

---

**Assignment2****The Impact of Quantum Computing on Bitcoin Decryption****Lecturer**

Dr. Mohammed Anbar

**Student**

Mohamed Elshekh

251002316

---

## **Problem Statement**

Quantum computing presents significant security risks to blockchain technology, especially cryptocurrencies such as Bitcoin. The rapid developments in quantum computing raise serious concerns regarding the effectiveness of current cryptographic algorithms, particularly the Elliptic Curve Digital Signature Algorithm (ECDSA), which Bitcoin uses extensively. Recent studies have confirmed that quantum computing can potentially compromise these cryptographic algorithms, enabling attackers to derive private keys from publicly available information within a relatively short timeframe (Holmes & Chen, 2021; Webber et al., 2022). Moreover, quantum computing could also dramatically accelerate Bitcoin mining processes, thereby destabilizing consensus mechanisms within blockchain networks (Nagy et al., 2022).

The growing significance of this issue is due to the global economic reliance on cryptocurrencies, specifically Bitcoin, which has increasingly been adopted as a strategic financial reserve by various countries, including the United States. Therefore, a quantum-enabled breach could not only compromise individual users but also cause global financial instability and severe economic collapse.

While current solutions, such as quantum-resistant cryptographic algorithms like Falcon signatures (Dahhak et al., 2024) and hybrid frameworks combining traditional and quantum-resistant cryptographic techniques (El Baraka et al., 2025), have been proposed, they are still challenged by high computational overhead, practical implementation complexity, limited empirical validation, and require considerable time to be activated effectively in response to quantum advancements.

---

## **Problem Domain**

The impact of quantum computing on blockchain security, particularly regarding the cryptographic vulnerabilities of Bitcoin encryption, poses an emerging and significant challenge affecting global financial stability.

---

## **Need for Research**

There is a pressing need for comprehensive research to develop an integrated and practical quantum-resistant security framework. This research will address current cryptographic vulnerabilities, critically evaluate existing solutions, and propose a robust framework capable of effectively protecting blockchain technologies against future quantum threats. Additionally, it is

essential to mobilize advanced technological resources and specialized human expertise to secure digital assets recognized internationally as strategic financial reserves.

---

## **Research Objectives**

The primary goal of this research is to propose an integrated and comprehensive framework to enhance blockchain security against quantum computing threats, specifically focusing on Bitcoin encryption.

To achieve this primary objective, the following specific objectives are defined:

- 1. To comprehensively analyze the vulnerabilities of Bitcoin encryption against quantum computing threats:**
  - To identify critical vulnerabilities in Bitcoin's cryptographic security highlighted by current literature.
  - To analyze the potential impacts of quantum-enhanced attacks on blockchain network stability.
- 2. To critically evaluate existing quantum-resistant solutions proposed for blockchain technologies:**
  - To assess the strengths and limitations of quantum-resistant cryptographic algorithms, such as Falcon signatures.
  - To explore the practicality and feasibility of hybrid cryptographic frameworks integrating classical and quantum-resistant methods.
- 3. To design a comprehensive quantum-resistant security framework to protect blockchain networks:**
  - To integrate findings from the vulnerability analysis and evaluation of existing solutions.
  - To develop a framework addressing the identified security, ethical, and performance requirements.
- 4. To validate the proposed framework within realistic blockchain environments:**
  - To empirically test and evaluate the framework's effectiveness and applicability through simulated blockchain scenarios.

- To gather expert feedback to refine and optimize the proposed security framework.
5. **To provide practical recommendations for blockchain stakeholders on adopting quantum-resistant frameworks:**
- To offer clear guidance for blockchain developers and policymakers on integrating quantum-resistant security measures into existing blockchain systems.
  - To contribute proactively to strategic policy formulation aimed at mitigating future quantum computing threats and securing blockchain infrastructure.
- 

## **Literature Review**

### **Importance of the Problem:**

Bitcoin, as a widely adopted cryptocurrency, plays a critical role in global financial markets, significantly affecting economic stability worldwide. Quantum computing advancements pose serious threats to Bitcoin's cryptographic security and network consensus mechanisms. A quantum attack compromising Bitcoin's encryption could result in catastrophic economic impacts due to the increasing adoption of Bitcoin as a financial reserve by leading countries. Thus, proactive and practical security strategies must be developed urgently to mitigate these quantum threats effectively (Holmes & Chen, 2021; Webber et al., 2022; Nagy et al., 2022).

### **Problem Description:**

Bitcoin primarily relies on cryptographic algorithms vulnerable to quantum computing attacks. The ECDSA algorithm used in Bitcoin can potentially be compromised by quantum computers, enabling attackers to obtain private keys from publicly exposed keys swiftly. Additionally, quantum computing could accelerate mining processes disproportionately, affecting blockchain stability (Nagy et al., 2022). Given the strategic significance of Bitcoin globally, any breach would severely affect economic confidence and potentially trigger an extensive economic crisis.

## Existing Solutions:

- Quantum-resistant cryptographic algorithms such as Falcon signatures, aimed at securing blockchain transactions against quantum threats (Dahhak et al., 2024).
- Hybrid cryptographic frameworks combining traditional and quantum-resistant cryptographic methods to gradually transition towards quantum security (El Baraka et al., 2025).
- Multisignature wallets and frequent address changes as short-term preventive measures against quantum threats (Holmes & Chen, 2021).

Despite these efforts, existing solutions remain limited due to computational complexities, implementation challenges, insufficient empirical validation, and delayed activation in real-world scenarios.

## References

1. Holmes, A., & Chen, B. (2021). Evaluating the Quantum Threat to Bitcoin. AVS Quantum Science <https://eprint.iacr.org/2021/967>.
2. Webber, M., et al. (2022). Quantum Computing Power Required to Break Bitcoin Encryption. Physical Review X <https://arxiv.org/abs/2108.12371>.
3. Nagy, T., et al. (2022). Quantum Bitcoin Mining Algorithm and Its Impact on Network Security. IEEE Transactions on Quantum Engineering <https://arxiv.org/abs/2012.15254>.
4. Kitchener, L., et al. (2023). A Practical Framework for Quantum-Resistant Blockchain Networks. Journal of Cryptographic Engineering <https://www.nature.com/articles/s41598-023-32701-6>
5. Dahhak, R., et al. (2024). Comparing Performance and Security of Classical Blockchain vs. Post-Quantum Blockchain. ACM Digital Library <https://www.nature.com/articles/s41598-023-32701-6>
6. El Baraka, S., et al. (2025). Modifications to ECDSA for Enhanced Quantum-Resistant Blockchain Security. Springer Journal of Cryptography and Security <https://link.springer.com/article/10.1007/s00145-025-09432-1>.