INTERNATIONAL MULTIDISCIPLINARY BOOK SERIES
https://ibseries.com/
Security and Privacy in AI Systems, Edited By: Dr. Sunita Chaudhary, Dr. Joydeb Patra

IMBS, Vol. 03, No. 1, (2025)
Open Access. Online & Print
ISSN:

CHAPTER 2
POST-QUANTUM CRYPTOGRAPHY FOR SECURING BLOCKCHAIN-BASED FINANCIAL TRANSACTIONS

Soumili Saha
BALLB Programme, Brainware University

Abstract
The rapid advancement of quantum computing poses a significant threat to classical cryptographic mechanisms that underpin blockchain-based financial systems. Current blockchain infrastructures rely heavily on public-key cryptography schemes such as Elliptic Curve Digital Signature Algorithm (ECDSA) and hashing techniques like SHA-256, which are vulnerable to quantum attacks using Shor's and Grover's algorithms (ResearchGate). This vulnerability raises critical concerns regarding the long-term security of financial transactions, including cryptocurrencies, smart contracts, and decentralized finance (DeFi) platforms.
Post-Quantum Cryptography (PQC) emerges as a promising solution by introducing cryptographic algorithms resistant to quantum attacks. This paper explores the integration of PQC into blockchain systems to enhance transaction security, data integrity, and user authentication. It evaluates key PQC algorithms such as lattice-based (CRYSTALS-Kyber, Dilithium), hash-based (SPHINCS+), and code-based cryptography. Furthermore, the study analyzes the performance implications, scalability challenges, and architectural redesign requirements associated with adopting PQC in blockchain ecosystems.
The findings indicate that while PQC significantly improves resistance against quantum threats, it introduces trade-offs in terms of computational overhead, larger key sizes, and network latency. Hybrid cryptographic models and crypto-agility frameworks are identified as practical transitional solutions for financial institutions. The study concludes that proactive adoption of PQC is essential for ensuring the resilience and future security of blockchain-based financial transactions in the emerging quantum era.

Keywords
Post-Quantum Cryptography (PQC), Blockchain Security, Quantum Computing, Financial Transactions, CRYSTALS-Kyber, Dilithium, Quantum-Resistant Algorithms, Distributed Ledger Technology (DLT), Cryptographic Agility, DeFi Security

1. Introduction

The emergence of blockchain technology has fundamentally transformed the landscape of financial transactions by enabling decentralized, transparent, and tamper-resistant systems. From cryptocurrencies such as Bitcoin and Ethereum to decentralized finance (DeFi) platforms and digital banking infrastructures, blockchain-based systems have become integral to modern financial ecosystems. These systems rely heavily on cryptographic primitives—particularly public-key cryptography and hashing algorithms—to secure communication, user authentication, and

ISBN (978-81-685212-9-2)

transaction integrity.

However, the rapid progress in quantum computing presents a significant and imminent threat to the security foundations of blockchain networks. Classical cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC), including the widely used Elliptic Curve Digital Signature Algorithm (ECDSA), derive their security from the computational difficulty of problems like integer factorization and discrete logarithms. Quantum algorithms, most notably Shor's algorithm, have demonstrated the potential to efficiently solve these problems, thereby rendering traditional cryptographic mechanisms vulnerable. Additionally, Grover's algorithm can reduce the security strength of hash functions, further exacerbating the risks to blockchain systems.

This evolving threat landscape raises serious concerns regarding the long-term viability of blockchain-based financial transactions. Sensitive financial data, digital assets, and user identities could be exposed if quantum-capable adversaries exploit these vulnerabilities. Moreover, the concept of "harvest now, decrypt later" attacks—where encrypted data is collected today and decrypted in the future using quantum computers—poses an additional layer of risk, especially for financial records requiring long-term confidentiality.

In response to these challenges, Post-Quantum Cryptography (PQC) has emerged as a critical area of research focused on developing cryptographic algorithms that are secure against both classical and quantum attacks. PQC algorithms are based on mathematically hard problems such as lattice-based constructions, hash-based signatures, and error-correcting codes, which are believed to resist quantum computational capabilities. The integration of PQC into blockchain systems offers a promising pathway to future-proof financial transactions and ensure sustained trust in decentralized financial infrastructures.

Despite its potential, the adoption of PQC within blockchain environments is not without challenges. Issues such as increased key sizes, computational overhead, scalability constraints, and compatibility with existing blockchain architectures must be carefully addressed. Therefore, a systematic exploration of PQC integration strategies, performance trade-offs, and implementation frameworks is essential.

This paper aims to analyze the role of post-quantum cryptography in enhancing the security of blockchain-based financial transactions. It examines existing vulnerabilities, evaluates suitable PQC algorithms, and discusses practical approaches for transitioning toward quantum-resistant blockchain systems.

2. Background

The convergence of blockchain technology and modern financial systems has reshaped how transactions are executed, verified, and recorded. To understand the necessity of post-quantum cryptography, it is essential to examine the foundational role of blockchain in financial ecosystems and the cryptographic mechanisms that support it.

Blockchain operates as a distributed ledger technology (DLT) where transactions are stored in a decentralized network of nodes. Each transaction is verified through consensus mechanisms and secured using cryptographic techniques, ensuring transparency, immutability, and trust without relying on centralized authorities. Financial institutions, fintech platforms, and decentralized applications increasingly depend on blockchain to deliver efficient, secure, and cost-effective services.

2.1 Blockchain in Financial Systems

Blockchain technology has become a cornerstone of innovation in the financial sector by enabling secure and decentralized transaction processing. Its application spans a wide range of financial services, fundamentally transforming traditional banking and payment systems.

Key Roles of Blockchain in Finance

1. Decentralized Transactions

Blockchain eliminates the need for intermediaries such as banks or payment processors. Peer-to-peer transactions are executed directly between participants, reducing transaction costs and processing time while increasing efficiency.

2. Enhanced Security and Transparency

Each transaction recorded on the blockchain is cryptographically secured and linked to previous transactions, forming an immutable chain. This ensures data integrity and prevents unauthorized alterations, which is critical for financial record-keeping.

3. Cryptocurrencies and Digital Assets

Blockchain serves as the underlying technology for cryptocurrencies like Bitcoin and Ethereum. These digital assets facilitate global financial transactions without the need for centralized control, enabling financial inclusion and cross-border payments.

4. Smart Contracts

Smart contracts are self-executing programs stored on the blockchain that automatically enforce contractual agreements when predefined conditions are met. They reduce the need for intermediaries and minimize the risk of fraud in financial agreements.

5. Decentralized Finance (DeFi)

DeFi platforms leverage blockchain to provide financial services such as lending, borrowing, trading, and insurance without traditional institutions. These systems rely heavily on cryptographic security for trust and automation.

Cryptographic Foundations in Blockchain Finance

Blockchain-based financial systems depend on several cryptographic components:
Public-Key Cryptography: Used for generating digital signatures and verifying transaction authenticity
Hash Functions: Ensure data integrity and link blocks securely
Digital Signatures (e.g., ECDSA): Authenticate users and authorize transactions
Consensus Mechanisms: Validate transactions across the network (e.g., Proof of Work, Proof of Stake)

Limitations in the Current Framework

While blockchain provides robust security under classical computing assumptions, its reliance on traditional cryptographic techniques exposes it to future risks:
Vulnerability of ECC and RSA to quantum attacks
Long-term exposure of financial transaction data
Dependence on fixed cryptographic standards lacking adaptability

In summary, blockchain technology has significantly enhanced the efficiency, transparency, and security of financial systems. However, its heavy dependence on classical cryptography creates potential vulnerabilities in the face of advancing quantum computing capabilities. This necessitates the exploration of quantum-resistant alternatives, which will be discussed in subsequent sections.

2.2 Quantum Threats to Blockchain

Key vulnerabilities include:
Breaking digital signatures (ECDSA)
Compromising wallet private keys
Attacking hash functions (reduced security via Grover's algorithm)

2.3 Post-Quantum Cryptography

PQC consists of algorithms based on hard mathematical problems resistant to quantum attacks, including:
Lattice-based cryptography
Code-based cryptography
Multivariate polynomial cryptography
Hash-based signatures

3. PQC Algorithms for Blockchain Security

Algorithm Type	Example	Key Features	Suitability for Blockchain
Lattice-based	CRYSTALS-Kyber, Dilithium	High security, efficient	Highly suitable
Hash-based	SPHINCS+	Stateless, secure	Large signatures
Code-based	McEliece	Strong security	Large key sizes
Multivariate	Rainbow (deprecated)	Fast signatures	Security concerns

Studies show CRYSTALS-Kyber achieves high adaptability and efficiency in financial systems.

4. Integration of PQC in Blockchain

4.1 Post-Quantum Blockchain (PQB) Architecture

Replace ECDSA with PQC signatures
Use quantum-resistant key exchange
Modify consensus mechanisms

4.2 Hybrid Cryptography Approach

Combine classical + PQC algorithms
Ensure backward compatibility
Gradual migration strategy

4.3 Smart Contract Security
PQC-secured authentication
Protection against future key exposure

5. Performance Analysis

Parameter	Classical Cryptography	PQC Algorithms
Key Size	Small	Large
Signature Size	Small	Large
Speed	Fast	Moderate
Security (Quantum)	कमजोर	Strong

Research indicates PQC introduces only minor performance overhead in some cases, while offering significantly higher security levels.

6. Challenges in PQC Adoption

6.1 Technical Challenges
Large key and signature sizes
Increased bandwidth requirements
Computational overhead

6.2 Blockchain-Specific Issues
Storage limitations
Transaction latency
Consensus redesign

6.3 Organizational Challenges
Lack of standardization
Integration with legacy systems
Regulatory uncertainty

7. Applications in Financial Transactions
PQC-secured blockchain can enhance:
Cryptocurrency security
Digital wallets
Cross-border payments
Banking systems
Smart contracts
Financial institutions are already experimenting with hybrid PQC systems to secure transactions (IJSRMT).

8. Future Research Directions
Lightweight PQC algorithms for blockchain
Scalable post-quantum consensus protocols
Integration with AI-based anomaly detection
Standardization and regulatory frameworks
Quantum-safe DeFi ecosystems

9. Conclusion
Post-Quantum Cryptography represents a critical advancement in securing blockchain-based financial transactions against emerging quantum threats. While current blockchain systems are vulnerable to quantum attacks, integrating PQC algorithms can ensure long-term data security and system integrity.

Despite challenges such as increased computational costs and system redesign requirements, hybrid approaches and crypto-agility strategies offer feasible transition pathways. As quantum computing continues to evolve, proactive adoption of PQC will be essential for maintaining trust, security, and resilience in global financial ecosystems.

References

1. Al-Janabi, S. (2025). Post-Quantum Blockchain: Challenges and Opportunities. (ResearchGate)
2. Marchsreiter, D. et al. (2025). Towards Quantum-Safe Blockchain. (IET Research Journal)
3. Revathi, K. (2025). Enhancing Blockchain Security Against Quantum Threats. (ScienceDirect)
4. AJRCOS (2025). Integrating PQC in Blockchain Systems. (Asian Journal of Computer Science)
5. IJSRMT (2025). Post-Quantum Cryptography for Secure Banking. (IJSRMT)
6. Yang, Z. (2024). Survey of Post-Quantum Blockchain Technologies. (arXiv)
7. Reddy, N.R. et al. (2025). Quantum-Secured Blockchain Framework. (Nature)
8. Fernandez-Carames, T.M., Fraga-Lamas, P. (2024). Post-Quantum Blockchain Review. (arXiv)
9. Schemitt, A.G. et al. (2025). Impact of PQC on Blockchain. (arXiv)
10. Commey, D., Crosby, G. (2025). PQS-BFL Framework. (arXiv)