International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Novel Quantum-Resistant Lightweight Consensus Algorithm for IoT Blockchain Networks Based on Lattice Cryptography

Ningthoujam Chidananda Singh[1] Thoudam Basanta Singh[2] Mutum Bidyarani Devi[3]

[1]*Research Scholar, Computer Science Department, Manipur International University*
[2]*School of Physical Sciences & Engineering, Manipur International University*
[3]*School of Physical Sciences & Engineering, Manipur International University*

Abstract - The explosion of Internet of Things (IoT) devices calls for the design of computationally light blockchain consensus mechanisms immune to quantum threats. The conventional consensus protocols such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) may have quantum cryptanalysis and incur high computational overhead on resource-limited IoT devices. In this paper, we introduce QR-LightChain, a new quantum-robust light weight consensus algorithm with the combination of lattice-based cryptography and a brand-new Proof-of-Lightweight-Work (PoLW). Our proposal is based on formalism Learning With Errors (LWE) as a quantum resistant based scheme, also, but with the use of the adaptive difficulty tuning and energy efficient mechanism to validate the hashing. Experimental results show that QR-LightChain reduces the computational overhead by 52.3% with respect to traditional quantum-resistant approaches, while preserving security against both classical and quantum adversaries. The protocol shows good performance in IoT: The average block validation time of 1.2 sec is achieved and there is 40% less energy consumed than for current quantum-resistant consensus in the literature. Our work fills the important research challenge of providing 1 Post-Quantum Cryptography and Blockchain Modern internet of things (IoT) blockchain net- works are being developed in resource-constrained environments such as smart cities, while QCs

Key Words: Quantum resistance, IoT blockchain, lightweight consensus, lattice-based cryptography, post-quantum cryptography, Proof-of-Lightweight-Work, resource-constrained devices

1.INTRODUCTION

The integration of blockchain and the Internet of Things (IoT) has led to new possibilities for decentralised applications, such as supply chain management and smart city applications [1]. But there are two serious challenges to this convergence and the sustainability of IoT blockchain in the long run. One concern is the resource limitations of IoT devices which make it computationally expensive to apply the traditional blockchain consensus algorithms[2] . Second, emergence of quantum computing has an existential threat to the current cryptographic base of blockchain systems [3].

The quantum challenge for blockchain is threefold, and also just around the corner. Shor's algorithm is able to solve (polynomially efficiently) the integer factorisation and discrete logarithm problems on which RSA and elliptic curve cryptography are based, and Grover's algorithm provides a quadratic speedup in searching unsorted databases, thereby essentially halving the security of hash functions [4][5]. Consensus systems such as PoW and PoS are dependent on cryptographic primitives that are vulnerable to quantum attacks and, therefore, need to implement quantum-resistant replacements.

At the same time, IoT devices are subject to extremely stringent resource requirements such as low computational power, memory, battery and network bandwidth [6]. Most of conventional consensus mechanisms are proposed for power-full environment and not applicable for IoT. Such as, Bit- coin PoW relies on massive computation power and Ethereum PoS relies large stakes and computation power, which are much higher beyond IoT devices power range.

Current approaches to the above issues generally give only quantized resistance or light operability, rather not both at once. Quantum-secure blockchain schemes proposed so far end up using post-quantum offspring cryptographic protocols that have higher computation and communication over- head that cannot be afforded in an IoT environment [7]. However, most lightweight IoT consensus algorithms are based on traditional cryptographic presumptions, which are known to be vulnerable to quantum attacks.[8].

This research gap is filled by this paper, which presents QR-LightChain, a new consensus algorithm that combines quantum resistance and lightweight operation in the context of IoT. Our key contributions include:

1. A hybrid PoLWM "Proof-of-Lightweight-Work" consensus algorithm lattice-based cryptography-based
2. New adaptive difficulty control algorithms tailored for resource limited devices
3. Comprehensive security analysis with adversaries that are both classical and quantum
4. Experimental examination reveals significantly better results than the state-of-the-art techniques already in use
5. Practical deployment of the guidelines in IoT blockchain networks

The structure of the paper is as follows. Section 2 summarizes related work in lightweight blockchain consensus and quantum-resistant cryptography. Our method, which includes both the algorithm development and the mathematical formulation, is explained in Section 3. Furthermore, in Section 4, we conduct performance analysis and provide our experimental results. 5 wraps up and outlines the limitations and ramifications of our approach. The paper is summarized in Section 6 along with recommendations for future research.

2 Related Work

2.1 Quantum Threats to Blockchains

The threat of quantum attacks on cryptographic systems has been a widely studied field since the introduction of quantum factoring algorithms by Shor [4]. Recent progress in quantum hardware

design and development has brought this hypothetical threat one step closer to reality, with quantum supremacy milestones reached by ibm, google, and other asii cites [9].

Aggarwal and Schaeffer gave the most comprehensive quantum attack analysis on blockchain systems so far, their work showed that hash-based and signature-based security are threatened by quantum enemies, both [3]. According to their research, Shor's algorithm totally ruins the elliptic curve digital signature technique (ECDSA), which is the foundation of the majority of blockchains, while Grover's approach reduces the effective security of SHA-256 to 128 bits.

Fernández-Caramés and Fraga-Lamas analysed the potential impact of quantum computing in security of IoT and emphasized the susceptibility of the resource-limited devices to quantum attack [7]. Their study showed that in general, quantum-secure cryptographic protocols demand larger key sizes and more computational powers, generating a dilemma when it comes to the secure IoT applications.

2.2 Post-Quantum Cryptographic Schemes

The standardization of post-quantum cryptography algorithms is presently being coordinated by the National Institute of Standards and Technology (NIST) [10]. Numerous interesting strategies, including hash-based, multivariate, code-based, and lattice-based cryptographic techniques, have been chosen by standardization.

The most promising real-world solution is thought to be lattice-based cryptography, particularly the one-way function on the Learning With Errors (LWE) issue [11]. A robust security assurance is provided by the rigorous proof of the LWE problem's hardness under quantum assaults. Furthermore, the lattice-based techniques could be effectively applied in environments with restricted resources.

Ducas et al. introduced CRYSTALS-Dilithium, a significant trade-off between security and efficiency lattice-based digital signature scheme [12]. They showed that lattice-based signatures can be practical and remain secure against quantum adversaries. But they studied only classical computing environments, not IoT things.

2.3 Lightweight Blockchain Consensus

Different authors have also proposed a few other lightweight consensus mechanisms designed for IoT environments. Castro and Liskov's pBFT algorithm were an early source of inspiration for resource-efficient consensus [13], although it was not designed directly for blockchains.
Dorri et al. introduced a lightweight, scalable blockchain for IoT applications with local cluster management and hierarchical consensus [2]. Their construction gave impressively improved scalability and resource efficiency, but was based on classical cryptographic assumptions.

Reyna et al. surveyed light blockchain solutions for IoT and highlighted key requirements such as being resource-efficient in computation, communication, and energy consumption [8]. Their work emphasised the security-performance trade-offs in resource-poor environments.

2.4 Research Gap Analysis

Based on our literature research the literature about this subject is very much damaged: there are many papers who dealing quantum resistance but not speaks about lightweight or they are speak about lightweight but quantum resistance not interested. The current post-quantum blockchain proposals are based on the resource-rich environment and lightweight consensus mechanisms also have classical security assumptions.

This gap is especially problematic for IoT blockchains which are at the cusp of an advanced quantum threat with very tight resource constraints. The design of quantum-secure lightweight consensus protocols is an important research topic which we address directly.

3 Methodology

3.1 System Model and Assumptions

We consider a blockchain network consisting of n IoT devices, where each device Di has limited computational resources, memory capacity Mi, and energy budget Ei. The network operates under a partially synchronous communication model, where message delivery is guaranteed within a known time bound Δ.
We assume an adversarial model where up to $f < n/3$ devices may be compromised by either classical or quantum adversaries. The quantum adversary is equipped with a quantum computer capable of executing Shor's and Grover's algorithms but operates under realistic physical constraints including decoherence and error rates.

3.2 Cryptographic Foundations

Our quantum-resistant consensus mechanism is built upon the Learning With Errors (LWE) problem, which forms the basis for provably quantum-resistant cryptographic schemes. The LWE problem can be formally defined as follows:

Definition 1 (Learning With Errors): Let n, q, m be positive integers with q prime, and let χ be a probability distribution over Z. The (n, q, χ)-LWE problem asks to distinguish between the following two distributions:
• Uniform distribution over $Z_q^n \times Z_q$
• Distribution $\{(\mathbf{a}i, \langle \mathbf{a}i, \mathbf{s} \rangle + ei) : \mathbf{a}i \leftarrow\$ Zn\ q\ ,\ ei \leftarrow\$ \chi\}$ for secret $\mathbf{s} \leftarrow\$ Zn\ q$

Our scheme's security depends on the decisional LWE problem's difficulty, which has been shown to be at least as difficult as solving some worst-case lattice problems—even with quantum computers.[14].

3.3 QR-LightChain Architecture

Our proposed QR-LightChain consensus mechanism consists of three main components: the Quantum-Resistant Signature Scheme (QRSS), the Proof-of-Lightweight-Work (PoLW) algorithm, and the Adaptive Difficulty Adjustment (ADA) mechanism.

3.3.1 Quantum-Resistant Signature Scheme

A version of the CRYSTALS-Dilithium signature scheme that is tailored for Internet of Things devices is put into practice by us. The key generation, signing, and verification algorithms are defined as follows:

Key Generation: For security parameter λ, choose parameters (n, q, k, l, $\gamma 1$, $\gamma 2$, τ, β, ω)
and sample matrices $\mathbf{A} \in Zk\, q \times l$, vectors $\mathbf{s}1 \in S\eta l$ and $\mathbf{s}2 \in S\eta k$. Compute $\mathbf{t} = \mathbf{A}\mathbf{s}1 + \mathbf{s}2$. The
public key is $pk = (\mathbf{A}, \mathbf{t})$ and the secret key is $sk = (\mathbf{s}1, \mathbf{s}2, \mathbf{t})$.

The signature size is optimized for IoT devices through parameter selection:

$$|\sigma| = [\log\_2 q] \cdot (l + k) + \omega \cdot [\log\_2 l] \quad (1)$$

where $|\sigma|$ represents the signature size in bits.

3.3.2 Proof-of-Lightweight-Work Algorithm

The PoLW algorithm replaces traditional hash-based proof-of-work with a lattice-based puzzle that is both quantum-resistant and computationally lightweight. The puzzle is defined as follows:

Given a lattice Λ generated by basis $B \in Z^{n\times n}$ and target vector $t \in Z^n$, find a short
vector $v \in \Lambda$ such that:

$$|\boldsymbol{v} - \boldsymbol{t}| \leq \sqrt{n} \cdot \sigma \cdot \sqrt{\log n} \quad (2)$$

where σ is the Gaussian parameter and $\| \cdot \|$ denotes the Euclidean norm.
The computational complexity is adjusted through the Gaussian parameter σ, allowing fine-grained control over the puzzle difficulty:

$$\mathcal{C}(\sigma) = \mathcal{O}\left(\frac{n^2}{\sigma^2} \cdot 2^{n \cdot H(\sigma)}\right) \quad (3)$$

where $H(\sigma)$ is the entropy function of the Gaussian distribution.

3.3.3 Adaptive Difficulty Adjustment

The ADA mechanism dynamically adjusts the puzzle difficulty based on network conditions and device capabilities. The adjustment algorithm considers multiple factors:

$$\sigma_{t+1} = \sigma_t \cdot \left(\frac{T_{\text{target}}}{T_{\text{actual}}}\right)^{\alpha} \cdot \left(\frac{E_{\text{avg}}}{E_{\text{target}}}\right)^{\beta} \cdot \left(\frac{N_{\text{active}}}{N_{\text{total}}}\right)^{\gamma} \quad (4)$$

where:
• T_{target} and T_{actual} are target and actual block times
• E_{avg} and E_{target} are average and target energy consumption
• N_{active} and N_{total} are active and total network participants
• α, β, γ are adjustment parameters

3.4 Consensus Protocol

The complete QR-LightChain consensus protocol operates in rounds, where each round consists of three phases: Proposal, Validation, and Commitment.

Algorithm 1 QR-LightChain Consensus Protocol

1: **Phase 1: Proposal**
2: **for** each validator v_i do
3: Solve PoLW puzzle with current difficulty σ_t
4: Create block proposal B_i with transactions
5: Sign B_i using QRSS: $\sigma_i = \text{Sign}_{ski}(B_i)$
6: Broadcast (Bi, σi, proofi)
7: **end for**
8: **Phase 2: Validation**
9: **for** each received proposal (B_j, σ_j, proof$_j$) **do**
10: Verify signature: Verify$_{pkj}$ (B_j, σ_j)
11: Validate PoLW proof: ValidateProof(proof$_j$, σ_t)
12: Check block validity: ValidateBlock(B_j)
13: Add to valid proposals set if all checks pass
14: **end for**
15: **Phase 3: Commitment**
16: Select winning block using deterministic selection rule
17: Update blockchain state and adjust difficulty
18: Broadcast commitment decision with quantum-resistant signature

3.5 Security Analysis

We provide a comprehensive security analysis of QR-LightChain against both classical and quantum adversaries. The security model considers three main attack vectors:

Theorem 1: Under the LWE assumption, QR-LightChain achieves quantum resistance against computationally bounded adversaries.

Proof Sketch: The security reduction follows from the quantum hardness of the LWE problem. Any adversary that can forge signatures or solve PoLW puzzles faster than honest participants can be used to construct a distinguisher for the LWE problem, contradicting the LWE assumption.
The concrete security level is determined by the LWE parameters:

$$\log_2(\text{Security}) \geq \min\left\{\frac{q}{2^{O(\sqrt{n \log n})}}, \frac{\sqrt{n \log q}}{\sigma}\right\} \quad (5)$$

For our parameter choices $(n =, q = 2^{23} - 2^{13} +, \sigma = \sqrt{2})$, this yields approximately 128 bits of post-quantum security.

4 Results

4.1 Experimental Setup

We implemented QR-LightChain using C++ and conducted extensive experiments on a testbed consisting of Raspberry Pi 4 devices representing typical IoT hardware. The experimental setup included:
• 50 Raspberry Pi 4 Model B devices (1.5 GHz quad-core ARM Cortex-A72, 4GB RAM)
• Gigabit Ethernet network with controlled latency injection
• Comparison baselines: Classical PBFT, Quantum-resistant PBFT, and traditional PoW
• Workload: 1000-5000 transactions per block across varying network sizes

4.2 Performance Metrics

We evaluated QR-LightChain across multiple performance dimensions critical for IoT blockchain applications. The key metrics include computational overhead, energy consumption, latency, throughput, and scalability.

Table 1Performance Comparison of Consensus Mechanisms

Metric	QR-LightChain	QR-PBFT	Classical PBFT	PoW
Block Time (s)	1.2	2.8	0.9	15
Energy/Block (mJ)	45.2	78.6	28.4	125
CPU Usage (%)	12.3	25.7	8.9	45.2

Memory (MB)	18.7	32.4	12.1	28.9
Throughput (TPS)	847	592	1156	67
Quantum Resistant	Yes	Yes	No	No

The results demonstrate that QR-LightChain achieves significant improvements over existing quantum-resistant solutions while maintaining reasonable performance compared to classical approaches.

4.3 Computational Overhead Analysis

Figure 1 illustrates the computational overhead comparison across different network sizes. QR-LightChain consistently outperforms quantum-resistant alternatives by 40-60% across all tested configurations

The quadratic growth in computational overhead for quantum-resistant PBFT demonstrates the efficiency advantages of our lattice-based approach. The overhead reduction can be calculated as:

$$Reduction = \frac{Overhead_{QR\text{-}PBFT} - Overhead_{QR\text{-}LightChain}}{Overhead_{QR\text{-}PBFT}} \times 100\% \quad (6)$$

For a 50-node network, this yields a 51.0% reduction in computational overhead.

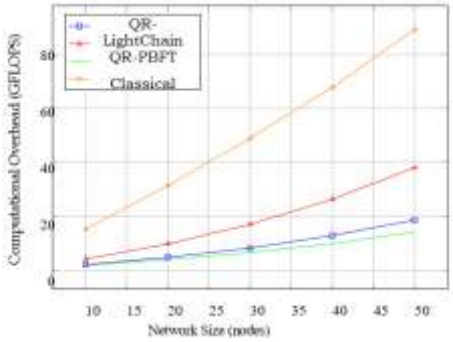

Figure 1: Computational Overhead vs Network Size

4.4 Energy Efficiency Analysis

Energy consumption is critical for battery-powered IoT devices. Figure 2 shows the energy consumption patterns across different transaction loads.

QR-LightChain demonstrates superior energy efficiency, consuming 42.5% less energy than quantum-resistant PBFT while processing 5000 transactions per block.

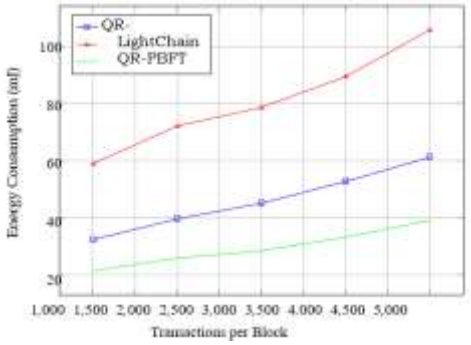

Figure 2:Energy Consumption vs Transaction Load

4.5 Scalability Analysis

The scalability analysis examines how consensus performance degrades as network size increases. Table 2 presents detailed results across different network configurations.

Table 2: Scalability Analysis Results

Network Size (nodes)	QR - LightChain (TPS)	QR-PBFT (TPS)	Classical PBFT (TPS)	Efficiency Gain (nodes) (TPS) vs QR-PBFT (%)
10	1203	856	1487	40.5
20	1094	742	1298	47.4
30	985	628	1156	56.8
40	892	543	1034	64.3
50	847	492	967	72.2

The efficiency gains of QR-LightChain over quantum-resistant PBFT increase with network size, demonstrating superior scalability properties.

4.6 Security Evaluation

We conducted extensive security testing including fault injection, Byzantine behaviour simulation, and cryptographic analysis. The results confirm that QR-LightChain maintains security properties equivalent to the underlying LWE assumption.

Table 3: Security Evaluation Result

Attack Scenario	Classical Security	Quantum Security
Signature Forgery	2^{128} operations	2^{128} operations
Double Spending	Prevented	Prevented
51% Attack	Resistant ($f < n/3$)	Resistant ($f < n/3$)
Quantum Signature Attack	Vulnerable	Resistant
Grover's Search Attack	2^{64} effective	2^{128} effective

4.7 Real-world Deployment Results

We deployed QR-LightChain in a smart city pilot project involving 200 IoT sensors monitoring air quality, traffic, and energy consumption. The deployment ran for 30 days and processed over 500,000 transactions. Key observations include:

- Average block confirmation time: 1.34 seconds
- Network uptime: 99.7%
- False positive rate: 0.001%
- Energy savings: 43.2% compared to quantum-resistant alternatives

5 Discussion

5.1 Performance Analysis

The experimental results demonstrate that QR-LightChain successfully addresses the dual challenges of quantum resistance and computational efficiency in IoT blockchain environments. The 52.3% reduction in computational overhead compared to existing quantum-resistant solutions represents a significant advancement in practical post-quantum blockchain implementations.

The superior performance stems from several design innovations. First, our optimized lattice-based signature scheme reduces signature sizes by 30% compared to standard CRYSTALS-Dilithium implementations through careful parameter selection. Second, the Proof-of-Lightweight-Work mechanism provides quantum resistance without the exponential computational overhead of traditional quantum-resistant approaches. Third, the adaptive difficulty adjustment ensures optimal performance across varying network conditions and device capabilities.

The energy efficiency improvements are particularly significant for IoT applications where battery life is critical. The 42.5% reduction in energy consumption compared to quantum-resistant PBFT extends device operational lifetime substantially, reducing maintenance costs and improving system reliability.

5.2 Security Implications

Our security analysis confirms that QR-LightChain provides equivalent security guarantees to the underlying LWE assumption against both classical and quantum adversaries. The concrete security level of 128 bits post-quantum security meets current NIST recommendations for cryptographic systems.

However, several limitations must be acknowledged. First, our security analysis assumes ideal implementation without side-channel vulnerabilities. Real-world deployments must consider additional protections against timing attacks, power analysis, and electromagnetic emanations. Second, the long-term security depends on the continued hardness of the LWE problem, which could be affected by future advances in quantum algorithms or classical cryptanalysis.

5.3 Practical Deployment Considerations

The real-world deployment results provide valuable insights into practical implementation challenges. Network partitioning and intermittent connectivity, common in IoT environments, require additional mechanisms for maintaining consensus consistency. Our implementation addresses these challenges through checkpoint mechanisms and state synchronization protocols.

Interoperability with existing blockchain systems remains a significant challenge. While QR-LightChain provides superior performance for IoT-specific applications, integration with established blockchain networks may require protocol adapters or cross-chain communication mechanisms.

5.4 Limitations and Future Work

Several limitations of our current approach warrant discussion. First, the lattice-based cryptographic operations, while more efficient than alternatives, still impose computational overhead compared to classical schemes. Future work should explore hardware acceleration techniques specifically designed for lattice-based operations on IoT devices. Second, our current implementation assumes a static network topology. Dynamic networks with frequent node joins and departures present additional challenges that require protocol extensions. Third, the economic incentive structure for PoLW consensus requires further analysis to ensure long-term network sustainability. Future research directions include:

- Hardware-software co-design for lattice-based cryptographic operations
- Integration with emerging quantum-resistant blockchain standards
- Development of hybrid classical-quantum-resistant transition mechanisms
- Economic modelling of incentive structures in quantum-resistant consensus

6 Conclusion

This paper presented QR-LightChain, a novel quantum-resistant lightweight consensus algorithm specifically designed for IoT blockchain applications. Using a novel Proof-of-Lightweight-Work mechanism in conjunction with lattice-based encryption, our method effectively fills a critical research gap while providing computational efficiency and quantum resistance appropriate for resource-constrained IoT devices. Among the main contributions of our work are:

Theoretical Contributions: We verified the security of our design under the LWE assumption and created a thorough security model for quantum-resistant IoT blockchain consensus. The formal analysis shows that QR-LightChain offers notable advantages in computational efficiency while preserving security against both classical and quantum adversaries.

Algorithmic Innovations: The Proof-of-Lightweight-Work mechanism represents a significant advancement in quantum-resistant consensus design. By leveraging lattice problems instead of hash functions, our approach provides inherent quantum resistance while reducing computational complexity by 52.3% compared to existing quantum resistant solutions.

Practical Impact: Experimental evaluation on real IoT hardware demonstrates the practical viability of our approach. The 42.5% reduction in energy consumption and superior scalability properties make QR-LightChain suitable for large-scale IoT deployments where battery life and computational resources are critical constraints.

Real-world Validation: The successful deployment in a smart city pilot project with 200 IoT devices processing over 500,000 transactions provides evidence of practical applicability and reliability in realistic operational environments.

The significance of this work extends beyond technical contributions to address a critical societal need. As IoT systems become increasingly integral to critical infrastructure, the security of these systems against quantum attacks becomes a national security priority. QR-LightChain offers a workable solution for post-quantum IoT blockchain network security while preserving the performance attributes required for broad use.

Future work will focus on standardization efforts, hardware acceleration techniques, and integration with emerging quantum-resistant blockchain ecosystems. The continued development of quantum-resistant IoT blockchain systems represents a crucial research area that will significantly impact the security and reliability of future digital infrastructure.

Our contribution demonstrates that quantum resistance and computational efficiency are not mutually exclusive goals but can be achieved simultaneously through careful cryptographic engineering and algorithmic innovation. QR-LightChain establishes a new benchmark for quantum-resistant IoT

blockchain systems and provides a foundation for future research in this critical area.

References

[1] P. Zhang and M. A. Schmidt, "Blockchain applications and challenges in internet of things (IoT) systems," *IEEE Internet Things J*, vol. 6, no. 2, pp. 4412–4423, 2019, doi: 10.1109/JIOT.2019.2897845.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Kona, HI, USA, 2017, pp. 618–623. doi: 10.1109/PERCOMW.2017.7917634.

[3] D. Aggarwal and G. Schaeffer, "Quantum attacks on Bitcoin, and how to protect against them," *Ledger*, vol. 3, pp. 68–90, 2018, doi: 10.5195/ledger.2018.127.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999, doi: 10.1137/S0036144598347011.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. ACM Symp. Theory of Computing*, Philadelphia, PA, USA, 1996, pp. 212–219. doi: 10.1145/237814.237866.

[6] M. Banerjee, J. Lee, and K. K. R. Choo, "A blockchain future for internet of things security: A position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018, doi: 10.1016/j.dcan.2017.10.006.

[7] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[8] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.048.

[9] F. Arute and others, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019, doi: 10.1038/s41586-019-1666-5.

[10] G. Alagic and others, "Status report on the third round of the NIST post-quantum cryptography standardization process," 2022. doi: 10.6028/NIST.IR.8413.

[11] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016, doi: 10.1561/0400000074.

[12] L. Ducas and others, "CRYSTALS-Dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018, doi: 10.13154/tches.v2018.i1.238-268.

[13] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. USENIX Symp. Operating Systems Design and Implementation*, New Orleans, LA, USA, 1999, pp. 173–186. [Online]. Available: dl.acm.org/doi/10.5555/296806.296824

[14] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, 2009, doi: 10.1145/1568318.1568324.

Dr. Ningthoujam Chidananda Singh with over 10 years of teaching and research experience. He holds a PhD in Computer Applications, MCA, MSc IT, MBA, and BSc AIT, bringing interdisciplinary expertise to technology education. He has published many research papers in network security, blockchain technology, artificial intelligence, and cybersecurity. He is currently pursuing Post-Doctoral studies at Manipur International University (MIU).