Leveraging Quantum Entropy in Blockchain Networks: Exploring the Decentralization of BB84 Key Generation and QRNG Modules

Paraxiom

January 17, 2024.

Contents

Abstract

This paper delves into the integration of quantum computing advancements in blockchain cryptography, with a dual focus: the implementation of the BB84 protocol within the Kirk network for quantum key generation, and the potential development of Decentralized Quantum Random Number Generators (DQRNGs). A significant aspect of our approach is the incorporation of Post-Quantum Verifiable Random Functions (PQ-VRFs), as detailed in "Post-Quantum VRF and its Applications in Future-Proof Blockchain System", for enhancing the security of blockchain consensus mechanisms and random beacon generation. We highlight the pivotal role of decentralized oracles in effectively integrating quantum-derived keys into blockchain systems, thereby fortifying network security and operational efficiency. This study presents the challenges and opportunities in harmonizing quantum cryptographic methods with blockchain technologies, underlining the immediate applicability of the BB84 protocol and the prospective integration of DQRNGs and PQ-VRFs. Our aim is to offer a comprehensive perspective on augmenting blockchain infrastructure against emerging quantum threats while preserving the decentralized essence of blockchain networks.

1 Background

The emergence of quantum computing presents unique challenges and opportunities in the domain of cryptography, profoundly influencing blockchain protocols and systems. Traditional cryptographic algorithms, like RSA and ECDSA, are vulnerable to quantum attacks, posing significant security risks to blockchain technologies.

1.1 Quantum Key Distribution (QKD) and BB84 Protocol

QKD, particularly through the BB84 protocol, provides a quantum-secure method for key distribution using quantum and classical communication channels. Despite its potential, QKD scalability is limited by factors such as quantum state attenuation over distance and infrastructure complexity.

1.2 Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) offers a suite of solutions to protect cryptographic processes from the looming threat of quantum computers. It focuses on addressing the vulnerabilities posed by quantum computers to traditional cryptographic algorithms. PQC includes various quantum-resistant asymmetric key algorithms, some of which are:

1. **Lattice-Based Cryptography**: This approach relies on the hardness of lattice problems and encompasses schemes like NTRUEncrypt and Kyber.

2. **Code-Based Cryptography**: These schemes leverage error-correcting codes, making them resistant to quantum attacks. Notable examples include McEliece and BIKE.

3. **Multivariate Polynomial Cryptography**: This category features schemes such as Rainbow and HFE, which are based on the complexity of solving multivariate polynomial equations.

4. **Hash-Based Cryptography**: Post-Quantum security is achieved by using hash functions, as seen in the Merkle Signature Scheme (MSS) and the Winternitz One-Time Signature Scheme.

5. **Isogeny-Based Cryptography**: This emerging field exploits isogenies between elliptic curves to create secure cryptographic primitives. SIKE (Supersingular Isogeny Key Encapsulation) is a prominent example.

6. **Hash-Based Cryptographic Signatures**: These schemes are derived from hash functions and are known for their quantum resistance. Notable examples include XMSS (eXtended Merkle Signature Scheme) and SPHINCS (SPHINCS-256).

7. **Code-Based Digital Signatures**: Code-based cryptography extends its protection to digital signatures with schemes like LUOV (Lizard - Union of Oil and Vinegar) and CFS (Classic McEliece & Falcon & Sphinx).

8. **Zero-Knowledge Proofs**: Quantum-resistant zero-knowledge proofs, such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), enhance privacy and security in blockchain and other applications.

These quantum-resistant asymmetric key algorithms play a crucial role in ensuring the continued security of digital communication and data protection in an era where quantum computers pose a significant threat to traditional cryptographic methods.

1.3 Decentralization of Quantum Entropy and Blockchain Integration

The inherent decentralization in blockchain necessitates decentralized quantum entropy sources. However, challenges have often led to centralized approaches. Efforts like Lacchain have made strides in distributing quantum entropy across nodes, paving the way for quantum-resistant blockchain technologies.

1.4 Advancements in Quantum Computing and Blockchain Security

The rapid progress in quantum computing presents a pressing need for blockchain networks to fortify their security measures. To address this challenge, we focus on

two key approaches: the utilization of the BB84 protocol for quantum-resistant blockchain networks and the exploration of Decentralized Quantum Random Number Generators (DQRNGs). These strategies are augmented by the integration of Post-Quantum Verifiable Random Functions (PQ-VRFs), which play a pivotal role in enhancing blockchain security, specifically in consensus mechanisms and the generation of random beacons. This alignment with blockchain's intrinsic decentralized nature positions us to proactively address emerging quantum threats while preserving the core principles of blockchain technology.

2 Enhancing Decentralization in BB84 QKD with Post-Quantum VRF

Incorporating Post-Quantum Verifiable Random Functions (PQ-VRFs) into the BB84 protocol of Quantum Key Distribution (QKD) offers a significant advancement in ensuring the security and decentralization of blockchain networks against quantum computing threats.

2.1 Integration of PQ-VRFs in BB84 Protocol

The process of integrating PQ-VRFs into the BB84 protocol involves:

1. Nodes within the blockchain network generating PQ-VRF proofs based on random values.
2. Achieving network consensus to validate these PQ-VRF proofs.
3. Selecting node pairs for initiating the BB84 QKD process based on the validated proofs.
4. Proceeding with the standard BB84 protocol for quantum key distribution by the selected node pairs.

2.2 Advantages of PQ-VRFs in Decentralized QKD

The use of PQ-VRFs in decentralized QKD systems offers several benefits:

- **Enhanced Security:** PQ-VRFs provide robust defense against quantum threats, contributing to the security of the QKD process.
- **Improved Scalability:** Facilitating efficient management of QKD sessions in large blockchain networks.
- **Decentralization and Trust:** Upholding the decentralized ethos of blockchain and enhancing trust among network participants.

This approach to integrating PQ-VRFs with the BB84 protocol presents a forward-looking strategy for blockchain-based quantum key distribution systems, aligning with the evolving landscape of quantum computing.

3 Enhancing Blockchain Security: Key State Management and Translation of Quantum Keys

As blockchain technology evolves, managing the state and translation of quantum keys becomes increasingly important. This section outlines innovative strategies for handling quantum keys in blockchain systems, particularly focusing on the integration of PQ-VRFs and the BB84 protocol.

3.1 Lifecycle Management of Quantum Keys

Key state management is essential in quantum-resistant systems. Our framework categorizes each quantum key into states like UNUSED, POSTED, or REDEEMED. This classification ensures the integrity and one-time use of each key, enhancing the security of the blockchain network.

3.2 Translating Quantum Keys for Diverse Blockchain Architectures

Our system includes a decentralized oracle for adapting BB84-derived quantum keys to fit various blockchain encryption schemas. This approach, integrated with PQ-VRFs, enhances the versatility and user-friendliness of our system. The oracle acts as a bridge, converting quantum-safe keys for use within traditional blockchain cryptographic frameworks, thus aligning with the quantum-resistant strategies of the future.

4 Integration and Operational Workflow

4.1 Decentralized Oracle as a Quantum-Safe Bridge

Our decentralized oracle, enhanced with PQ-VRFs, serves as a critical interface between the quantum network and classical blockchain systems. It plays a pivotal role in translating quantum cryptographic elements like QRNG outputs and BB84 keys into formats compatible with blockchain architectures, ensuring the integrity and usability of quantum-enhanced security features within the blockchain's native protocols.

4.2 Operational Workflow with PQ-VRF Integration

1. Generation of quantum keys and random numbers using QRNGs and the BB84 protocol within the quantum network.

2. Application of PQ-VRFs for transparent and unbiased node selection in the quantum key generation process.

3. The decentralized oracle retrieves, translates, and distributes these quantum elements for blockchain encryption, ensuring their compatibility and security.

4. Tracking and managing the lifecycle of each key (UNUSED, POSTED, REDEEMED) for enhanced security and integrity.

4.3 Kirk: Numana's Quantum Communication Network Testbed

The Numana-Quebec-Bell Canada alliance's quantum communication testbed, as a platform for practical evaluation, supports these strategies, providing an environment for testing and refining quantum-resistant technologies in decentralized blockchain networks.

5 Approach 1: Decentralized BB84 Oracle Enhanced with PQ-VRFs

Our approach to quantum-resistant blockchain cryptography centers on the implementation of a decentralized BB84 oracle that is further fortified with Post-Quantum Verifiable Random Functions (PQ-VRFs). This strategy aims to harness the quantum security of the BB84 protocol while introducing robust cryptographic techniques to enhance security within the Kirk network and blockchain systems.

5.1 Decentralized BB84 Oracle Implementation

The core of our approach lies in the implementation of a decentralized BB84 oracle within the Kirk network. This decentralized oracle serves as a critical interface between the quantum network and classical blockchain systems, ensuring the secure integration of quantum-generated keys into blockchain protocols.

5.2 Integration of PQ-VRFs into the Decentralized BB84 Oracle

To fortify the security of the decentralized BB84 oracle, we integrate Post-Quantum Verifiable Random Functions (PQ-VRFs). These cryptographic primitives play a pivotal role in ensuring the verifiability and randomness of key generation within the BB84 protocol. The process involves:

1. Nodes within the decentralized BB84 oracle generating PQ-VRF proofs based on random values.

2. Achieving network consensus to validate these PQ-VRF proofs, enhancing trust and security.

3. Selecting node pairs for initiating the BB84 QKD process based on the validated proofs.

4. Proceeding with the standard BB84 protocol for quantum key distribution by the selected node pairs, now bolstered by PQ-VRFs.

5.3 Advantages of Decentralized BB84 Oracle Enhanced with PQ-VRFs

The incorporation of PQ-VRFs into the decentralized BB84 oracle offers several compelling advantages:

- **Enhanced Security:** PQ-VRFs provide an additional layer of security by ensuring the verifiability and randomness of quantum key generation, making it resistant to quantum and classical attacks.
- **Improved Trust and Transparency:** The use of PQ-VRFs enhances trust among network participants, as the verifiability of key generation processes becomes transparent and tamper-evident.
- **Resilience Against Quantum Threats:** This approach significantly bolsters the decentralized BB84 oracle's resilience against emerging quantum threats, ensuring the long-term security of blockchain systems.

By combining the decentralized BB84 oracle with PQ-VRFs, our approach provides a quantum-resistant foundation for secure key generation and distribution within blockchain networks, aligning with the evolving landscape of quantum computing.

6 Approach 2: Exploring Decentralized QRNGs for Future Blockchain Integration

Our second strategy focuses on the exploration and potential deployment of Decentralized Quantum Random Number Generators (DQRNGs) within blockchain networks. While this approach is currently conceptual, it holds promise in harnessing the inherent randomness of quantum mechanics to strengthen blockchain cryptography.

6.1 Unlocking Enhanced Cryptographic Security with QRNGs

QRNGs represent a compelling avenue for elevating cryptographic security to unprecedented levels. They offer the ability to generate cryptographic keys and encrypt data using quantum-level randomness, surpassing the capabilities of classical Random Number Generators (RNGs). The integration of QRNGs into blockchain networks has the potential to significantly enhance security, safeguarding against both existing and future computational threats.

6.2 Pioneering Future Deployment of Decentralized QRNGs

The vision of deploying Decentralized Quantum Random Number Generators (DQRNGs) within blockchain networks is an area of ongoing research and innovation. This strategy entails the distribution of QRNG capabilities across blockchain nodes, aligning seamlessly with the decentralized ethos of blockchain technology.

However, it is essential to acknowledge the formidable technical and operational challenges associated with this endeavor. Achieving uniformity and reliability in quantum entropy quality across the network is a complex task that requires meticulous design and testing. Overcoming these challenges is crucial for the successful integration of DQRNGs and the realization of their potential in enhancing blockchain security.

As we delve deeper into the exploration of DQRNGs, we remain committed to addressing these challenges and working toward a future where blockchain networks can harness the power of quantum randomness to fortify their cryptographic foundations.

7 Current Focus and Future Directions

7.1 Immediate Focus on Quantum Network Integration with Blockchain

Currently, our efforts are concentrated on establishing a robust interface between the quantum network and classical blockchain systems. This includes the development of an effective decentralized oracle system to manage the translation and integration of quantum cryptographic elements into blockchain infrastructures.

7.2 Long-Term Vision for Decentralized Quantum Technologies

In the long term, we aim to advance the integration of decentralized quantum technologies, such as DQRNGs, into blockchain systems. This progression will be contingent on the maturation of quantum technologies and their alignment with the distributed, trustless ethos of blockchain networks.

7.3 Ongoing Research and Development

Our ongoing research and development efforts are dedicated to exploring these innovative quantum-resistant strategies, ensuring that blockchain networks remain secure and resilient in the face of evolving quantum computing capabilities.

8 Current Focus and Future Directions

8.1 Immediate Focus on Quantum Network Integration with Blockchain

Our immediate focus is on establishing a robust interface between the quantum network and classical blockchain systems, specifically within the context of decentralized BB84, Post-Quantum Verifiable Random Functions (vRF), and Quantum Random Number Generators (QRNG). This endeavor encompasses the development of an efficient decentralized oracle system to facilitate the seamless translation and integration of quantum cryptographic elements into blockchain infrastructures.

8.2 Long-Term Vision for Decentralized Quantum Technologies

In the long term, our vision is to advance the integration of decentralized quantum technologies, including Decentralized Quantum Random Number Generators (DQRNGs), within blockchain systems. The realization of this vision will be contingent on the maturation of quantum technologies and their alignment with the decentralized, trustless ethos intrinsic to blockchain networks.

8.3 Ongoing Research and Development

Our persistent research and development efforts are dedicated to the exploration and refinement of innovative quantum-resistant strategies. We are committed to ensuring that blockchain networks remain secure and resilient in the face of evolving quantum computing capabilities through the incorporation of decentralized BB84, vRF, and QRNG technologies.

8.4 Synthesis of Comparative Insights

Summarizing our comparative analysis, we recognize that both the current implementation of the BB84 protocol within the Kirk Network, enhanced by Post-Quantum Verifiable Random Functions (vRF), and the prospective development of Decentralized Quantum Random Number Generator (DQRNG) modules offer distinctive approaches to fortifying blockchain security in the context of quantum computing threats.

The current implementation of the BB84 protocol within the Kirk Network signifies a significant stride in operationalizing quantum-resistant strategies. This approach emphasizes practical application, immediate quantum security enhancements, and the integration of Post-Quantum vRF to bolster security. Despite the inherent complexities and investments involved, it underscores a proactive stance in countering quantum computing risks while maintaining decentralization.

Conversely, DQRNG modules represent a forward-looking and future-focused strategy that seamlessly aligns with the decentralized nature of blockchain. While these modules are in the conceptual stage and not yet realized, their potential to provide enhanced security through genuine quantum randomness is substantial. This approach signifies a long-term vision, with the ultimate goal of fully integrating quantum advancements into the decentralized framework of blockchain, complementing the decentralized BB84 and vRF approach.

9 Scalability Analysis

While the BB84 protocol, complemented by Post-Quantum Verifiable Random Functions (vRF) and Quantum Random Number Generators (QRNG), provides robust security, its scalability within a decentralized network, particularly for blockchain systems spanning a global scale, remains a significant challenge.

The scalability challenge encompasses various aspects:

9.1 Efficient Distribution of Quantum Keys

Efficiently distributing quantum keys across a decentralized blockchain network is a complex task. Ensuring that quantum keys reach their intended recipients while maintaining the security and integrity of the keys is crucial. Future research efforts are directed toward optimizing key distribution mechanisms to accommodate large and diverse node populations.

9.2 Maintenance of Network Integrity

As blockchain networks grow in size and diversity, maintaining network integrity becomes increasingly vital. Ensuring that all nodes operate in a trustworthy manner and that the network remains secure against various threats, including quantum attacks, is a multifaceted challenge. The integration of Post-Quantum vRF and QRNG adds an additional layer of complexity to network integrity management.

9.3 Uniformity in Quantum Entropy Quality

The deployment of Decentralized Quantum Random Number Generators (DQRNGs) across decentralized nodes raises questions about the uniformity of quantum entropy quality. Consistency in the randomness generated by DQRNGs is essential to ensure the reliability and security of blockchain operations. Research and development efforts are focused on standardizing and optimizing the quality of quantum entropy generated by DQRNGs.

9.4 Network-Wide Synchronization

Synchronizing the activities and operations of a globally distributed blockchain network is a critical consideration. Maintaining synchronization is not only

important for the proper functioning of blockchain consensus mechanisms but also for the coordinated use of quantum cryptographic elements. Achieving network-wide synchronization is a fundamental challenge in the practical implementation of DQRNGs in blockchain systems.

Ultimately, the choice between the two strategies, decentralized BB84 with vRF and DQRNGs, may depend on a variety of factors:

- **Immediacy of Quantum Threats:** The urgency of countering quantum threats may influence the choice of strategy.
- **Availability of Resources:** The resources available for development and implementation play a significant role in strategy selection.
- **Long-Term Strategic Objectives:** The long-term objectives of a blockchain network, including its vision for quantum-resilience, guide decision-making.

The BB84 protocol, coupled with Post-Quantum vRF, offers a more immediate and concrete solution to quantum security challenges. It provides practical application and immediate enhancements, making it suitable for addressing imminent quantum threats.

Conversely, DQRNGs hold the promise of a more deeply integrated and inherently decentralized quantum-resilient blockchain future. While they are currently in the conceptual stage, their potential for providing enhanced security through true quantum randomness is substantial. This approach represents a long-term vision, aligning with the decentralized nature of blockchain networks.

As the field of quantum computing continues to evolve, so too will the strategies for maintaining blockchain security. A flexible and forward-looking approach to the development and implementation of these strategies is imperative to address the dynamic nature of quantum threats and ensure the security of blockchain systems.

10 Conclusion

This paper has meticulously examined the integration of the BB84 protocol within the Kirk Network as a pragmatic approach to enhance blockchain security against the looming quantum computing threat. Grounded in the fundamental principles of quantum mechanics, this approach showcases a promising synergy between quantum key distribution and blockchain technology.

While the BB84 protocol within the Kirk Network signifies a significant leap towards quantum-resistant blockchain systems, it is not without its challenges, particularly concerning integration and scalability, especially when deployed across diverse blockchain architectures.

Furthermore, the concept of decentralized Quantum Random Number Generator (QRNG) modules, in alignment with the decentralized ethos of blockchain, has been discussed as a forward-looking strategy. The development of DQRNG

modules holds immense potential for advancing the field of blockchain cryptography. However, it is essential to acknowledge that DQRNGs currently represent a long-term goal, contingent on the evolution of quantum technology and its seamless integration into blockchain infrastructure.

In conclusion, our study underscores the paramount importance of continuous research and development in the realm of quantum-resistant blockchain technologies. The choice between prioritizing the implementation of the BB84 protocol or exploring the potential of DQRNG modules, or even a combination of both, will be contingent on several factors. These factors include the immediate security needs of blockchain networks, the pace of progress in quantum technology, and strategic considerations related to resource allocation and long-term objectives.

As the quantum computing landscape continues to evolve at a rapid pace, it is imperative that blockchain methodologies evolve in parallel. This evolution is essential to ensure the robust protection of blockchain-based systems against emerging quantum threats. Only by embracing a flexible and forward-looking approach can we safeguard the sustainability and resilience of blockchain technologies in an era increasingly influenced by the rapid advancements in quantum computing.

Annexes

A.1 MVP with Numana: Current and Future Integration Tests

To evaluate the integration of the quantum network with classical blockchain networks through a decentralized oracle, we have outlined a testing strategy that caters to both current capabilities with the BB84 protocol and prospective developments like DQRNGs.

A.1.1 Interface Functionality and Performance Tests

1. Interface Setup: Establish and validate the interface between the current quantum network (using BB84 protocol) and classical blockchain networks.
2. Functionality Testing: Assess the ability of the interface to effectively transmit BB84-derived keys to blockchain networks. Future tests will include QRNG outputs upon development.
3. Performance Metrics: Evaluate throughput, latency, and reliability of the interface under diverse operational conditions, focusing on current quantum-to-blockchain integration.

A.1.2 Security Assessment of the Interface

1. Quantum Security Features: Test and verify the security enhancements provided by BB84 keys in blockchain applications, with a roadmap for future QRNG integration.

2. Eavesdropping Resistance: Examine the interface's capability in preventing unauthorized interception of quantum keys, focusing on current quantum cryptographic standards.

3. Quantum vs Classical Threats: Contrast the interface's defense mechanisms against both quantum and classical cybersecurity threats.

A.1.3 Integration and Scalability Tests

1. Blockchain Integration: Test compatibility and integration with various blockchain protocols and networks, emphasizing both public and private blockchain platforms.

2. Scalability Analysis: Assess how the interface, especially with the BB84 protocol, scales with an increasing number of nodes and transaction volumes, with projections for future QRNG capabilities.

3. Decentralized Oracle Functionality: Evaluate the effectiveness of the decentralized oracle in managing and disseminating quantum-derived information within the blockchain network, with an emphasis on current technologies and a look towards future enhancements.

A.2 Quantum-Safe Blockchain System Testing Strategy

This section outlines a comprehensive strategy for validating the quantum-safe capabilities of blockchain systems facilitated by the interface, spanning from 2024 through 2026. The strategy includes methodologies for continuous testing, improvement, and adaptation, especially as new quantum cryptographic technologies like Decentralized Quantum Random Number Generators (DQRNGs) become available. We propose a phased approach:

- **Phase 1 (2024 - Early 2025)**: Focus on integrating and stress-testing the BB84 protocol within existing blockchain frameworks. This phase will involve rigorous testing for security vulnerabilities, performance benchmarks, and compatibility assessments with current blockchain architectures.

- **Phase 2 (Late 2025)**: Initiate pilot projects to test the integration of emerging quantum technologies, such as DQRNGs, in controlled blockchain environments. This phase will explore the scalability, reliability, and security implications of DQRNGs in decentralized networks.

- **Phase 3 (2026)**: Implement a broader deployment of DQRNGs across diverse blockchain platforms, refining the technology based on feedback and performance data from Phase 2. This stage will emphasize seamless integration, ensuring minimal disruption to existing blockchain operations.

A.3 Technical Specifications and Development Roadmap

This section provides detailed specifications and operational insights into the quantum-to-blockchain interface, with a focus on the integration of quantum cryptographic elements into classical blockchain infrastructures. Key points of discussion include:

- **Current Challenges and Solutions for BB84 Implementation**: Analyze

  the technical hurdles faced during the initial integration of the BB84 protocol within blockchain networks, including quantum key distribution, node compatibility, and network security. Document innovative solutions and best practices developed during this process.

  sql

- **Development Roadmap for DQRNG Integration (2024-2026)**:
  - **2024**: Conceptualization and initial design of DQRNG modules, with emphasis on compatibility with various blockchain architectures.
  - **2025**: Development and testing of prototype DQRNG modules in controlled environments, assessing their performance, security, and integration capabilities.
  - **2026**: Rollout of DQRNG modules in broader blockchain networks, incorporating feedback and improvements from prototype testing.

A.4 Verifiable Random Function (VRF) Integration

This section outlines the testing strategy, technical specifications, and development roadmap for the integration of Verifiable Random Function (VRF) within blockchain systems. It covers aspects such as:

A.4.1 Interface Functionality and Performance Tests for VRF

1. Interface Setup: Establish and validate the interface between VRF and classical blockchain networks.
2. Functionality Testing: Assess the ability of the interface to effectively generate verifiable random values and integrate them into blockchain networks.
3. Performance Metrics: Evaluate throughput, latency, and reliability of the VRF interface under diverse operational conditions.

A.4.2 Security Assessment of VRF Integration

1. Security Features: Test and verify the security enhancements provided by VRF in blockchain applications, including resistance to manipulation and tampering.
2. Unauthorized Access: Examine the interface's capability to prevent unauthorized access to VRF-generated random values.
3. Threat Analysis: Contrast the security mechanisms of VRF against potential cybersecurity threats.

A.4.3 Integration and Scalability Tests for VRF

1. Blockchain Integration: Test compatibility and integration with various blockchain protocols and networks, emphasizing both public and private blockchain platforms.
2. Scalability Analysis: Assess how the interface scales with an increasing number of nodes and transaction volumes.
3. Decentralized Oracle Functionality: Evaluate the effectiveness of the decentralized oracle in managing and disseminating VRF-generated random values within the blockchain network.

A.4.4 Development Roadmap for VRF Integration (2024-2026)

- **2024**: Conceptualization and initial design of VRF modules, with emphasis on compatibility with various blockchain architectures.
- **2025**: Development and testing of prototype VRF modules in controlled environments, assessing their performance, security, and integration capabilities.
- **2026**: Rollout of VRF modules in broader blockchain networks, incorporating feedback and improvements from prototype testing.

References

[1] Allende, M., León, D. L., Cerón, S., Pareja, A., Pacheco, E., Leal, A., ... & Venegas-Andraca, S. E. (2023). Quantum-resistance in blockchain networks. *Scientific Reports*, 13(5664). https://doi.org/10.1038/s41598-023-32701-6

[2] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179.

[3] Jones, D. J., Merriman, B., & Gilmore, J. (2022). Quantum Origin: A quantum-safe cryptographic entropy source. *Journal of Quantum Computing*, 4(2), 156-164.

[4] Chen, L., et al. (2016). Report on Post-Quantum Cryptography. *U.S. Department of Commerce, National Institute of Standards and Technology.*

[5] Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. *Cambridge University Press.*

[6] Doyle, W. D., & Dallaire-Demers, P.-L. (2024). Lamport Authenticated Messaging for Blockchains. Pauli Group Canada.

[7] Li, Z., Tan, T. G., Szalachowski, P., Sharma, V., & Zhou, J. (2021). Post-Quantum VRF and its Applications in Future-Proof Blockchain System. arXiv:2109.02012v1 [cs.CR].