure each recorded transaction.

5) Secure Authentication and Key Exchange: Integrating IE-CPS with Quantum Blockchain allows for secure authentication of CIoT devices [48]. For two devices D_A and D_B, a mutual authentication process using QKD can be described as:

$$\text{Auth}(D_A, D_B) = \{(D_A, D_B) \mid H(QK_{D_A}) = H(QK_{D_B})\} \tag{12}$$

Where: $\text{Auth}(D_A, D_B)$ signifies that devices D_A and D_B have been authenticated if their quantum keys match after a hashing operation. This prevents unauthorized devices from joining the CIoT network, ensuring only legitimate nodes can communicate.

D. Salient Contributions

In this paper, we use quantum blockchain, which significantly enhances scalability and reliability while addressing the unique security needs of commercial and governmental applications within secure Consumer IoT networks. It includes novel contributions such as the Quantum Currency Security Protocol, Distributed Ledger Data Blocks for Consumer IoT Networks, Quantum Ledger Verification using Quantum Cryptography, and solutions for middleman attacks in blockchain using quantum security and privacy measures. It also integrates Elliptic Curve Cryptography (ECC)-based security measures to further enhance consumer IoT network protection.

- Introduces the Quantum Currency Security Protocol and Distributed Ledger Data Blocks to enhance security and privacy for commercial and governmental applications, like securing financial transactions in smart home CIoT networks.
- Proposes a design that improves transaction transparency and scalability in Distributed Ledger Data Blocks, for example, ensuring accurate tracking of data and payments in industrial CIoT systems.
- Uses Quantum Ledger Verification with quantum cryptography to ensure transaction integrity and authenticity, such as securely storing and verifying patient records in healthcare CIoT systems.
- Provides solutions for middleman attacks using advanced quantum security, like preventing data tampering in-vehicle communications in smart transportation CIoT systems.
- Employs quantum principles like entanglement to secure blockchain networks from middleman attacks, ensuring secure communication between vehicles in transportation CIoT systems.
- Integrates Quantum Key Distribution (QKD) and post-quantum methods to protect sensitive data from quantum threats, like securing supply chain communications between suppliers and logistics providers in CIoT networks.
- Enhances encryption for CIoT networks using Elliptic Curve Cryptography (ECC), ensuring secure, efficient communication in resource-constrained devices like wearable medical equipment.

E. Paper Organization

In this section, the organization of the paper is outlined. The rest of the paper is organized as follows: Section II provides a comprehensive review of existing research and developments related to blockchain security, quantum computing, and their integration with a particular focus on Consumer IoT (CIoT) networks. Section III details the objectives to enhance CIoT security by developing quantum-resistant protocols and techniques that address quantum computing threats. Section IV describes the methodologies used, including the Quantum Currency Security Protocol, Distributed Ledger Data Blocks, Quantum Ledger Verification using Quantum Cryptography, Quantum Solutions for Middleman Attacks,

and ECC-Integrated Security Measures. Section V presents the results obtained from integrating cryptocurrency and blockchain with quantum technologies, emphasizing their scalability, reliability, and effectiveness in addressing the unique security needs of CIoT networks. Section VI concludes the key findings and highlights their implications for future blockchain and quantum security in Consumer IoT. Section VII discusses the challenges encountered during the research and outlines potential directions for future work, focusing on optimizing the proposed protocols for enhanced performance and broader applicability in quantum-resistant blockchain systems.

TABLE III: List of Abbreviations and their meanings used in the paper.

Abbreviation	Used Term
AES	Advanced Encryption Standard
AI	Artificial Intelligence
BB84	Bennett-Brassard 1984
BCT	Block Creation Time
BFT	Byzantine Fault Tolerance
CIoT	Consumer Internet of Things
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CPU	Central Processing Unit
DLTs	Distributed Ledger Technologies
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EdDSA	Edwards-Curve Digital Signature Algorithm
GDP	Gross Domestic Product
HSMs	Hardware Security Modules
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
MEC	Mobile-Edge Computing
NVMe SSD	Non-Volatile Memory Express Solid State Drive
NVIDIA H100	NVIDIA H100 Tensor Core Graphics Processing Unit
PKI	Public Key Infrastructure
PoS	Proof of Stake
PoW	Proof of Work
PUFs	Physically Unclonable Functions
QDS	Quantum Digital Signature
QEC	Quantum Error Correction codes
QKD	Quantum Key Distribution
QBIF	Quantum Blockchain Identity Framework
QIT	Quantum Identity Token
QRNG	Quantum Random Number Generators
QR-PoS	Quantum-Resistant Proof of Stake
QR-PoW	Quantum-Resistant Proof of Work
RAM	Ferroelectric Random Access Memory
RSA	Rivest–Shamir–Adleman
SCADA	Supervisory Control and Data Acquisition
SHA	Secure Hash Algorithm
SVP	Shortest Vector Problem
TLS	Transport Layer Security
ZKP	Zero Knowledge Proofs

II. Literature Survey

Integrating quantum blockchain into Consumer IoT networks offers a promising approach to enhance security through quantum-resistant cryptographic techniques and tamper-proof data management. This literature review explores existing research on the fusion of quantum blockchain technology with IoT networks, focusing on how it addresses critical security challenges such as authentication, data integrity, and scalability. Table VI shows a comparative analysis of several research papers focused on enhancing security and privacy in Consumer IoT (CIoT). It categorizes the papers based on specific technological approaches such as Blockchain Integration, Quantum Technology, Encryption Methods, and Post-Quantum Cryptography. It provides a clear overview of each paper's methodologies to address security challenges. Singamaneni *et al.* [6] introduced a multi-qubit Quantum Key Distribution (QKD) Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model to enhance cloud security for consumers. The proposed model demonstrated improvements in key generation rate and transmission distance, offering stronger encryption with minimal computational overhead for cloud environments. Awan *et al.* [8] proposed an AI-driven SDN architecture for Consumer IoT, incorporating Ubiquitous AI, Quantum-Inspired ML, and a Decentralized Trust Evaluation mechanism. The approach achieved detection accuracies of 98.5% for passive eavesdropping attacks and 95% for Sybil attacks. The model maintained low computational costs and high network throughput across different attack scenarios. Wang et al. [49] developed a blockchain-enabled decentralized edge intelligence framework for 6G consumer electronics, integrating edge servers and blockchain consensus. The proposed system achieved 96% offloading efficiency and low latency of 50ms across 2000 devices and 100 edge servers in simulations, highlighting its scalability and efficiency. Datta *et al.* [50] introduced a blockchain-based smart contract model for securing healthcare transactions using consumer electronics and Mobile-Edge Computing (MEC). Their approach utilized AES, RSA, EdDSA, and ECDSA for encryption, achieving high security and scalability. Experimental results showed the proposed scheme's better efficiency in communication cost and processing time compared to existing models. Ayub *et al.* [51] developed a secure, consumer-centric demand response management protocol for resilient smart grids using blockchain-based authentication. Their protocol incorporates Physically Unclonable Functions (PUFs) to prevent physical attacks, ensuring privacy and security for consumer IoT devices. The method showed lower computation and communication costs than similar protocols, making it an efficient solution for Industry 5.0 applications. Wu *et al.* [52] presented state-of-the-art research opportunities for next-generation consumer electronics, emphasizing IoT standardization (IEEE 2668) and cybersecurity. Their work proposed a comprehensive framework for enhanced interoperability and security in consumer IoT systems, showcasing potential research directions like complex network analysis for improved device reliability and network performance. Peelam *et al.* [53] explored quantum computing applications for IoT, focusing on network optimization, quantum-secured IoT, and quantum sensors. Their approach, which employed quantum algorithms like Grover's and Shor's, demonstrated improved IoT network efficiency and security performance, achieving enhanced data accuracy and optimization for industrial IoT environments. Balogh *et al.* [54] reviewed IoT security challenges, focusing on cloud and blockchain integration, post-quantum cryptography, and evolutionary techniques

TABLE IV: Comparative analysis of various Consumer IoT (CIoT) research papers, highlighting the various technological approaches and methodologies used for enhancing security and privacy.

Author Reference	BI	QT	CIoT	EM	SF	DP	QCS	LDB	LV	MAS	PQC
Singamaneni *et al.* [6]	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Awan *et al.* [8]	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗
Wang *et al.* [49]	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗
Datta *et al.* [50]	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗
Ayub *et al.* [51]	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗
Wu *et al.* [52]	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Peelam *et al.* [53]	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗
Balogh *et al.* [54]	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗
Aggarwal *et al.* [55]	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Yang *et al.* [44]	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Muralidharan *et al.* [56]	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗
Yu *et al.* [57]	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗
Proposed Paper	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

* Abbreviations: BI = Blockchain Integration, QT = Quantum Technology, CIoT = Consumer IoT, EM = Encryption Methods, SF = Security Features, DP = Data Privacy, QCS = Quantum Currency Security, LDB = Ledger Data Blocks, LV = Ledger Verification, MAS = Middleman Attack Solution, PQC = Post-Quantum Cryptography.

for securing consumer electronics. Their methodology employed evolutionary algorithms to address security issues, demonstrating improved attack detection in IoT networks while ensuring efficient computational performance. Aggarwal *et al.* [55] proposed a secure smart grid authentication system by integrating Quantum Key Distribution (QKD) and blockchain technology into Supervisory Control and Data Acquisition (SCADA) systems for consumer electronics. Their approach demonstrated improved data integrity and lower computational overhead, with simulations significantly enhancing throughput and system security. Yang *et al.* [44] conducted a theoretical analysis on quantum blockchain for decentralization, focusing on quantum identity authentication using quantum Public Key Infrastructure (PKI). Their work introduced the Quantum Blockchain Identity Framework (QBIF) to address identity management challenges in consumer IoT, demonstrating enhanced security against quantum attacks and offering a decentralized solution for user authentication. Muralidharan *et al.* [56] introduced a decentralized ME-centric framework for consumer IoT, integrating edge computing, decentralized storage, and blockchain to enhance scalability and security. Their model demonstrated improved latency and data privacy, addressing interoperability challenges in CIoT systems. Yu *et al.* [57] proposed a blockchain-based Shamir's threshold cryptography scheme for data protection in Industrial IoT (IIoT) settings. The approach integrates edge computing and blockchain to enhance security by decentralizing key storage. Their model demonstrated significant data confidentiality and integrity improvements, with efficient key reconstruction and encryption performance. The Black Bird 51% attack becomes dangerous in quantum computing because it exploits the majority control of a blockchain network's hashing power, denoted as $P \geq 0.51$ [58]. In classical systems, this attack allows a malicious actor to double-spend or reverse transactions by re-mining blocks faster than honest nodes. Quantum computing, with its ability to factor large integers efficiently (e.g., Shor's algorithm for breaking RSA), can solve complex hash functions faster, reducing the time complexity from $O(2^n)$ to $O(n^2)$, where n represents the number of qubits used. This means the time needed to gain 51% control and re-mine blocks could drastically decrease [29]. Using quantum-resistant encryption schemes like lattice-based cryptography or Elliptic Curve Cryptography (ECC) adapted for quantum environments could counteract this by ensuring the cryptographic primitives remain secure even against quantum-based threats [19]. Integrating such quantum-resistant algorithms ensures that the blockchain maintains its security by keeping the computational difficulty of controlling 51% intact, despite quantum advancements. Quantum computing poses significant challenges to distributed sensor networks and cryptocurrencies [59]. In distributed sensor networks, quantum algorithms can break traditional encryption, compromising data integrity and secure communication [60]. For cryptocurrencies, quantum computers threaten the security of cryptographic methods like Elliptic Curve Cryptography (ECC), making wallets vulnerable to theft and enabling faster 51% attacks (as shown in Table V) that disrupt transaction consensus. These challenges necessitate the adoption of quantum-resistant algorithms to secure blockchain applications in these fields. Table V shows a comparative analysis of PoW and PoS under quantum threats, highlighting key factors such as attack difficulty, block time impact, energy consumption, and network scalability. It illustrates how PoS is generally more resilient to quantum attacks due to lower reliance on computational puzzles and faster adaptability to quantum-resistant cryptographic solutions.

III. Aims And Objective

The paper aims to explore the integration of quantum computing with blockchain technology in Consumer IoT networks, focusing on enhanced security and efficiency. It examines Quantum Currency with public keys, aims to improve cryptocurrency transactions, and reduces quantum attacks. It covers Quantum Verification of Ledger using

TABLE V: Comparison of Proof of Work (PoW) and Proof of Stake (PoS) under Quantum Threats.

Factor	Proof of Work (PoW)	Proof of Stake (PoS)
51% Attack Difficulty [61]	Requires 1.5–2.5 exahashes/second of hashing power	Requires control of 30M–50M tokens in stake (depends on network size)
Block Time Impact under Quantum Threat [62]	30% reduction in block creation time	Minimal change (3%-5% reduction in block time)
Transaction Finality Time [63]	10 minutes per block, can reduce to 6–7 minutes	2–5 seconds per block, no significant change
Energy Consumption [64]	70 TWh/year	90% lower than PoW (2–5 TWh/year)
Quantum-Resistant Cryptography Integration Time [65]	3–5 years for transition to quantum-safe algorithms	1–2 years for transition due to flexible architecture
Consensus Algorithm Impact [64]	Mining difficulty may be affected by faster quantum mining	Stake validation remains secure with minor vulnerabilities
Network Scalability under Quantum Threat [65]	TPS may reduce from 7 to 5 TPS	Minimal TPS impact, remains at 1,000–10,000 TPS
Attack Surface for Quantum Mining [65]	High vulnerability due to reliance on SHA-256	Lower vulnerability, less dependent on computational puzzles

Quantum Cryptography to develop robust cryptographic techniques that ensure blockchain integrity. It proposes solutions for Middle Man Attacks in Blockchain, addressing intermediary vulnerabilities. The integration of Quantum Security and Privacy measures is investigated to enhance transaction confidentiality in the presence of quantum threats. It uses the application of Elliptic Curve Cryptography (ECC) in quantum blockchain for its effectiveness in quantum-resistant cryptographic algorithms. To maintain the relationships and connections between the various components used in the paper, the Quantum Currency Security Protocol worked alongside Distributed Ledger Data Blocks to secure transaction validation and storage. Quantum Ledger Verification further enhanced the authentication and validation of these transactions [66]. The Quantum Solutions for Middleman Attacks provided additional protection against unauthorized access, reinforced by the Quantum Security and Privacy Measures to secure sensitive information [67]. ECC-Integrated Security Measures ensured efficient encryption, maintaining the system's performance across all components [68].

The following points show the aims and objectives of the proposed methodology, highlighting the relationships and connections between the various components used in the methodology section.

- Proposed a **Quantum Currency Security Protocol** to enhance the security of cryptocurrency transactions by utilizing quantum-resistant cryptographic algorithms, ensuring secure data transfer within Consumer IoT networks.
- Designed **Distributed Ledger Data Blocks** that improved transactions' transparency, scalability, and data integrity, ensuring each transaction was securely validated and added to the blockchain without vulnerabilities.
- Implemented **Quantum Ledger Verification** uses quantum cryptographic techniques to authenticate and ensure generating unique key pairs, encrypting transactions, and utilizing changes.
- Proposed **Quantum Solutions for Middleman Attacks** that leveraged quantum principles like entanglement and superposition to prevent unauthorized interception and transaction manipulation, safeguarding the blockchain's data flow.
- Integrated **Quantum Security and Privacy Measures** within the blockchain to enhance confidentiality and safeguard sensitive information against quantum-enabled cyber threats, ensuring the long-term security of Consumer IoT networks.
- Applied **Elliptic Curve Cryptography (ECC)-Integrated Security Measures** to improve encryption efficiency and data protection in Consumer IoT devices, enabling lightweight cryptographic solutions that support secure communication and data transfer across constrained environments.

IV. Methodology

This section explores several quantum-based methodologies for securing Consumer IoT networks. First, we discuss the Quantum Currency Security Protocol, which provides a robust framework for digital transactions within consumer IoT networks. Next, we address the utilization of Distributed Ledger Data Blocks, which are crucial for maintaining the integrity and transparency of transactions. Quantum Ledger Verification, underpinned by quantum cryptography, enhances the accuracy and security of ledger verification processes. We also examine quantum solutions designed to counteract middleman attacks in blockchain systems, a critical aspect of maintaining trust in digital communications. The role of quantum security and privacy measures in blockchain technology is highlighted to reinforce the further protection of sensitive information. Elliptic Curve Cryptography (ECC) is also considered for its efficiency and strength in encryption, complementing the aforementioned techniques in ensuring a secure consumer IoT network.

A. Quantum Currency Security Protocol in Consumer IoT Networks

The integration of quantum technology into blockchain at the cryptocurrency level can be facilitated by referencing various quantum cash schemes developed since the 1960s [69]. Quantum currency employing public keys explores superposition to prevent unauthorized replication of quantum states used as coins. This security stems from the inability of

attackers to ascertain the cryptographic keys used to construct these states, thereby thwarting attempts to measure each qubit in the correct basis [70]. Stephen Wiesner initially proposed the concept of generating public-key quantum money in 1960 [71]. The Quantum Currency Security Protocol (QCSP) ensures secure quantum-resistant currency transactions by generating unique key pairs, encrypting transactions, and utilizing quantum-resistant consensus mechanisms for validation and blockchain integration. It introduces public-key quantum money to enhance asset security within consumer IoT networks. QCSP utilizes QKD and quantum-secure digital signatures to enhance the security of digital transactions. QCSP first establishes a secure quantum channel between the sending device U_i and the receiving device U_j using QKD to initiate a transaction in a consumer IoT network. This process generates a pair of quantum keys: QK_{pub_i} (public quantum key of U_i) and QK_{priv_i} (private quantum key of U_i). Simultaneously, a shared secret key K_{ij} is established between U_i and U_j. Once the quantum channel is established, U_i initiates a transaction by preparing a message M containing transaction details such as the amount (Amount), sender's address (SenderAddress), recipient's address (RecipientAddress), and timestamp (Timestamp). This message M is hashed using a quantum-secure hash function to produce $H(M)$:

$$H(M) = \text{HashFunction}(M) \tag{13}$$

U_i signs $H(M)$ using their private quantum key QK_{priv_i}, resulting in a digital signature S_i:

$$S_i = \text{Sign}(QK_{priv_i}, H(M)) \tag{14}$$

The signed message (M, S_i) is transmitted to U_j over a classical communication channel. Upon receiving (M, S_i), U_j verifies the authenticity of the transaction by using QK_{pub_i} to verify S_i and ensure that M has not been tampered during transmission:

$$\text{Verification}(QK_{pub_i}, M, S_i) \rightarrow \{\text{True}, \text{False}\} \tag{15}$$

If the verification is successful (Verification = True), U_j proceeds with the transaction; otherwise, it rejects the transaction. To ensure the integrity and authenticity of the transaction, U_i generates an authentication token T using the shared secret key K_{ij} and sends it along with the signed message (M, S_i) to U_j. U_j validates T using K_{ij} to confirm that the message originated from U_i and has not been altered:

$$T = \text{AuthenticationToken}(K_{ij}) \tag{16}$$

$$\text{ValidateToken}(T, K_{ij}) \rightarrow \{\text{True}, \text{False}\} \tag{17}$$

The Quantum Currency Security Protocol is described in Algorithm 1. It uses unique key pairs, encryption, and strong validation mechanisms to protect quantum-resistant currency transactions in consumer IoT networks. By integrating public-key quantum money, QCSP strengthens asset security, incorporating measures to defend against quantum threats in digital currency transactions

Algorithm 1 Quantum Currency Security Protocol in Consumer IoT Networks

Input: Transaction message M, Quantum key pair $(QK_{pub_i}, QK_{priv_i})$, Shared secret key K_{ij}
Output: Transaction confirmation or rejection
Function QuantumCurrencySecurityProtocol(M, QK_{pub_i}, QK_{priv_i}, K_{ij})
begin
  Establish quantum channel between U_i and U_j;
  Generate sequence of qubits $\{q_i\}$ with random basis;
  Transmit $\{q_i\}$ to U_j;
  U_j measures $\{q_i\}$ with random basis;
  Compare bases over classical channel;
  if *bases match* **then**
    $K_{ij} \leftarrow$ extract key from matching bits;
  else
    abort process and report error;
  $S_i \leftarrow$ QuantumSign(QK_{priv_i}, M);
  Send (M, S_i) to U_j;
  $verification\_status \leftarrow$ QuantumVerify(QK_{pub_i}, M, S_i);
  if $verification\_status == True$ **then**
    proceed with transaction;
  else
    reject transaction;
  $T \leftarrow$ Generate authentication token using K_{ij};
  Send T along with the signed message;
  if *validate token* T *with* K_{ij} **then**
    confirm integrity and authenticity;
  else
    report tampering;
  return transaction confirmation or rejection;

B. Dual Authentication in Quantum Currency Security Protocol

The Quantum Currency Security Protocol (QCSP) employs dual authentication using quantum public-private keys and quantum identity tokens to enhance security in CIoT networks [72]. This approach solves the vulnerabilities of single authentication, such as impersonation, quantum attacks (e.g., Shor's algorithm), and eavesdropping. In dual authentication, quantum keys and tokens are required for secure access, providing a quantum-resilient solution [73].

1) Basis of Dual Authentication: The Quantum Public-Private Key (QPK) system encrypts a message M using the public quantum key k_{pub}, and the encryption can be formulated as:

$$E_{QPK}(M) = M \otimes \langle k_{pub}|\psi\rangle \tag{18}$$

Where ψ represents the quantum state associated with the user. Due to the no-cloning theorem, any attempt to copy or measure $\langle k_{pub}|\psi\rangle$ disturbs the system, alerting legitimate parties of an attack. The Quantum Identity Token (QIT) is a unique quantum state $|QIT\rangle$ assigned to each user. Verification is conducted by measuring:

$$P_{verify}(|QIT\rangle) = 1 \text{ if valid, otherwise } 0 \tag{19}$$

Due to the uncertainty principle, an attacker cannot measure or replicate the token without disturbing it, leading to failed verification attempts.

Theorem: *In a Consumer IoT network, dual authentication with quantum public-private keys and quantum identity tokens*

guarantees secure communication, impersonation resistance, and robustness against quantum and classical attacks [74].
Proofs:

- ***Impersonation Resistance:*** Let the probability of success for an adversary attempting to impersonate a user be denoted by $P_{\text{impersonate}}$. In single authentication, this probability depends on successfully guessing or stealing the public-private key pair:

$$P_{\text{single}} = P(\text{break QPK}) \tag{20}$$

The adversary must break the QPK system and replicate the QIT state for dual authentication. The total probability of success is:

$$P_{\text{dual}} = P(\text{break QPK}) \times P(\text{break QIT}) \tag{21}$$

Given that both probabilities are exponentially small due to quantum mechanics:

$$P(\text{break QPK}) \approx \frac{1}{2^n}, \quad P(\text{break QIT}) \approx \frac{1}{2^m} \tag{22}$$

Where n and m represent the security parameters (number of qubits), we have:

$$P_{\text{dual}} = \frac{1}{2^n} \times \frac{1}{2^m} = \frac{1}{2^{n+m}} \tag{23}$$

Thus, the adversary's probability of success in impersonation is exponentially smaller with dual authentication than with single authentication.

- ***Resistance to Quantum Attacks:*** Classical encryption schemes are vulnerable to quantum attacks, such as Shor's algorithm, where the probability of success is high [75]:

$$P_{\text{Shor}} \approx 1 \tag{24}$$

Quantum public-private key encryption relies on quantum superposition and entanglement, which are not affected by Shor's algorithm [29]. The probability of successfully breaking a quantum public-private key system is negligible:

$$P(\text{break QPK with Shor}) \approx 0 \tag{25}$$

To break dual authentication, the adversary must also replicate the quantum identity token, which is again protected by the no-cloning theorem:

$$P(\text{break QIT}) \approx 0 \tag{26}$$

Thus, the total probability of breaking the system through quantum attacks is:

$$P_{\text{quantum attack}} = P(\text{break QPK}) \times P(\text{break QIT}) \approx 0 \tag{27}$$

- ***Security:*** The security of dual authentication defined as:

$$P_{\text{success}} = P(\text{break QPK}) \times P(\text{break QIT}) = \frac{1}{2^{n+m}} \tag{28}$$

The security parameters are where n and m. Therefore, the system's security is exponential for the size of the quantum keys and tokens [76]. This probability becomes negligibly small for practical values of n and m, making dual authentication exponentially more secure than single authentication.

$$P_{\text{success}} = \frac{1}{2^{n+m}} \approx 0 \tag{29}$$

Thus, dual authentication ensures that both the QPK and QIT components are required for successful authentication, and breaking both is computationally infeasible, even for quantum computers [77].

C. Distributed Ledger Data Blocks for Consumer IoT Networks

Blockchain technology faces significant challenges related to scalability, efficiency, and sustainability. Addressing these concerns is crucial for blockchain to become a responsible and widely adopted technology. These issues could be solved with the advent of practical quantum computers, allowing blockchain to be used extensively in mission-critical applications in sectors such as banking and consumer electronics [78]. Quantum computing not only promises solutions to existing blockchain problems but also has the potential to enhance the implementation of blockchain technologies, including cryptocurrencies [18]. In a blockchain-based consumer IoT, the distributed ledger maintains the ownership and status of all devices and transactions [79]. This ledger is composed of a chain of blocks, where each block references its predecessor. The header of each valid block contains a hash H of the previous block in the chain. Typically, each block includes a timestamp T, a nonce N, and a list of transactions *Txns*. When a transaction occurs in this network, the current state of the ledger is updated by a function Calculate that takes the initial state S_0 and the transaction *Txn* and returns the next state S_1 or an error Err. This can be expressed mathematically as:

$$\text{Calculate}(S_0, \mathit{Txn}) = \begin{cases} S_1 & \text{if the transaction is valid} \\ \text{Error} & \text{if the transaction is invalid} \end{cases} \tag{30}$$

Each block B_i in the blockchain can be represented as:

$$B_i = \{H_{i-1}, T_i, N_i, \mathit{Txns}_i\} \tag{31}$$

where H_{i-1} is the hash of the previous block B_{i-1}, ensuring the integrity of the chain. The hash function H can be defined as:

$$H_i = \text{Hash}(B_i) = \text{Hash}(H_{i-1}, T_i, N_i, \mathit{Txns}_i) \tag{32}$$

The state transition function can be represented as:

$$S_{t+1} = \text{Calculate}(S_t, \mathit{Txn}_t) \tag{33}$$

This equation illustrates how the state of the ledger S_t at time t is updated to S_{t+1} after processing the transaction Txn_t. A consensus algorithm such as Proof of Work (PoW) or Proof of Stake (PoS) is used to ensure consensus across the network. For PoW, miners solve a computationally intensive puzzle, which can be represented as:

$$H(B_i) < \text{Target} \tag{34}$$

Where the target is a value that adjusts the puzzle's difficulty, for PoS, the probability of validating the next block depends on the validator's stake in the network. Fig. 4 shows the structure of the distributed ledger data blocks in a blockchain-based consumer IoT network.

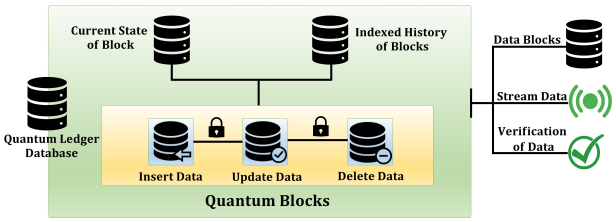

Fig. 4: Blockchain cryptocurrency's distributed ledger data blocks.

D. Quantum Ledger Verification using Quantum Cryptography

Using quantum cryptography to verify ledgers significantly boosts the security and reliability of consumer IoT networks [80]. Quantum cryptography relies on unique properties of quantum mechanics, such as entanglement and superposition, to create highly secure and tamper-resistant transactions [81]. For example, entangled photon pairs securely share cryptographic keys in QKD. The state of an entangled photon pair can be represented as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{35}$$

This equation shows that the photons are linked, so any attempt to intercept them will disrupt their state, alerting the parties involved. Quantum cryptography verifies ledger entries, ensuring each transaction remains unaltered and trustworthy. For a transaction T, its verification is:

$$V(T) = H(T) \oplus K_q \tag{36}$$

Here, $H(T)$ is a hash function applied to the transaction, and K_q is a quantum key. The result $V(T)$ confirms that only authenticated transactions, verified by quantum keys, are recorded on the ledger. This quantum-enhanced verification ensures the privacy and integrity of ledger data, leading to more secure and decentralized systems in our increasingly digital world. Algorithm 2 utilizes quantum computing and cryptography to authenticate ledger transactions. It employs superposition ($|L\rangle = \alpha|0\rangle + \beta|1\rangle$) and measurement ($P(r = 0) = |\alpha|^2$) techniques, alongside entanglement ($|\psi\rangle = |L\rangle \otimes |V\rangle$) for enhanced security. Quantum error correction and key distribution ensure ledger integrity. Output is determined by the measurement outcome (r) and can be either "Authentic (1)" or "Not Authentic (0)". This algorithm is vital for secure financial record-keeping in quantum computing environments.

E. Quantum Solution for Middleman Attack in Blockchain

Blockchain, a distributed ledger, allows trustless parties to transact without a centralized intermediary [82], and is

Algorithm 2 Quantum Ledger Verification Protocol

Input: Ledger state L, quantum computing system with N qubits, quantum cryptographic keys
Output: Verification result (Authentic (1) or Not Authentic (0))
Step 1: Initialize Quantum Ledger Parameters
begin
  foreach *transaction* T **do**
    Generate a unique public-private key pair (PK_T, SK_T) for the sender;
    Encrypt T using a quantum-resistant algorithm E with PK_T;
    Ciphertext_C $\leftarrow E(T, PK\_T)$;
    Attach PK_T to T;
Step 2: Quantum Superposition
begin
  Prepare the ledger state L in a quantum superposition:
  $$|L\rangle = \alpha|0\rangle + \beta|1\rangle$$
  where $|0\rangle$ and $|1\rangle$ represent computational basis states, and α and $\beta \in \mathbb{C}$ are complex probability amplitudes with normalization:
  $$|\alpha|^2 + |\beta|^2 = 1$$
Step 3: Quantum Measurement
begin
  Apply Hadamard gate H to transform the ledger state into superposition:
  $$|L'\rangle = H|L\rangle = \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{2}}$$
  Perform quantum measurement on $|L'\rangle$ in the computational basis, yielding probabilities:
  $$P(r=0) = |\langle 0|L'\rangle|^2 = \frac{|\alpha|^2}{2}, \quad P(r=1) = |\langle 1|L'\rangle|^2 = \frac{|\beta|^2}{2}$$
Step 4: Quantum Entanglement
begin
  Entangle the ledger state with verification qubits $|V\rangle$.
  The combined system is now in the state:
  $$|\psi\rangle = |L\rangle \otimes |V\rangle = \alpha|0\rangle_L \otimes |0\rangle_V + \beta|1\rangle_L \otimes |1\rangle_V$$
  This establishes an entangled state between the ledger qubits and verification qubits.
Step 5: Quantum Cryptographic Checks
begin
  Apply Quantum Error Correction codes (QEC) to detect and correct errors in the ledger state;
  Use quantum entanglement swapping to facilitate secure communication;
  Perform QKD using protocols like BB84 to verify the authenticity of the ledger;
Step 6: Quantum Verification
begin
  Measure the verification qubits $|V\rangle$ to obtain the final result. The quantum system collapses into a classical state.
Step 7: Quantum Ledger Verification
begin
  if *verification qubits collapse to* $|0\rangle$ **then**
    Output: "Ledger is Authentic (1)";
  else
    Output: "Ledger is Not Authentic (0)";

characterized by its immutability, unforgeability, traceability, transparency, and security. These features are underpinned by public-key cryptography, whose security traditionally hinges on the computational difficulty of specific problems. With the rise of quantum computing, concerns have emerged regarding the security of blockchain systems based on traditional public-key cryptosystems. The resilience of blockchain against quantum computational threats is paramount [20]. Quantum-resistant public-key cryptosystems, particularly lattice-based cryptosystems, have gained attention. These cryptosystems are currently invulnerable to known quantum algorithms, providing a robust defense against

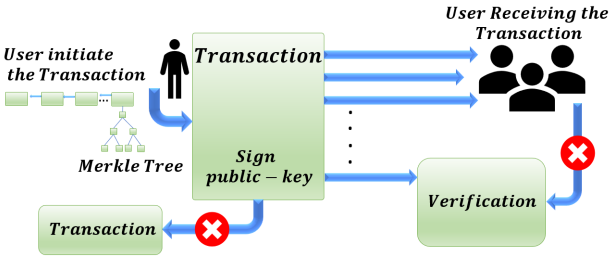

Fig. 5: Secure data management in consumer IoT networks with quantum ledger database.

quantum attacks. Lattice-based cryptosystems often require larger key sizes and signatures [83]. Quantum encryption has become crucial for blockchain technology in consumer IoT networks, protecting against middleman attacks by using the principles of quantum mechanics to create unbreakable cryptographic keys. This ensures the integrity and confidentiality of blockchain transactions, as illustrated in Fig. 5. A quantum solution is proposed to enhance blockchain security against middleman attacks. Algorithm 3 shows the quantum principles to protect blockchain transactions. It employs a quantum circuit with n qubits, where n corresponds to the blockchain transaction length. The algorithm initializes these qubits and applies quantum gates like X and Hadamard to create an entangled state, subsequently measuring the qubits. By checking the measurement outcomes for any result other than '0'$*n$ and '1'$*n$, the algorithm detects potential middleman attacks, enhancing transaction security. The quantum circuit U_{entangle} applies the Hadamard gate H to each qubit, creating an entangled state as:

$$H^{\otimes n} |0\rangle^n = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \,. \tag{37}$$

Following entanglement, the measurement operation U_{measure} collapses the state $|\psi\rangle$ to a classical bitstring, verifying outcomes to detect anomalies. This approach is summarized as follows:

$$|\psi\rangle = \sum_{i,j=0}^{1} \alpha_{ij} |i\rangle |j\rangle \,, \tag{38}$$

Deviations from the expected patterns of '0'$*n$ and '1'$*n$, where '0'$*n$ represents a string of zeros and '1'$*n$, a string of ones, serve as signals for potential tampering. This mechanism enhances the security of blockchain transactions against threats posed by quantum-enabled technologies.

F. Quantum Security and Privacy used in Blockchain

Quantum security and privacy are essential for enhancing secure consumer IoT networks by addressing inherent vulnerabilities [84]. According to quantum physics principles, quantum technology ensures privacy and resolves safety issues in conventional network systems [67]. For instance, the QKD protocol enables devices to share information securely,

Algorithm 3 Quantum Middleman Attack Resilient Transaction (QMART) Protocol

Input: Blockchain Transaction (blockchain_transaction)
Output: Security Result (Security_Result)
Function QMART Protocol(blockchain_transaction)
begin
  $n \leftarrow$ length of blockchain_transaction;
  Quantum_Circuit $\leftarrow$ QuantumCircuit(n, m);
  foreach $i \in \{0, 1, \ldots, n-1\}$ **do**
    if *blockchain_transaction*$[i] =' 1'$ **then**
      Apply X gate to Quantum_Circuit at qubit i;
  foreach $i \in \{0, 1, \ldots, n-2\}$ **do**
    Apply H gate to Quantum_Circuit at qubit i;
    Apply CNOT gate to Quantum_Circuit from qubit i to $i+1$;
  Result $\leftarrow$ execute(Quantum_Circuit, backend, shots $= 1$);
  Counts $\leftarrow$ Result.get_counts();
  if *length of Counts* $= 1$ *and '1'* $\times nin Counts$ **then**
    Security_Result $\leftarrow$ *"Middleman attack detected! Transaction compromised.";*
  else
    Security_Result $\leftarrow$ *"Transaction secure. No middleman attack detected.";*
  return Security_Result;

utilizing the Heisenberg uncertainty principle as follows:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \tag{39}$$

Where Δx and Δp represent uncertainties in position and momentum, and $\hbar$ is the reduced Planck's constant. This principle guarantees that any eavesdropping attempt will introduce detectable disturbances. The Quantum Digital Signature (QDS) [85] mechanism replaces the elliptic curve-based conventional digital signature technique. Traditional signature is represented as:

$$s = k^{-1}(H(m) + r \cdot d_A) \mod n \tag{40}$$

Where s is the signature, k is a random integer, $H(m)$ is the hash of the message, r is part of the signature, d_A is the private key, and n is the order of the curve, are vulnerable to quantum attacks. QDS, rooted in quantum superposition and entanglement, is described as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{41}$$

where $|\psi\rangle$ is the quantum state, and α and β are complex probability amplitudes of states $|0\rangle$ and $|1\rangle$, provides a more secure alternative as it can only be tampered with by the owner. Implementing quantum-resistant algorithms is crucial, as classical cryptographic methods like RSA are based on the difficulty of factoring large integers.

$$N = pq \tag{42}$$

Where p and q are primes, they are susceptible to quantum attacks via Shor's algorithm. Quantum algorithms can factorize N exponentially faster than classical algorithms, posing a significant threat. Lattice-based cryptography, which relies on hard problems like the Shortest Vector Problem (SVP) in high-dimensional lattices, is preferred for its resilience against quantum computing capabilities. Quantum Random

Number Generators (QRNG) use the inherent unpredictability of quantum phenomena to produce true random numbers, essential for encryption keys [86]. This unpredictability is mathematically grounded in quantum mechanics, ensuring non-replicable randomness for secure key generation. To quantify the security enhancements brought by quantum technology, we introduce the quantum security factor Q, defined as:

$$Q = \frac{1}{2}(\alpha + \beta) \tag{43}$$

Where α represents the classical security parameter, and β is the quantum enhancement coefficient. This equation highlights the relation between classical and quantum security measures. Quantum entanglement in secure communication channels allows the implementation of quantum teleportation protocols [87], represented as:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \tag{44}$$

Where $|\psi\rangle_{AB}$ denotes an entangled state shared between devices A and B. This entanglement ensures that any change in one part of the system instantaneously affects the other, providing a secure method for transmitting information. Quantum teleportation for consensus in blockchain explores the security of quantum cryptography, primarily utilizing entanglement and the no-cloning theorem. For example, if two smart consumer electronics devices share an entangled pair $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, any measurement on one device affects the state of the other [88, 89]. If an eavesdropper attempts to intercept, the state collapses, violating the superposition principle, as the no-cloning theorem $|\phi\rangle \neq |\psi\rangle$ prevents duplicating unknown quantum states. QKD based on the BB84 protocol uses the polarization of photons, represented by states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, ensuring only the intended devices share the key. Any interception alters the measurement outcomes due to Heisenberg's uncertainty principle $\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$, thus guaranteeing secure transmission and consensus in blockchain networks [90]. Transitioning to quantum-based security mechanisms secures consumer IoT networks against future quantum computing threats, ensuring long-term security [91, 92]. Quantum cryptographic techniques offer a level of security unattainable by classical methods, addressing emerging vulnerabilities and enhancing the resilience of interconnected devices. This comprehensive security framework is vital for protecting sensitive information and maintaining the integrity of consumer IoT networks in an increasingly complex digital landscape.

G. Elliptic Curve Cryptography (ECC)-Integrated Security Measures in Consumer IoT Networks

ECC is essential in consumer electronics networks to provide robust security and efficient performance [93, 94]. Unlike traditional algorithms like RSA, ECC achieves comparable security with much smaller key sizes, translating to faster computation and reduced storage requirements crucial for resource-constrained devices [95]. ECC is based on the complex mathematics of elliptic curves, making it challenging for attackers to decipher encrypted data without the private key [96, 97]. This high level of security and efficiency ensures that sensitive data transmitted between devices, such as personal information or financial transactions, remains protected against unauthorized access while minimizing the impact on device performance and battery life. It is asymmetric public key cryptography based on the properties of a particular type of equation based on a mathematical group. Vector Miller and Neal Koblitz proposed the cryptographic use of Elliptic curves as shown in Fig. 6. In 1985 [98], Lenstra's elliptic curve factoring algorithm used ECC. In consumer IoT, ECC is a highly efficient method for securing device communications, serving as a robust alternative to the RSA algorithm. ECC provides comparable security with much smaller key sizes, essential for devices with limited computational resources. This efficiency is due to the elliptic curve equation:

$$y^2 = x^3 + ax + b \tag{45}$$

Here, the curve is symmetric about $y = 0$ because the values of x are $\pm$. The elliptic curve is denoted as $E_p(a, b)$, where a and b are restricted by the modulo p operation, with p being a prime number. Given a point P on the curve and a scalar k, the corresponding point $Q = kP$ can be computed efficiently. If P and Q are known, determining k is computationally challenging due to the discrete logarithmic problem. To facilitate secure communications between devices, Algorithm 4 generates public and private keys. In this algorithm, "nA" and "nB" denote the private keys for devices A and B, "G" is a fixed generator point on the elliptic curve, and "n" is a prime constant. The algorithm computes the public keys "PA" and "PB" by multiplying the private keys with the generator point G. It then derives the secret keys "kA" and "kB" through additional operations on these public keys, thereby providing the cryptographic keys necessary for secure message encryption and decryption between devices.

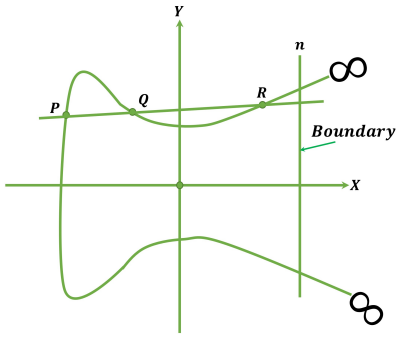

Fig. 6: Elliptic Curve Cryptography illustrating secure operations and boundary limits in consumer IoT.

1) Encryption of Elliptic Curve: Let the message M be encrypted on ECC by the point Pm and let a random positive integer k for encryption. Then, the cipher point sent to the receiver is Cm.

$$Cm = \{k * tG, Pm * PB\} \tag{46}$$

Algorithm 4 Elliptic Curve Key Generation and Secret Key Computation for Secure Electronic Devices

Input: Private key for Device A (n_A), Private key for Device B (n_B), Generator point (G), Prime number (p)
Output: Public key for Device A (P_A), Public key for Device B (P_B), Secret key for Device A (k_A), Secret key for Device B (k_B)
Function EllipticCurveKeyGenerationAndSecretKeyComputation(n_A, n_B, G, p)
begin
Step 1: Generate Public Keys
$P_A \leftarrow n_A \cdot G \mod p$;
$P_B \leftarrow n_B \cdot G \mod p$;
Step 2: Generate Secret Keys
$k_A \leftarrow n_A \cdot P_B \mod p$;
$k_B \leftarrow n_B \cdot P_A \mod p$;
Step 3: Return Values
return P_A, P_B, k_A, k_B;

2) Decryption of Elliptic Curve: For decryption, the receiver's secret key is multiplied by the value of the first coordinate point on ECC, that is: $nB * kG$ After that, it will be subtracted from the second coordinate in the pair.

$$Pm + k * PB - (kG * nB) \tag{47}$$

Since $PB = nB * G$, hence

$$Pm + k * PB - k * PB \tag{48}$$

So, the receiver gets the same point, which is Pm.

H. Elliptic Curve Cryptography (ECC) for Quantum Security in Consumer IoT Using Quantum Mathematics

ECC is widely used in resource-constrained environments like Consumer IoT due to its efficiency and smaller key sizes than traditional methods like RSA [93]. The emergence of quantum computers seriously threatens ECC's security, as quantum algorithms, such as Shor's algorithm, can efficiently solve the underlying Elliptic Curve Discrete Logarithm Problem (ECDLP) [99, 100]. By integrating ECC with quantum-resistant techniques and using principles of quantum mathematics, we can enhance its security against quantum attacks [101].

I. Elliptic Curve Cryptography for Quantum-Resilient Consumer IoT Networks

ECC is an efficient cryptographic solution for securing resource-constrained devices in Consumer IoT networks due to its smaller key sizes and robust security [101]. The advent of quantum computing presents significant challenges, as quantum algorithms, like Shor's algorithm, can efficiently break ECC by solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). To enhance ECC's resilience against quantum attacks, hybrid cryptographic schemes, which combine ECC with quantum-resistant algorithms, are essential for maintaining secure communications in Consumer IoT networks [93].

1) ECC in Quantum-Resilient System: ECC is based on the properties of elliptic curves over finite fields. The elliptic curve E over a finite field $\mathbb{F}_p$ is defined by the equation:

$$y^2 = x^3 + ax + b \pmod{p} \tag{49}$$

Where a and b are constants, and $4a^3 + 27b^2 \neq 0$ ensures that the curve has no singular points. The security of ECC arises from the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP): given points P and $Q = kP$, finding k is computationally infeasible for classical computers but is solvable using quantum computers with Shor's algorithm. In the quantum context, scalar multiplication on elliptic curves is represented using quantum superposition:

$$|kP\rangle = \sum_{k=0}^{n-1} \alpha_k |P\rangle \tag{50}$$

Where $|kP\rangle$ is the quantum state representing the result of scalar multiplication by k, and α_k are the corresponding probability amplitudes.

Theorem: *Let $E(\mathbb{F}_p)$ be an elliptic curve over a finite field, and $P \in E(\mathbb{F}_p)$ a generator of a cyclic subgroup of order n. ECC combined with quantum-resistant cryptographic techniques such as lattice-based cryptography to ensure quantum resilience, resulting in a hybrid cryptographic system that is secure against classical and quantum adversaries.*

Proofs:

- ***Classical Security of ECC*:** In classical cryptographic systems, the Elliptic Curve Discrete Logarithm Problem (ECDLP) remains difficult to solve using classical algorithms, such as Pollard's rho algorithm, which has complexity $O(\sqrt{n})$ [102]. This guarantees security against classical attackers.
- **Vulnerability to Quantum Attacks:** Shor's algorithm can solve the ECDLP in polynomial time $O((\log n)^2)$, making ECC vulnerable to quantum computing attacks [29]. Shor's algorithm utilizes quantum Fourier transforms and modular arithmetic to efficiently compute discrete logarithms, compromising ECC's security.
- **Hybrid Quantum-Resilient Approach:** To counter quantum threats, ECC is combined with quantum-resistant algorithms. One such method is lattice-based cryptography, which is resistant to quantum attacks [73]. The hybrid cryptographic scheme ensures that lattice-based components remain secure even if a quantum adversary breaks the ECC component. The encryption process for a message m using this hybrid scheme can be written as:

$$E_{\text{Hybrid}}(m) = E_{\text{ECC}}(m) \oplus E_{\text{Lattice}}(m) \tag{51}$$

  Where:
  - $E_{\text{ECC}}(m)$ represents encryption using Elliptic Curve Cryptography,
  - $E_{\text{Lattice}}(m)$ represents encryption using lattice-based cryptography.
- **Quantum Computation in ECC:** Quantum encryption processes in ECC involve the use of quantum gates for scalar multiplication [103]. The quantum state representing a point P on the elliptic curve evolves as follows:

$$U_{\text{ECC}}|P\rangle = |kP\rangle \tag{52}$$

  Here, U_{ECC} is a unitary operator representing scalar

multiplication in the elliptic curve group. Combining this with lattice-based cryptography ensures the cryptographic system is resilient to quantum attacks.

- **Quantum Resistance Against Attacks:** The hybrid approach ensures that the decryption process remains secure, even in the presence of quantum computers [104]. The decryption equation is given as:

$$m = D_{\text{Hybrid}}(c) = D_{\text{ECC}}(c_{\text{ECC}}) \oplus D_{\text{Lattice}}(c_{\text{Lattice}}) \quad (53)$$

Since no efficient quantum algorithm exists for breaking lattice-based cryptographic schemes, this ensures quantum resilience for Consumer IoT networks.

V. Result

In this section, we have summarized our work by combining cryptocurrency and blockchain with quantum technology. We have explored key areas such as using quantum methods for secure verification of transactions, designing quantum currency protocols with public keys, and using quantum solutions to protect blockchain systems from middleman attacks. We have also looked at ways to improve the security and performance of traditional blockchain systems using quantum technology. To ensure accurate results, we have conducted experiments on a high-performance setup with multi-core processors, 64GB of RAM, NVIDIA H100 Tensor Core GPUs, high-speed NVMe SSD storage, and specialized quantum simulation tools. This setup allowed us to test the impact of quantum solutions on blockchain security and performance. We have conducted a detailed Security Level Comparison of Cryptographic Algorithms in Pre-Quantum and Post-Quantum contexts using data from Google's Cirq and IBM's Qiskit simulators. Our Proposed Comparative Complexity Analysis of security protocols in Consumer IoT (CIoT) networks utilized these simulators to evaluate key performance metrics, including error rates and verification times. We analyzed the Comparison of Classical, Hybrid, and Quantum Blockchain Technologies by measuring attack success rates, verification time, error rates (bars), and privacy levels (line), using the outputs from Cirq and Qiskit to ensure accurate results. The performance metrics of quantum protocols across various security parameters were also assessed, providing valuable observations into CPU usage for classical versus post-quantum algorithms measured across different platform transaction rates. Our findings show that quantum technology enhances security and improves the efficiency of blockchain networks by reducing computational demands and enhancing encryption. The research highlights the practical use of quantum solutions to make blockchain systems more secure and efficient in the future. Fig. 7 illustrates the frequency distribution of various solved challenges within the field of quantum blockchain. Quantum Blind Signature and New Consensus techniques each account for 24.6% of the solved challenges, highlighting their significant roles in maintaining transaction anonymity and developing new consensus mechanisms suitable for quantum environments. Quantum Key Distribution follows with 19.3%, emphasizing

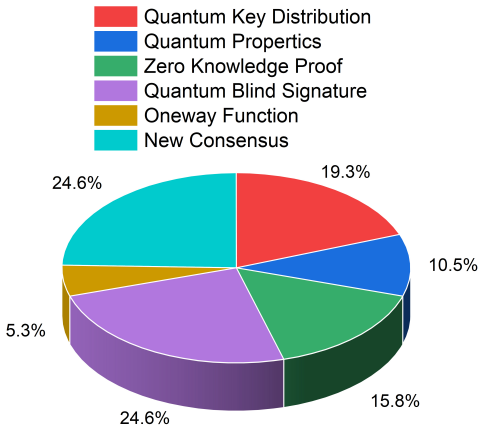

Fig. 7: Frequency Analysis of the Solved Challenges using Quantum Blockchain.

its importance in securing blockchain transactions through quantum-secured communication channels.The inclusion of real-world application data further validates the significance of these techniques, as demonstrated by the frequency analysis where Quantum Blind Signatures and New Consensus techniques account for 24.6% each, and Quantum Key Distribution (QKD) follows at 19.3%. In the consumer electronics industry, these techniques are essential for securing smart devices, particularly in secure communications and encrypted data transactions between IoT-enabled devices. This application data highlights how these methods are theoretically important and critical in ensuring consumer electronics' security and privacy, justifying their high usage percentages. Zero Knowledge Proofs (ZKP) contribute to 15.8% of the solutions, providing privacy-preserving verification methods. Quantum Properties are used in 10.5% cases to enhance blockchain protocols using superposition and entanglement. One-way Functions, essential for ensuring blockchain data's irreversible and secure hashing, make up 5.3% of the resolved challenges. This detailed frequency analysis provides insight into the specific areas within quantum blockchain where significant progress has been made in addressing technical challenges. Fig. 8 compares the security levels

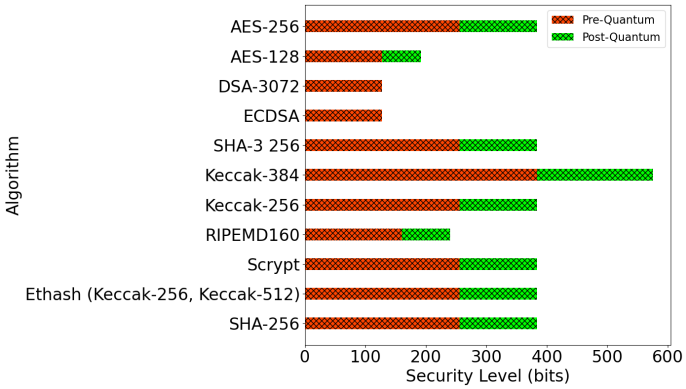

Fig. 8: Security Level Comparison of Cryptographic Algorithms in Pre-Quantum and Post-Quantum Contexts.

(measured in bits) of various cryptographic algorithms in pre- and post-quantum contexts. A significant increase in security levels is required for cryptographic algorithms to maintain their strength against quantum computing attacks. For instance, AES-256 and SHA-3 256 show substantial gains in their security levels in the post-quantum scenario, while algorithms like DSA-3072 and ECDSA maintain robust security even in quantum computing threats. In consumer IoT networks, the security level comparison shows significant improvements, especially using AES-256 and SHA-3 256. These encryption methods provide higher security when facing post-quantum threats. The move from 256-bit encryption to 512-bit encryption increases quantum protection. This stronger security comes with higher energy consumption and processing demands in smart devices, which can lead to increased resource use. Implementing such advanced encryption will require careful optimization to ensure that devices can handle these requirements without sacrificing performance or efficiency. This comparison highlights the importance of advancing cryptographic techniques to ensure data protection in the quantum computing era, especially for consumer IoT, which increasingly relies on secure communication and data storage. Table VI compares the time

TABLE VI: Proposed comparative complexity analysis of security protocols in Consumer IoT (CIoT) Networks.

Proposed Security Protocols	Time Complexity	Space Complexity
Quantum Currency Security Protocol	$O(nlogn)$	$O(n)$
Distributed Ledger Data Blocks	$O(n^2)$	$O(n)$
Quantum Ledger Verification	$O(n^2)$	$O(n)$
Quantum Solution for Middleman Attack	$O(nlogn)$	$O(n)$
Quantum Security and Privacy	$O(n^2)$	$O(nlogn)$
ECC-Integrated Security Measures	$O(nlogn)$	$O(n)$

and space complexities for different security protocols in the methodology section IV. The data have been taken from the proposed algorithms used in the papers, which discuss cryptographic techniques such as lattice-based cryptography, elliptic curve cryptography, and other quantum-resistant methods. These values reflect the computational requirements of each protocol as analyzed in these studies. Fig. 9 compares CPU usage across classical and post-quantum algorithms across different transaction rates. The plot demonstrates that post-quantum algorithms tend to have higher CPU usage, which is essential given the increasing complexity of securing consumer IoT networks. As quantum computing evolves, it threatens classical encryption methods, making it crucial to adopt quantum-resistant algorithms. This ensures that networks remain secure against future quantum attacks, protecting sensitive consumer data from potential breaches. The data on CPU usage and verification times highlights system efficiency, but its impact becomes more meaningful when applied to real-world CIoT networks. For instance, in a smart home network with devices like smart locks and cameras, lower CPU usage and faster verification ensure quick authentication, reducing latency and enhancing security

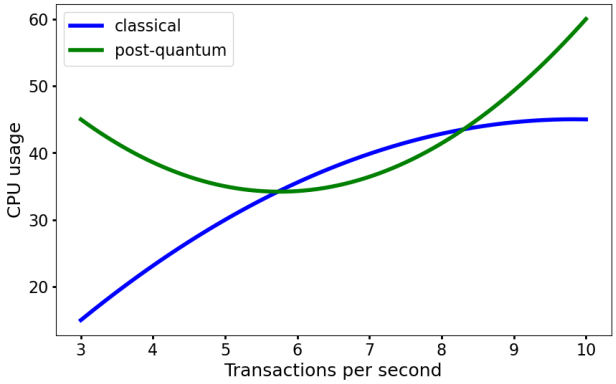

Fig. 9: Comparison of CPU usage for classical versus post-quantum algorithms across varying transaction rates.

and user experience in real-time applications. Fig. 10 shows

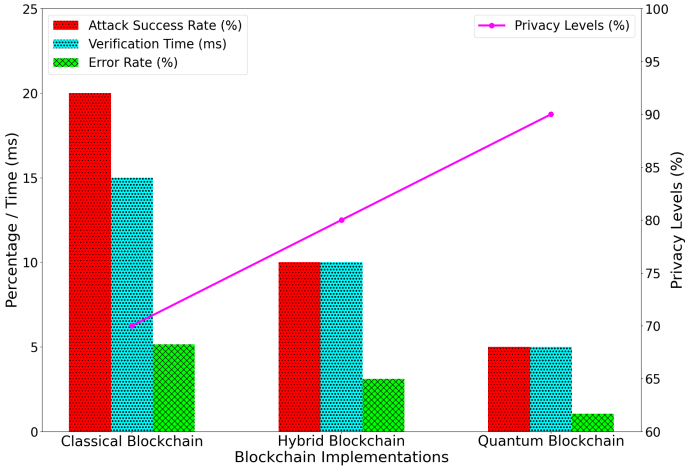

Fig. 10: Comparison of classical, hybrid, and quantum blockchain technologies showing attack success rate, verification time, error rate (bars), and privacy levels (line).

that quantum blockchain provides enhanced security in consumer IoT networks compared to classical and hybrid systems. Using QKD ensures that unauthorized access is detectable, reducing the attack success rate to 5% and achieving a verification time of 5 milliseconds. Quantum blockchain also has a lower error rate of 1.05%. It maintains a high privacy level of 90%, making it a robust solution for protecting sensitive data and securing networks against future cyber threats. The reduction in attack success rates to 5% and verification times to just 5 milliseconds in quantum blockchain offers significant improvements in security and speed for consumer IoT networks. These advancements allow for stronger protection against breaches and faster transaction processing, ensuring real-time operations and enhancing the performance of smart devices. This directly benefits CIoT environments by providing efficient, secure communication critical for the better functioning of interconnected devices in a quantum-resilient ecosystem. Fig. 11 shows a comparative analysis of four quantum security protocols in Secure Consumer IoT Networks, evaluating

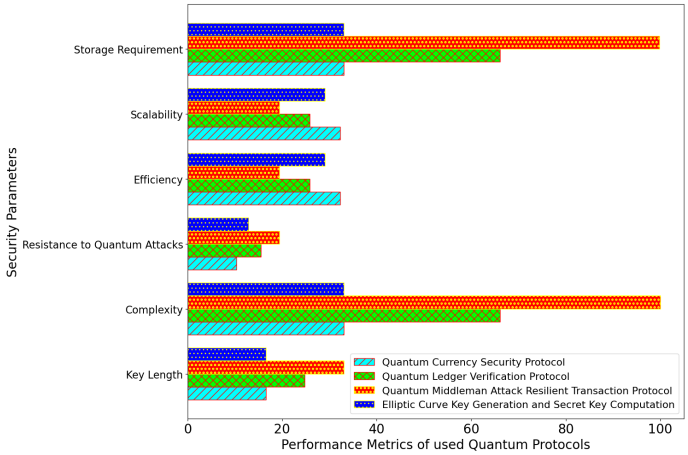

Fig. 11: Performance metrics of quantum protocols across different security parameters used for Quantum Blockchain in consumer IoT networks.

six key parameters: Key Length, Complexity, Resistance to Quantum Attacks, Efficiency, Scalability, and Storage Requirement. The Quantum Middleman Attack Resilient Transaction Protocol excels in Complexity (100%) and Resistance to Quantum Attacks (100%), making it highly robust. The Elliptic Curve Key Generation and Secret Key Computation show balanced performance, particularly in Efficiency (90%) and Scalability (90%), indicating versatility. The Quantum Currency Security Protocol is the most efficient (100%) and scalable (100%), suitable for high-performance needs. However, it has lower complexity (33%) and storage requirement (33%). This analysis helps identify protocols based on specific security and performance requirements, balancing high security and operational efficiency. The data was obtained through experiments using a Python script that generated numerical values for Key Length, Complexity, Resistance to Quantum Attacks, Efficiency, Scalability, and Storage Requirement and normalized these values for comparison.

VI. Conclusion

Integrating quantum computing with blockchain technology offers a transformative solution for enhancing the security and efficiency of consumer IoT networks. This paper highlights the potential of quantum-resistant cryptographic algorithms, including the Quantum Currency Security Protocol (QCSP) and Elliptic Curve Cryptography (ECC), to protect blockchain transactions against quantum attacks, ensuring the confidentiality, integrity, and availability of sensitive data. The practical benefits of CIoT networks include real-time data transmission between smart consumer devices, efficient resource management, and enhanced security against cyber threats. These networks support fast, reliable communication among interconnected devices, improving the user experience and ensuring smart devices operate smoothly with minimal delays and higher resilience to attacks. Quantum Ledger Verification and Quantum Middleman Attack Resilient Transaction Protocol improve the accuracy and security of ledger verification and transaction processes. By incorporating these quantum technologies into blockchain frameworks, we can significantly strengthen the resilience of consumer IoT networks, addressing critical security challenges and creating a more secure and reliable digital future. This comprehensive approach ensures that consumer IoT devices and data remain protected, leading to more robust and trustworthy platforms.

VII. Challenges and Future Research

Developing robust quantum-resistant algorithms remains a significant challenge as they must be secure against quantum attacks and efficient for practical use in consumer electronic networks [105]. Ensuring blockchain systems' high performance and scalability integrated with quantum-resistant mechanisms is crucial, as the computational overhead can impact transaction speeds and network efficiency. Achieving interoperability between existing classical and new quantum-enhanced systems is complex and essential for widespread adoption without disrupting current operations. The lack of standardization in quantum-resistant cryptographic protocols and blockchain frameworks can impede implementation and acceptance, making establishing widely accepted standards necessary [106]. Implementing these solutions can be resource-intensive and costly, posing financial and logistical challenges. Future research focused on optimizing quantum-resistant algorithms, developing efficient quantum consensus mechanisms, and validating these concepts through real-world implementations. Efforts should also be made to enhance interoperability, establish standards and best practices, and address cost and resource efficiency through innovative solutions. The following shows the potential future work:

- Optimize quantum-resistant algorithms to enhance their efficiency and security.
- Develop efficient quantum consensus mechanisms to accommodate the unique requirements of blockchain systems.
- Conduct experimental studies and real-world implementations to validate theoretical concepts and assess practical feasibility.
- Enhance interoperability between classical and quantum-enhanced systems.
- Establish standards and best practices for quantum-resistant blockchain implementations.
- Explore cost-effective solutions and resource-efficient approaches for implementing quantum-resistant blockchain systems.

References

[1] M. Möller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethics and information technology*, vol. 19, pp. 253–269, 2017.

[2] O. J. Unogwu, R. Doshi, K. K. Hiran, and M. M. Mijwil, "Introduction to quantum-resistant blockchain," in *Advancements in Quantum Blockchain With Real-Time Applications*. IGI Global, 2022, pp. 36–55.

[3] X. Lai, M. Lu, L. Qin, J. Han, and X. Fang, "Asymmetric encryption and signature method with dna technology," *Science China Information Sciences*, vol. 53, pp. 506–514, 2010.

[4] G. Shankar, L. H. Ai-Farhani, P. Anitha Christy Angelin, P. Singh, A. Alqahtani, A. Singh, G. Kaur, I. A. Samori *et al.*, "Improved multisignature scheme for authenticity of digital document in digital forensics using edward-curve digital signature algorithm," *Security and Communication Networks*, vol. 2023, 2023.

[5] C. Adams and S. Lloyd, *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional, 2003.

[6] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1092–1101, 2024.

[7] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of network and computer applications*, vol. 149, p. 102481, 2020.

[8] K. A. Awan, I. Ud Din, A. Almogren, and J. J. P. C. Rodrigues, "Artificial intelligence and quantum synergies in trust-enhanced consumer applications for software defined networks," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 791–799, 2024.

[9] S. Ghosh, "Quantum-resistant security framework for scada communication in industrial control systems," Ph.D. dissertation, 2023.

[10] Y.-Y. Fei, X.-D. Meng, M. Gao, H. Wang, and Z. Ma, "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," *Scientific reports*, vol. 8, no. 1, p. 4283, 2018.

[11] A. Kottahachchi Kankanamge Don, I. Khalil, and M. Atiquzzaman, "A fusion of supervised contrastive learning and variational quantum classifiers," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 770–779, 2024.

[12] Y. Maleh, S. Lakkineni, L. Tawalbeh, and A. A. AbdEl-Latif, "Blockchain for cyber-physical systems: Challenges and applications," *Advances in blockchain technology for cyber physical systems*, pp. 11–59, 2022.

[13] F. Qi, K. N. Smith, T. LeCompte, N.-f. Tzeng, X. Yuan, F. T. Chong, and L. Peng, "Quantum vulnerability analysis to guide robust quantum computing system design," *IEEE Transactions on Quantum Engineering*, vol. 5, pp. 1–11, 2024.

[14] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 1–17, 2020.

[15] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–41, 2019.

[16] M. Raghu and K. Ravishankar, "Application of classical encryption techniques for securing data-a threaded approach," *International Journal on Cybernetics & Informatics*, vol. 4, no. 2, pp. 125–132, 2015.

[17] N. Sun, C.-T. Li, H. Chan, B. D. Le, M. Z. Islam, L. Y. Zhang, M. R. Islam, and W. Armstrong, "Defining security requirements with the common criteria: Applications, adoptions, and challenges," *IEEE Access*, vol. 10, pp. 44 756–44 777, 2022.

[18] A. I. Sanka, M. Irfan, I. Huang, and R. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Computer communications*, vol. 169, pp. 179–201, 2021.

[19] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the internet of things: Survey and research directions," *IEEE Communications Surveys Tutorials*, vol. 26, no. 3, pp. 1748–1774, 2024.

[20] 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.

[21] B. Halak, T. Gibson, M. Henley, C.-B. Botea, B. Heath, and S. Khan, "Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices," *IEEE Access*, vol. 12, pp. 8791–8805, 2024.

[22] A. Sunyaev and A. Sunyaev, "Distributed ledger technology," *Internet computing: Principles of distributed systems and emerging internet-based technologies*, pp. 265–299, 2020.

[23] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE access*, vol. 7, pp. 36 500–36 515, 2019.

[24] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE access*, vol. 7, pp. 112 713–112 725, 2019.

[25] H. Yin and Y. Lyu, "Gwo-based power allocation optimization algorithm for consumer iot networks," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1294–1301, 2024.

[26] M. Xu, X. Ren, D. Niyato, J. Kang, C. Qiu, Z. Xiong, X. Wang, and V. C. Leung, "When quantum information technologies meet blockchain in web 3.0," *IEEE Network*, 2023.

[27] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "A secure blockchain enabled v2v communication system using smart contracts," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 4651–4660, 2022.

[28] 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. 36 038–36 077, 2021.

[29] M. S. Peelam and R. Johari, "Enhancing security using quantum computing (esuqc)," in *Machine Learning, Advances in Computing, Renewable Energy and Communication: Proceedings of MARC 2020*. Springer, 2022, pp. 227–235.

[30] M. A. Hafeez, W.-K. Lee, A. Karmakar, and S. O. Hwang, "High throughput acceleration of scabbard key exchange and key encapsulation mechanism using tensor core on gpu for iot applications," *IEEE Internet of Things Journal*, vol. 10, no. 22, pp. 19 765–19 781, 2023.

[31] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, H. Arshad *et al.*, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security*, vol. 112, p. 102494, 2022.

[32] 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.

[33] X. Xiang, J. Cao, and W. Fan, "Decentralized authentication and access control protocol for blockchain-based e-health systems," *Journal of network and computer applications*, vol. 207, p. 103512, 2022.

[34] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys Tutorials*, vol. 26, no. 2, pp. 967–1002, 2024.

[35] S. Ullah, R. Z. Radzi, T. M. Yazdani, A. Alshehri, and I. Khan, "Types of lightweight cryptographies in current developments for resource constrained machine type communication devices: Challenges and opportunities," *IEEE Access*, vol. 10, pp. 35 589–35 604, 2022.

[36] A. Javadpour, F. Ja'fari, T. Taleb, Y. Zhao, B. Yang, and C. Benzaïd, "Encryption as a service for iot: Opportunities, challenges, and solutions," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7525–7558, 2024.

[37] A. Abuarqoub, S. Abuarqoub, A. Alzu'bi, and A. Muthanna, "The impact of quantum computing on security in emerging technologies," in *Proceedings of the 5th International Conference on Future Networks and Distributed Systems*, 2021, pp. 171–176.

[38] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Communal acts of iot consumers: A potential threat to security and privacy," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 1, pp. 64–72, 2019.

[39] J.-P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, 2017.

[40] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," 2018.

[41] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, 2019.

[42] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[43] H.-J. Korber, H. Wattar, and G. Scholl, "Modular wireless real-time sensor/actuator network for factory automation applications," *IEEE Transactions on Industrial Informatics*, vol. 3, no. 2, pp. 111–119, 2007.

[44] Z. Yang, T. Salman, R. Jain, and R. D. Pietro, "Decentralization using quantum blockchain: A theoretical analysis," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–16, 2022.

[45] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019.

[46] J. Lu, J. Shen, P. Vijayakumar, and B. B. Gupta, "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5422–5431, 2021.

[47] S. A. Alzakari, A. Sarkar, M. Z. Khan, and A. A. Alhussan, "Converging technologies for health prediction and intrusion detection in internet of healthcare things with matrix- valued neural coordinated federated intelligence," *IEEE Access*, vol. 12, pp. 99 469–99 498, 2024.

[48] J. Lu, J. Shen, P. Vijayakumar, and B. B. Gupta, "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5422–5431, 2022.

[49] X. Wang, A. Shankar, K. Li, B. D. Parameshachari, and J. Lv, "Blockchain-enabled decentralized edge intelligence for trustworthy 6g consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1214–1225, 2024.

[50] S. Datta and S. Namasudra, "Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4026–4036, 2024.

[51] M. F. Ayub, X. Li, K. Mahmood, S. Shamshad, M. A. Saleem, and M. Omar, "Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1370–1379, 2024.

[52] C. K. Wu, C.-T. Cheng, Y. Uwate, G. Chen, S. Mumtaz, and K. F. Tsang, "State-of-the-art and research opportunities for next-generation consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 937–948, 2023.

[53] M. S. Peelam, A. A. Rout, and V. Chamola, "Quantum computing applications for internet of things," *IET Quantum Communication*, vol. 5, no. 2, pp. 103–112, 2024. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12079

[54] S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, "Iot security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques," *Electronics*, vol. 10, no. 21, p. 2647, 2021.

[55] S. Aggarwal and G. Kaddoum, "Authentication of smart grid by integrating qkd and blockchain in scada systems," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5768–5780, 2024.

[56] S. Muralidharan, B. Yoo, and H. Ko, "Decentralized me-centric framework—a futuristic architecture for consumer iot," *IEEE Consumer Electronics Magazine*, vol. 12, no. 3, pp. 39–50, 2023.

[57] K. Yu, L. Tan, C. Yang, K.-K. R. Choo, A. K. Bashir, J. J. P. C. Rodrigues, and T. Sato, "A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8154–8167, 2022.

[58] D. Romano and G. Schmid, "Beyond bitcoin: A critical look at blockchain-based systems," *Cryptography*, vol. 1, no. 2, p. 15, 2017.

[59] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate internet-of-things data," *Future generation computer systems*, vol. 112, pp. 307–319, 2020.

[60] P.-Y. Kong, "A review of quantum key distribution protocols in the perspective of smart grid communication security," *IEEE Systems Journal*, vol. 16, no. 1, pp. 41–54, 2020.

[61] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: A mining behavior study," *IEEE access*, vol. 9, pp. 140 549–140 564, 2021.

[62] M. Mosca and M. Piani, "Quantum threat timeline report 2020," *Global Risk Insitute.[ ]. : https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020*, 2021.

[63] M. Pacheco, G. Oliva, G. K. Rajbahadur, and A. Hassan, "Is my transaction done yet? an empirical study of transaction processing times in the ethereum blockchain platform," *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 3, pp. 1–46, 2023.

[64] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020.

[65] 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. 74 088–74 100, 2023.

[66] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. Lvovsky, and A. K. Fedorov, "Quantum-secured blockchain," *Quantum Science and Technology*, vol. 3, no. 3, p. 035004, 2018.

[67] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2218–2247, 2021.

[68] T. Salah, H. Hasan, M. J. Zemerly, C. Y. Yeun, M. Al-Qutayri, Y. Al-Hammadi, and J. Hu, "Secure autonomous mobile agents for web services," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[69] M. O. Okwu, L. K. Tartibu, C. Maware, D. R. Enarevba, J. O. Afenogho, and A. Essien, "Emerging technologies of industry 4.0: Challenges and opportunities," in *2022 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*. IEEE, 2022, pp. 1–13.

[70] E. Biham, B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Physical Review A*, vol. 54, no. 4, p. 2651, 1996.

[71] 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.

[72] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[73] H. Ghaemi and D. Abbasinezhad-Mood, "Novel blockchain-integrated quantum-resilient self-certified authentication protocol for cross-industry communications," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 5, pp. 4493–4502, 2024.

[74] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. Jawahar, "Blind authentication: a secure crypto-biometric verification protocol," *IEEE transactions on information forensics and security*, vol. 5, no. 2, pp. 255–268, 2010.

[75] J. K. Cheng, E. M. Lim, Y. Y. Krikorian, D. J. Sklar, and V. J. Kong, "A survey of encryption standard and potential impact due to quantum computing," in *2021 IEEE Aerospace Conference (50100)*, 2021, pp. 1–10.

[76] X. Xu, J. Wu, A. K. Bashir, and M. Omar, "Machine learning and zero knowledge empowered trustworthy bitcoin mixing for next-g consumer electronics payment," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2210–2223, 2024.

[77] J. Zong, C. Wang, J. Shen, C. Su, and W. Wang, "Relac: Revocable and lightweight access control with blockchain for smart consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3994–4004, 2023.

[78] S. S. Gill, S. Tuli, M. Xu, I. Singh, K. V. Singh, D. Lindsay, S. Tuli, D. Smirnova, M. Singh, U. Jain *et al.*, "Transformative effects of iot, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges," *Internet of Things*, vol. 8, p. 100118, 2019.

[79] M. M. Akhtar, M. Z. Khan, M. A. Ahad, A. Noorwali, D. R. Rizvi, and C. Chakraborty, "Distributed ledger technology based robust access control and real-time synchronization for consumer electronics," *PeerJ Computer Science*, vol. 7, p. e566, 2021.

[80] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM computing surveys (CSUR)*, vol. 52, no. 6, pp. 1–34, 2019.

[81] S. Ghosh, M. Zaman, R. Joshi, and S. Sampalli, "Multi-phase quantum resistant framework for secure communication in scada systems," *IEEE Transactions on Dependable and Secure Computing*, 2024.

[82] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, no. 10, 2017.

[83] M. Platt and P. McBurney, "Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance," *Algorithms*, vol. 16, no. 1, p. 34, 2023.

[84] N. Ahmed, "Tinyzmq++: A privacy preserving content-based publish/subscribe iot middleware," in *2023 6th Conference on Cloud and Internet of Things (CIoT)*, 2023, pp. 40–46.

[85] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, "Experimental quantum secure network with digital signatures and encryption," *National Science Review*, vol. 10, no. 4, p. nwac228, 2023.

[86] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

[87] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3808–3833, 2020.

[88] 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.
[89] V. Hassija, V. Chamola, A. Goyal, S. S. Kanhere, and N. Guizani, "Forthcoming applications of quantum computing: peeking into the future," *IET Quantum Communication*, vol. 1, no. 2, pp. 35–41, 2020.
[90] P. Busch, T. Heinonen, and P. Lahti, "Heisenberg's uncertainty principle," *Physics reports*, vol. 452, no. 6, pp. 155–176, 2007.
[91] 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.
[92] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, and M. Guizani, "Present landscape of quantum computing," *IET Quantum Communication*, vol. 1, no. 2, pp. 42–48, 2020.
[93] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72 514–72 550, 2018.
[94] M. S. Peelam, S. Sai, and V. Chamola, "Explorative implementation of quantum key distribution algorithms for secure consumer electronics networks," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2024.
[95] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on rsa and ecc-based cipher suites for iot high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, 2018.
[96] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18*. Springer, 2014, pp. 157–175.
[97] N. M. Wani, G. K. Verma, and V. Chamola, "Dynamic anonymous quantum-secure batch-verifiable authentication scheme for vanet," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2024.
[98] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International journal of information security*, vol. 1, pp. 36–63, 2001.
[99] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2019.
[100] A. Mukherjee, V. Hassija, and V. Chamola, "Quarcs: Quantum anomaly recognition and caption scoring framework for surveillance videos," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2024.
[101] S. Bajrić, "Enabling secure and trustworthy quantum networks: current state-of-the-art, key challenges, and potential solutions," *IEEE Access*, vol. 11, pp. 128 801–128 809, 2023.
[102] Y. Huang, Z. Su, F. Zhang, Y. Ding, and R. Cheng, "Quantum algorithm for solving hyperelliptic curve discrete logarithm problem," *Quantum Information Processing*, vol. 19, no. 2, p. 62, 2020.
[103] D. S. C. Putranto, R. W. Wardhani, H. T. Larasati, and H. Kim, "Space and time-efficient quantum multiplier in post quantum cryptography era," *IEEE Access*, vol. 11, pp. 21 848–21 862, 2023.
[104] M. U. Rehman, A. Shafique, and A. B. Usman, "Securing medical information transmission between iot devices: An innovative hybrid encryption scheme based on quantum walk, dna encoding, and chaos," *Internet of Things*, vol. 24, p. 100891, 2023.
[105] T. M. Fernández-Caramès 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.
[106] R. Saha, G. Kumar, T. Devgun, W. J. Buchanan, R. Thomas, M. Alazab, T. Hoon-Kim, and J. J. Rodrigues, "A blockchain framework in post-quantum decentralization," *IEEE Transactions on Services Computing*, vol. 16, no. 1, pp. 1–12, 2021.