

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 1 March 2025

Hand-in Date: 8 March 2025

Hand-in Method: Online Submission via E-Learning

Assignment Report: The Impact of Quantum Computing on Bitcoin Decryption: A Comprehensive Literature Review

Student ID: 251002316

Student Name: Mohamed Elshekh

Table of Contents:

- Introduction
- Summary of Research Papers
- Critical Analysis
- Connections
- Conflicts Between the Findings
- Synthesis Matrix for Literature Review
- References

Introduction

With the rapid advancement of quantum computing, concerns have emerged regarding its impact on the security of digital currencies, particularly Bitcoin. Bitcoin relies on encryption algorithms to secure transactions and protect private keys. This review aims to analyze six research papers discussing the effect of quantum computing on Bitcoin encryption, focusing on each paper's objectives, methodology, key findings, and providing a critical analysis highlighting strengths and weaknesses. A comparative analysis is conducted to identify links and contradictions between the studies, followed by a summary table for a structured overview.

Summary of Research Papers

Paper 1: Evaluating the Quantum Threat to Bitcoin and Similar Cryptocurrencies

This paper analyzes the potential risk posed by quantum computers to Bitcoin's cryptographic security, specifically focusing on its ECDSA signature scheme. The authors conduct a theoretical analysis of a quantum attack, modeling the unconfirmed transaction time window and assessing the quantum resources required to break Bitcoin's encryption. Key findings indicate that a quantum attack is only feasible during the public key exposure before transaction confirmation. The study recommends avoiding address reuse and utilizing multigeniture (multisig) wallets as mitigation strategies. However, the research is based solely on theoretical models, assumes the existence of powerful quantum computers that do not yet exist, and lacks practical testing. (Holmes & Chen, 2021)

Paper 2: Quantum Computing Power Required to Break Bitcoin Encryption

This paper investigates the computational power necessary for a quantum computer to break Bitcoin's encryption. The authors use computational modeling to estimate the quantum resources required, incorporating the latest error correction techniques. Key findings suggest that approximately 13 million qubits are needed to break a Bitcoin key within 24 hours, while 300 million qubits would be required to achieve the same in one hour. The study concludes that Bitcoin remains secure for now, but a quantum threat could emerge within the next 10 years. However, the research depends on technical assumptions that may evolve and presumes the existence of a fully functional quantum computing model with perfect error correction, which has not yet been realized. (Webber et al., 2022)

Paper 3: Quantum Bitcoin Mining Algorithm and Its Impact on Network Security

This paper explores the potential impact of quantum computing on Bitcoin mining, proposing a hybrid quantum-classical mining algorithm that leverages Grover's algorithm for faster nonce searching. Key findings indicate that quantum mining can achieve quadratic acceleration ($\sqrt{N}$) in solving cryptographic puzzles. If a sufficiently powerful quantum computer becomes available, it could consistently outperform all traditional miners, potentially leading to a disruption in Bitcoin's proof-of-work consensus mechanism. However, the study assumes the availability of large-scale quantum computers and does not take into account quantum error correction or the high energy constraints of quantum mining. (Nagy et al., 2022)

Paper 4: A Practical Framework for Quantum-Resistant Blockchain Networks

This paper presents an experimental implementation of a quantum-secure framework for blockchain networks, specifically applied to Ethereum. The authors test three different verification methods for post-quantum digital signatures to evaluate their feasibility. Key findings demonstrate the successful implementation of a dual-signature scheme (ECDSA + Falcon), proving that quantum-resistant upgrades can be integrated without the need to rebuild an entirely new blockchain. However, the study identifies key challenges, such as increased computational overhead and the high complexity of implementation, which could hinder large-scale adoption. (Kitchener et al., 2023)

Paper 5: Comparing Performance and Security of Classical Blockchain (ECDSA) vs. Post-Quantum Blockchain (Falcon)

This paper investigates the performance and security trade-offs between classical ECDSA-based blockchains and post-quantum Falcon-based blockchains. The authors set up two identical test blockchain networks and evaluate their resilience against cyberattacks. Key findings indicate that Falcon signatures significantly enhance encryption security against quantum threats but at the cost of increased resource consumption compared to ECDSA. However, the study is limited by its focus solely on Falcon signatures, and the test environment may not fully replicate real-world blockchain conditions. (Dahhak et al., 2024)

Paper 6: Modifications to ECDSA for Enhanced Quantum-Resistant Blockchain Security

This paper explores potential modifications to ECDSA that could improve its resistance to quantum attacks. The authors conduct a theoretical analysis of three different strategies to strengthen Bitcoin's cryptographic framework, ultimately proposing a hybrid ECDSA scheme that integrates a post-quantum cryptographic (PQC) algorithm. Key findings suggest that this hybrid approach could serve as a transitional solution before a full migration to post-quantum cryptography (PQC). However, the study remains purely conceptual, lacking practical implementation or empirical validation, and its effectiveness requires further testing. (El Baraka et al., 2025)

Critical Analysis

The research on the quantum threat to blockchain security presents both strengths and limitations in addressing the risks posed by quantum computing. The studies take a comprehensive approach by evaluating cryptographic vulnerabilities, implementing experimental security solutions, and modeling the computational power required for quantum attacks. However, some critical weaknesses remain, including reliance on theoretical models, assumptions about large-scale quantum computers, and limited real-world testing. Future research should explore trade-offs between security, computational overhead, and blockchain scalability.

Connections

1. **Common Focus:** All studies examine the impact of quantum computing on blockchain security.
2. **Threat Assessment:** Each paper explores different aspects of the quantum threat.
3. **Proposed Mitigation Strategies:** Various security solutions are suggested.
4. **Performance vs. Security Trade-offs:** Studies assess computational requirements and efficiency.
5. **Implementation and Feasibility:** Some studies model threats, while others implement security solutions.

Conflicts Between Findings

1. **Theoretical vs. Practical Implementation:** Some studies model quantum threats, while others implement security measures.
2. **Encryption vs. Mining Risks:** Some focus on breaking encryption, others on mining efficiency.
3. **Hybrid vs. Full Post-Quantum Transition:** Different approaches to security upgrades.

▪ **Synthesis Matrix for Literature Review**

Year	Authors	Methodology	Key Findings	Weaknesses
2021	Holmes & Chen	Theoretical analysis of a quantum attack on Bitcoin's signature (ECDSA) + modeling of the unconfirmed transaction time window; assessment of quantum resources required and decryption time.	Found that a quantum attack is only feasible during the exposure of the public key (before transaction confirmation). Recommended avoiding address reuse and using multisig to mitigate the risk.	Based on theoretical models; assumes quantum computers of significant power which do not yet exist. No practical testing conducted.
2022	Webber et al.	Computational modeling of quantum requirements for breaking encryption; incorporating the latest error correction techniques.	Estimated that ~13 million qubits are needed to break a Bitcoin key in 24 hours, and ~300 million qubits for breaking it in one hour. Bitcoin is currently safe, but the threat may materialize within ~10 years.	Relies on technical assumptions that may change; assumes a perfect quantum computing model with sufficient error correction.
2022	Nagy et al.	Developing a hybrid quantum-classical mining algorithm utilizing Grover's algorithm for faster nonce searching.	Quantum mining achieves quadratic acceleration ($\sqrt{N}$) in finding the nonce. If a sufficiently powerful quantum computer is available, it could consistently outperform all	Assumes the availability of large-scale quantum computers. Does not consider quantum error correction or energy constraints of quantum mining.

			traditional miners.	
2023	Kitchener et al.	Experimental implementation of a quantum-secure framework on an existing blockchain (Ethereum); testing three verification methods for post-quantum signatures.	Successfully implemented a blockchain network using dual signatures (ECDSA + Falcon). Demonstrated the feasibility of quantum upgrades without rebuilding a new blockchain.	Additional computational overhead; high complexity in implementation.
2024	Dahhak et al.	Setting up two identical test blockchain networks; evaluating the impact of post-quantum signatures on performance and security under cyberattack scenarios.	Falcon signatures improved encryption security against quantum attacks but significantly increased resource consumption compared to ECDSA.	Performance results are limited to Falcon; test environment may not fully replicate real-world blockchain conditions.
2025	El Baraka et al.	Theoretical analysis of three strategies to modify ECDSA to make it more resistant to quantum attacks.	Suggested that hybrid ECDSA (dual-signature with a PQC algorithm) could serve as a transitional solution for protecting Bitcoin before a full transition to post-quantum cryptography.	A conceptual study without practical implementation; effectiveness of modifications requires further testing.

References

- Holmes, A., & Chen, B. (2021). Evaluating the Quantum Threat to Bitcoin. AVS Quantum Science [Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies](#).
- Webber, M., et al. (2022). Quantum Computing Power Required to Break Bitcoin Encryption. Physical Review X [The Impact of Hardware Specifications on Reaching Quantum Advantage in the Fault Tolerant Regime](#) ..
- Nagy, T., et al. (2022). Quantum Bitcoin Mining Algorithm and Its Impact on Network Security. IEEE Transactions on Quantum Engineering [Quantum Multi-Solution Bernoulli Search with Applications to Bitcoin's Post-Quantum Security](#).
- Kitchener, L., et al. (2023). A Practical Framework for Quantum-Resistant Blockchain Networks. Journal of Cryptographic Engineering [Quantum-resistance in blockchain networks](#).
- Dahhak, R., et al. (2024). Comparing Performance and Security of Classical Blockchain vs. Post-Quantum Blockchain. ACM Digital Library [Downtime Required for Bitcoin Quantum-Safety](#)
- El Baraka, S., et al. (2025). Modifications to ECDSA for Enhanced Quantum-Resistant Blockchain Security. Springer Journal of Cryptography and Security [Modifications to ECDSA for Enhanced Quantum-Resistant Blockchain Security](#).