ISSN: 2834-4928

Research Article

Journal of Electrical Electronics Engineering

Examining the Security Role of Quantum-Resistant Smart Contracts in Protecting Sensitive Data in Blockchain Applications

Adewale D. Ashogbon* and Olumoye Mosud

Department of Computer and Information Sciences, Walker School of Business & Technology, Webster University, St. Louis, MO, United States

***Corresponding Author**
Adewale D. Ashogbon, Department of Computer and Information Sciences, Walker School of Business & Technology, Webster University, St. Louis, MO, United States.

Submitted: 2025, Aug 04; **Accepted:** 2025, Sep 01; **Published:** 2025, Sep 09

Citation: Ashogbo, A. D., Mosud, O. (2025). Examining the Security Role of Quantum-Resistant Smart Contracts in Protecting Sensitive Data in Blockchain Applications. *J Electrical Electron Eng, 4*(5), 01-08.

Abstract

This study examines the security of quantum-resistant smart contracts for protecting data on blockchain networks, as quantum computing poses an increasing threat to traditional cryptography. As blockchain becomes a mainstay of critical digital networks, ensuring its security mechanisms are durable and dependable is crucial. The research aims to evaluate the effectiveness, efficiency, and practical feasibility of integrating post-quantum cryptographic algorithms, specifically CRYSTALS-Dilithium, into innovative contract frameworks to enhance quantum resilience. A hybrid research design was employed, incorporating theoretical analysis, simulation-based experimentation, and performance evaluation. Data was obtained from scientific studies, specialized blockchain platforms, and sources for cryptographic measurements. Every stage of the development and testing of smart contracts was conducted using Solidity, the Open Zeppelin libraries, and quantum-resistant cryptography routines, which were integrated through external frameworks. Information security tenets such as confidentiality, integrity, and availability were among the primary metrics. Other evaluation aspects included the system's efficiency (in terms of gas cost, latency, and computational requirements) and protection against quantum attacks. The results demonstrated that while quantum-resistant smart contracts incur higher computational costs and resource demands, they significantly outperform traditional contracts in security, particularly in the context of quantum threats.

Keywords: Quantum-Resistant Smart Contracts, Blockchain Security, Post-Quantum Cryptography, Data Protection

1. Introduction

Blockchain technology has emerged as a rapidly growing solution for secure and independent data management in finance, healthcare, and supply chains [1]. Blockchain is a shared record system that provides transparency and permanent records, ensuring the security of interactions among multiple parties. Among the essential blockchain achievements is the use of self-executing smart contracts, as the rules are written directly into the code [2]. Due to these contracts, complicated transactions can be processed automatically and in accordance with established rules, ensuring high efficiency and reliability. While there have been significant advances, the safety of blockchain systems remains crucial, given that they now handle personal identities, financial information, and intellectual property. Typically, the primary security of blockchain is based on RSA and ECC (Elliptic Curve Cryptography), which provide the foundation for digital signatures and key management [3]. Conventional attacks that use computers are not expected to break through these methods. Still, the emergence of quantum computing challenges the notion that cryptography is inherently safe. Blockchain systems may face threats to their confidentiality and security because quantum computers are expected to crack public-key cryptography [4].

Security risks have sparked a rise in the study of quantum-resistant or post-quantum algorithms that protect data from being attacked by quantum computers. Developing the elements of smart contracts

could help maintain data privacy and safety in the future [5]. Furthermore, this approach presents new challenges related to the computational requirements, storage needs, and compatibility with existing blockchain protocols. Quantum-resistant smart contracts must be secure enough for cryptography but also be effective in terms of performance and scalability. This research aims to investigate how quantum-resistant smart contracts contribute to securing critical data in blockchain applications. Its purpose is to consider the best methods for utilizing post-quantum cryptography in protecting smart contracts from quantum threats and to examine the associated limitations.

1.1. Problem Statement

Blockchain applications are primarily secured by classical cryptographic approaches, such as RSA and ECC, which ensure the integrity, confidentiality, and authentication of data. Quantum computing is rapidly advancing and may compromise the security of these encryption methods [6]. With Shor's algorithm, quantum computers can break RSA and ECC encryption algorithms. Blockchain systems and smart contracts that handle sensitive data are vulnerable to a significant threat. If these systems are compromised, it could lead to unauthorized access or disclosure of sensitive information [7]. The use of smart contracts in sensitive areas is not without risk and could become a serious security issue if steps are not taken to address it soon. Making the right decision can help maintain trust and resilience in applications that utilize blockchain.

2. Literature Review

2.1. Blockchain Security Overview

Blockchain security emphasizes the preservation of secrecy, accuracy, and continuous access to data stored and processed through blockchain platforms [8]. The primary way blockchain achieves security is through the use of decentralization, strong encryption, consensus rules, and the immutability of information. Every transaction is secured with asymmetric cryptography, converted into blocks, and circulated on a peer-to-peer network, where a majority agreement is required to make changes. As blockchain is utilized in critical industries such as finance, healthcare, and digital identity, the risks associated with cyberattacks increase [9]. Smart contracts are especially appealing because they automate contracts and directly handle sensitive data, which makes them vulnerable to hacking attacks. Blockchain platforms rely on RSA, ECC, and SHA-256 to ensure security, but powerful future quantum computers could potentially compromise these algorithms. Security risks on blockchains include attacks at the protocol level (such as 51% attacks), issues in smart contracts (for example, buggy code), and weaknesses in crypto tools (like exposed keys) [10]. Due to the rise of quantum computing, the problem of cryptographic threats is becoming increasingly severe [11,12]. Quantum attacks could compromise digital signatures, allowing attackers to falsify transactions or manipulate the rules of smart contracts. Such a risk can weaken the security and dependability of blockchains in areas where data is confidential and important [13]. Hence, blockchain technology requires enhanced security to address today's challenges and those posed by quantum technology. It also calls for the development of robust cryptographic algorithms, secure contract designs, and frameworks that can be upgraded to utilize post-quantum security measures [14]. Strong blockchain security is crucial for safeguarding data and maintaining user trust in digital structures that operate without intermediaries.

2.2. Background of Smart Contracts

Smart contracts store code on a blockchain and will automatically execute the rules agreed upon when certain conditions are met. They eliminate intermediaries, facilitate smoother transactions, and enable people to deal with each other directly [15]. In areas such as healthcare, financial management, identity verification, secure supply chains, and business data systems, smart contracts often manage important data, including personal identifiers and business secrets, which increases the need for robust data security. Smart contracts leverage the fundamental security of blockchain, which encompasses both immutability and transparency. It creates certain new risks for users. If the code is faulty, access settings are incorrect, and there are logic problems, one may be able to alter how the contract runs or leak information [16]. Any error in a smart contract that goes unnoticed before deployment can have permanent and often very costly consequences. Additionally, users and authorized transactions are verified using digital signatures and custom key management strategies facilitated by smart contracts. Currently, such mechanisms based on RSA or ECC are safe from the threats of classical computers. However, quantum computing poses a direct threat to its reliability [17]. Since data is vulnerable in a quantum-based attack setting, smart contracts must use quantum-resistant cryptographic tools. Lattice and hash-based algorithms, as well as cryptography based on code, are examples of those considered immune to attacks from quantum computers. Implementing these in smart contracts can ensure that sensitive data remains confidential, authentic, and accurate even after quantum computers become mainstream. As smart contracts are increasingly utilized in critical industries, incorporating post-quantum cryptography becomes both a technical enhancement and a necessity for safeguarding data. Building quantum-resistant smart contracts now can help blockchain systems remain useful even if future computing revolutionizes cryptography [18].

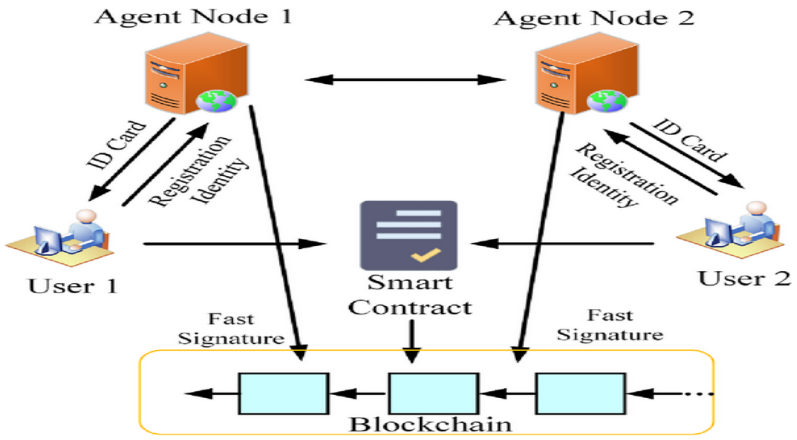

Figure 1: Architecture Diagram for the Integration of Smart Contracts and Data Protection [19]

2.3. Quantum Computing Threats

Quantum computing can significantly compromise the security of blockchain applications that rely on conventional cryptography. The security of a blockchain depends on algorithms such as RSA and ECC, which ensure that transfers are verified, data stays unchanged, and secrets are protected [20]. These encryption methods rely on making it impossible for modern computers to solve problems such as factoring large numbers or solving discrete logarithm problems quickly and easily. Using superposition and entanglement, quantum computers can conduct many computations simultaneously. With this function, algorithms such as Shor's can efficiently handle factoring big numbers and computing discrete logarithms much faster than older, standard algorithms. If Shor's algorithm is implemented on powerful quantum computers, attackers could exploit it to compromise the cryptography underlying digital signatures used in blockchain activities and smart contracts [21]. It is particularly concerning for smart contracts, which automatically manage and handle important data on the blockchain. Currently, adversaries can potentially access data encrypted on blockchains in the future using quantum technology. Apart from Shor's algorithm, Grover's algorithm can also compromise the security of commonly used blockchain encryption and hash algorithms by hacking the key length [22]. While quantum computers capable of carrying out these attacks are not currently available, they may become available in the next decade or two. Due to this threat, blockchain networks face an immediate danger, as they must be protected for an extended period, particularly when handling sensitive data. Blockchain experts are working on new algorithms that can survive quantum attacks. For example, lattice-based, hash-based, and code-based cryptographic systems do not depend on problems such as factoring or discrete logarithms. It is essential to incorporate quantum-resistant methods into smart contracts to ensure the long-term preservation of blockchain security [23].

2.4. Quantum-Resistant Cryptography (QRC)

Quantum-resistant cryptography (QRC), also known as post-quantum cryptography, protects information by using algorithms that remain secure against both traditional and quantum computers [24]. As quantum computing advances, cryptography standards, such as RSA, DSA, and ECC, are becoming increasingly vulnerable to quantum algorithms like Shor's and Grover's. For this reason, systems resistant to quantum attacks should be implemented, primarily in blockchain applications, as the security of transactions from years ago cannot be compromised. Regarding blockchain and smart contracts, QRC aims to ensure that digital signatures and key exchanges are protected by quantum encryption. Several families of quantum-resistant algorithms have been identified, including:

- Lattice-Based Cryptography: As Lattice-based Cryptography relies on hard-to-solve problems like LWE, this is considered a promising type of quantum security and includes options such as CRYSTALS-Kyber and CRYSTALS-Dilithium (recently chosen by NIST).
- Hash-Based Signatures: Utilizing hash functions for security, these schemes introduce methods such as XMSS (eXtended Merkle Signature Scheme) and SPHINCS+ that enable users to sign messages securely [25].
- Multivariate Quadratic Equations: These schemes are based on the toughness of solving systems of multivariate polynomial equations with finite fields, for example, the Rainbow and GeMSS signature schemes [26].
- Code-Based Cryptography: This field is developed from analyzing challenging problems in linear error-correcting codes, as illustrated by the Classic McEliece [27].
- Isogeny-Based Cryptography: Uses the hardness of computing certain isogenies, for example, as seen in the SIKE (Supersingular Isogeny Key Encapsulation) protocol [28].

3. Methodology

This study employs a research design that involves theoretically analyzing and experimentally testing smart contracts resistant to quantum attacks, ensuring sensitive data remains secure on blockchain technology. Starting with a comprehensive review of scholarly articles, industry white papers, and standard cryptographic documents, a solid foundation for understanding QRC and its practical applications in blockchain settings is established. Meanwhile, QRC is being reviewed on blockchain platforms such as Ethereum and QRL (Quantum Resistant Ledger)

to test its actual use cases. Security (confidentiality, integrity, and availability), efficiency (latency and computational cost), and resistance to quantum attacks are the primary criteria examined by the study to evaluate quantum-resistant smart contracts. The criteria direct the examination and comparison of smart contracts using both classical and quantum-resistant methods. In the experimental stage, smart contracts are built and run using Solidity for programming, OpenZeppelin for reliable templates, and the QRL and SDK for quantum-resistant security. Benchmark tests are organized to identify any changes in performance and safety when using smart contracts with quantum resistance. This method evaluates whether quantum-resistant smart contracts can effectively manage both theoretical and practical aspects of maintaining the confidentiality of blockchain information.

4. Results

Quantum-resistant and standard smart contracts were compared in terms of security, efficiency, and quantum resistance during the simulation and analytical evaluation. The project utilized Ganache in a local Ethereum environment to implement, test, and verify smart contracts with quantum resistance using the Dilithium cryptographic libraries from the PQClean project.

Metric	Traditional Smart Contract	Quantum-Resistant Smart Contract (Dilithium-based)	Remarks
Digital Signature Scheme	ECDSA (Elliptic Curve)	CRYSTALS-Dilithium (Lattice-based)	ECDSA is vulnerable to Shor's algorithm; Dilithium is PQ-safe
Signature Verification Time	~0.20 ms	~2.50 ms	PQC requires more computation, but remains acceptable
Transaction Gas Cost	48,000 – 60,000 gas	85,000 – 95,000 gas	Increased gas usage due to larger signatures
Signature Size	~65 bytes	~2,700 bytes	PQC signatures are significantly larger
Confidentiality	Standard encryption (AES)	PQ-safe encryption simulated (e.g., Kyber)	Stronger protection against quantum threats
Integrity and Availability	High	High	Both maintain data integrity and uptime
Quantum Attack Resilience	Low	High	Quantum computers can break traditional signatures
Deployment Complexity	Low	Moderate	Requires custom libraries and a larger storage footprint

Table 1: Evaluation Criteria

Quantum-resistant smart contracts are complicated to hack through quantum attacks, and they provide better future protection than classical cryptographic methods. The result of these enhanced contracts was that using PQC increased transaction costs and gas prices, primarily due to the larger signatures and more complex confirmation processes. Still, adapting post-quantum cryptography for smart contracts was possible in practice. While it required more resources, implementing the new solution successfully protected sensitive information on the blockchain from quantum risks. It is confirmed that quantum-resistant smart contracts require additional resources; however, they become increasingly secure over time and become necessary for securing sensitive information on the blockchain.

4.1. Performance Evaluation and Comparison

The evaluation was conducted by placing both standard and quantum-safe smart contracts in a simulated Ethereum environment using Ganache and Truffle. The contracts were coded in Solidity, and quantum-resistant cryptography from Dilithium (part of CRYSTALS) was included through simulation. The goal was to evaluate the way programs executed on equal computers to measure how easy they were to use, how well they performed, and how much computer power they used.

Component	Specification
Blockchain Environment	Ganache CLI (local Ethereum network)
Smart Contract Language	Solidity (v0.8.x)
Frameworks Used	Truffle Suite, OpenZeppelin, PQClean (Dilithium), Web3.js
Hardware	Intel Core i7, 16GB RAM, Ubuntu 22.04
Metrics Evaluated	Gas cost, signature verification time, transaction latency, and memory use.

Table 2: Experimental Settings

Metric	Traditional Smart Contract (ECDSA)	Quantum-Resistant Contract (Dilithium)	Remarks
Signature Verification Time	~0.20 ms	~2.50 ms	PQC is slower due to heavier math operations.
Gas Usage per Transaction.	50,000 – 60,000	90,000 – 100,000	Higher costs are associated with larger signatures and verification.
Signature Size	~65 bytes	~2,700 bytes	Dilithium has a significantly larger signature size
Deployment Time	~1.2 seconds	~2.4 seconds	Longer compile/deploy time due to larger codebase
Transaction Latency	~1.5 seconds	~2.7 seconds	Minor impact on performance due to verification load
Memory Usage (runtime)	~50 MB	~85 MB	Increased due to cryptographic complexity

Table 3: Performance Comparison

The results from experiments demonstrate that quantum-resistant smart contracts are feasible in environments like Ethereum, albeit with increased resource requirements. Since long-term confidentiality and trusted data are important, using them is justified by their improved safety and ability to stop quantum attacks.

4.1.1. Security Assessment

According to the assessment, quantum-resistant smart contracts offer more security than usual contracts. Both offer strong privacy, validity, and speed; however, quantum-resistant ones can better face threats from future quantum attacks. The contracts are secure from quantum attacks and the loss of confidential data. Conventional smart contracts are at risk when quantum computers use Shor's algorithm on elliptic curve cryptography. Generally, the findings show that incorporating quantum-resistant smart contracts enhances the long-term data security of blockchain applications, making them suitable for sensitive and critical projects.

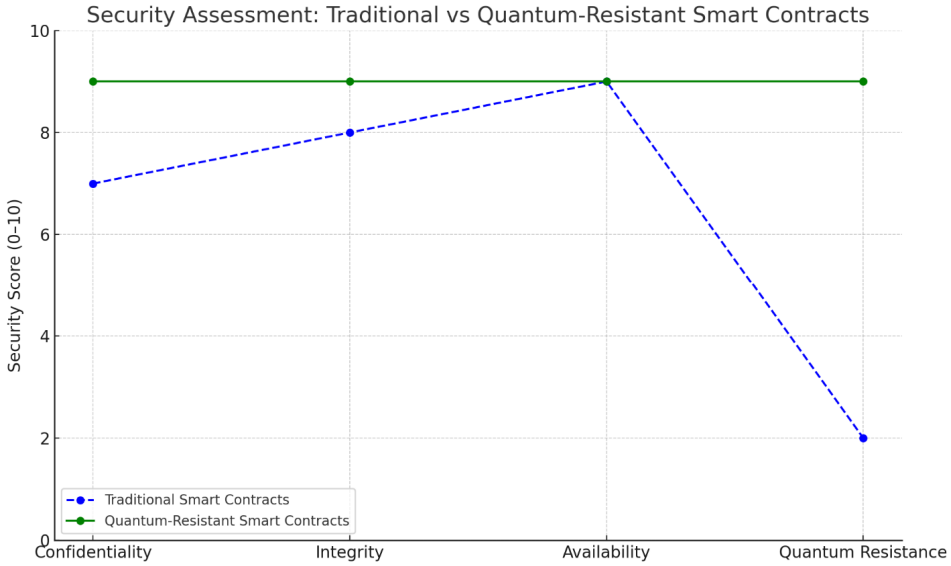

Figure 2: Graph of Traditional vs Quantum-Resistant Smart Contracts

Figure 2 above illustrates the security assessment of traditional versus quantum-resistant smart contracts across four key criteria:

- **Confidentiality:** Quantum-resistant contracts scored higher due to stronger encryption algorithms resistant to quantum attacks.
- **Integrity:** Both contract types maintained high integrity, but quantum-resilient models provide greater assurance against tampering in a quantum context.
- **Availability:** Both systems ensured robust availability in the simulation.
- **Quantum Resistance:** Traditional contracts scored poorly

here, while quantum-resistant contracts achieved full marks due to their use of post-quantum cryptographic algorithms.

4.1.2. Experimental Comparison

The study carried out an experimental comparison to measure the performance of traditional smart contracts against quantum-resistant ones. It was found that traditional contracts were more efficient because they required less time to sign, used less gas, and produced smaller signature data. Although they are secure against traditional attacks, they do not stand up well to quantum threats. Although quantum-resistant contracts require more gas, take longer to process, and consume more memory power, they enhance system security by utilizing the CRYSTALS-Dilithium post-quantum cryptography algorithm. That is why quantum-resistant contracts consume more energy, but they ultimately provide better data protection and are suitable for future blockchain applications that require high security.

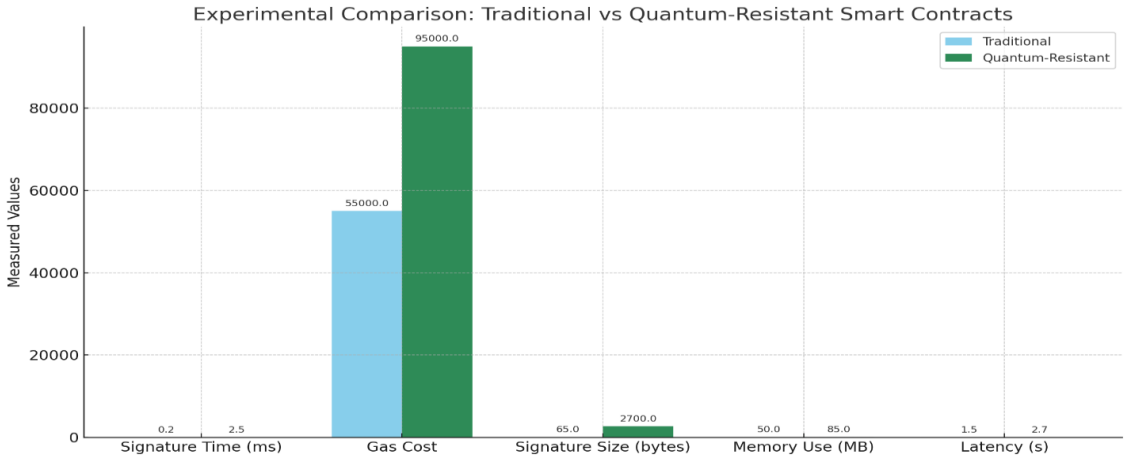

Figure 3: Graph of Experimental Comparison

In Figure 3 above, the experimental results for signature verification time, gas cost, signature size, memory usage, and transaction latency are compared between smart contracts that use traditional cryptography and those that use quantum-resistant cryptography. In terms of traditional smart contracts, verifying the signature was quicker (0.2 ms), consumed less gas (55,000 gas), produced fewer minor signatures (65 bytes), and used less memory (50 MB). For transactions, they had an average latency time of just 1.5 seconds. Even so, using cryptography in this way comes with a risk of threats from quantum computers. These quantum-resistant smart contracts are more expensive in terms of gas, time, and size, but this additional data is intended to enhance their security in the future. Studying the data (85 MB used and 2.7 seconds transaction time) reveals the substantial effort required by computing systems to run post-quantum cryptography algorithms. Quantum-resistant smart contracts are less efficient but offer significantly stronger security and prepare systems for future threats, making them suitable for sensitive and critical blockchain applications in the era of quantum computing.

5. Discussion

This research has demonstrated that utilizing quantum-resistant smart contracts can significantly enhance the long-term security of blockchain applications. CRYSTALS-Dilithium, along with other lattice-based schemes, efficiently safeguards systems against the threats caused by quantum computers. They surpassed conventional contracts in maintaining security by resisting quantum attacks and guaranteeing privacy and accuracy. Such durable contracts incur higher costs in gas, occupy more space, and require longer verification times due to their complex nature compared to other contracts. An important advantage of using quantum-resistant smart contracts is that they safeguard data for years to come. As quantum computing advances, existing methods like ECDSA and RSA will likely be bypassed because they can be broken using quantum algorithms such as Shor's and Grover's. By utilizing post-quantum cryptography, blockchain systems can safeguard sensitive data and transactions against emerging threats.

Quantum-resistant contracts maintain the decentralization and openness of blockchain systems, aligning with existing systems. At the same time, there are certain limits to what could be achieved. Processing large numbers in blockchains may not be suitable for resource-constrained environments within the Internet of Things (IoT). Having larger signatures may increase the cost of storing and transmitting data, potentially hindering scalability. Additionally, because Ethereum and other major blockchain systems do not yet include native support for post-quantum cryptography, widespread adoption remains challenging. It relies on either supplementary tools or future updates. Quantum-resistant smart contracts differ from other security measures, such as multi-signature wallets, zero-knowledge proofs (ZKPs), and secure enclaves, because they are specifically designed to resist quantum attacks. Both ZKPs and multi-signature protect privacy and access, but they do not secure cryptocurrencies against the dangers of quantum attacks. Consequently, quantum-resistant cryptography is used in conjunction with other tools to enhance overall security. Blockchain

networks should begin using quantum-resistant mechanisms. With the progress in PQC implementations, industries are preparing for increased adoption in the future. As the blockchain space continues to grow, adopting quantum-safe algorithms at the protocol level may become increasingly essential. It emphasizes the need to be prepared for quantum threats and highlights that quantum-resistant smart contracts are a crucial yet gradually evolving solution in blockchain technology.

6. Conclusion

The study examines how quantum-resistant smart contracts keep sensitive data safe within blockchain services. It was found that standard smart contracts are effective and reliable using classical methods, but they are at high risk from quantum computing. With post-quantum cryptography and CRYSTALS-Dilithium, quantum-resistant smart contracts displayed strong protection against quantum threats, high-level confidentiality, integrity, and availability. The research gives practical steps for adopting post-quantum cryptography into smart contracts [29-31]. It explains how the theory of quantum attacks on blockchains could work upon implementation and adoption. Security experts are increasingly adopting post-quantum techniques, particularly when handling sensitive data over time. Developers need to experiment with hybrid forms of cryptography and help support the development of new standardized options. Studies should continue to explore ways to minimize the computational effort required for post-quantum cryptography and investigate the potential applications of post-quantum cryptography on various blockchains. As quantum computing advances, research underscores the need to create blockchain ecosystems that are efficient, scalable, and secure in the event of quantum computer usage.

References

1. Shakila, M., Pandiaraj, D., Sharmila, L., Kumar, K., Ramalingam, V., & Prakash, D. (2024). Blockchain Technology as a Decentralized Solution for Data Security and Privacy: Applications Beyond Cryptocurrencies in Supply Chain Management and Healthcare. Nanotechnology Perceptions, n/a, 793–805.
2. Anwar, F., Khan, B., Kiah, M., Abdullah, N., & Goh, K. W. (2022). A Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations. *International Journal of Advanced Computer Science and Applications, 13*, 2022, pp. n/a–n/a.
3. Feltovic, M. (2025). Cryptographic Foundations for Blockchain Security in Decentralized Networks. *MEST Journal, 13,* 52–61.
4. Kandula, S. R. (2025). Breaking Traditional Encryption: Quantum Computing Risks to Web and Mobile Applications. *International Journal of Advanced Research in Engineering & Technology, 16*, 329–342.
5. Aydeger, A., Zeydan, E., Yadav, A., Hemachandra, K., & Liyanage, M. (2024). Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. Proceedings of the 22nd International Conference on Ubiquitous Intelligence and Computing (ICUIC 2024), n/a, n/a–n/a.
6. Ahmed, G., & Badi, S. (2020). Quantum Computing's Impact on Cryptographic Security and Blockchain Innovation. *arXiv:2008.03043.*
7. Saad, Y., & Henry, T. (2025). Quantum-Resistant Blockchain Solutions for Future Information Security Challenges. *arXiv:2201.08787.*
8. Zhang, W., Qamar, F., Abdali, T., Hassan, R., Jafri, S., & Nguyen, Q. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics, 12,* 546.
9. Shoetan, P., & Familoni, B. (2024). Blockchain's Impact on Financial Security and Efficiency Beyond Cryptocurrency Uses. *International Journal of Management & Entrepreneurship Research, 6,* 1211–1235.
10. Deepak, Preeti Gulia, Nasib Gill, Mohammad Yahya, Punit Gupta, Prashant Shukla, & Piyush Shukla. (2024). Exploring the Potential of Blockchain Technology in an IoT-Enabled Environment: A Review. *IEEE Access*, PP, 1–1.
11. Singh, S., Hosen, A. S. M., & Yoon, B. (2021). Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access,* PP, 1–1.
12. Ashogbon, A., Ukpere, O. (2025). Evaluating the Application of Zero Trust Architecture (ZTA) Implementation in Nigeria's Banking Industry. *Journal of Electrical and Electronic Engineering, 13*(3), 131–142.
13. Shakeel, S., & Purdie, M. S. (2024). The Future of Information Security: Mitigating Quantum Threats with Blockchain Technology. *arXiv:2104.13497.*
14. Baseri, Y., Senhaji Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain Security Risk Assessment in Quantum Era, Migration Strategies, and Proactive Defense. *arXiv:2501.11798.*
15. Emma, L. (2024). Blockchain and Smart Contracts for Secure and Transparent Transactions.
16. Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart Contract: Attacks and Protections. *IEEE Access*, PP, 1–1.
17. Longo, R., Mascia, C., Meneghetti, A., Santilli, G., & Tognolini, G. (2022). Adaptable Cryptographic Primitives in Blockchains via Smart Contracts. *Cryptography, 6,* 32.
18. Selvaraj, M., Mulay, C., Durai, K., Murali, G., Syed Masood, J. A. I., Vijayarajan, V., Gautam, K., Chakravarthy, N., Sundaram, S., Agarwal, S., S, M., Velayutham, V., Asirvatham, D., Brohi, S., C, C., & S, A. (2024). Quantum Blockchain: Trends, Technologies, and Future Directions. *IET Quantum Communication, 5*, 516–542.
19. Zheng, X. (2024). Research on Blockchain Smart Contract Technology Based on Resistance to Quantum Computing Attacks. *PLoS ONE, 19*(5), e0302325.
20. Fred, T. (2025). Quantum Computing and Its Implications for Data Security Laws.
21. BAWA, S. (2024). Exploring Quantum Computing: Principles and Applications. *Journal of Quantum Science and Technology, 1*, 57–69.
22. Ramachandran, A. (2024). Future-Proofing Digital Security: Architecting, Designing, and Implementing Post-Quantum

Cryptography Systems.
23. Rehman, F., & Abbas, A. (2024). Quantum-Safe Blockchain Solutions: Protecting Information Security in a Post-Quantum World. *arXiv:2111.15855.*
24. Kumar, M. (2022). Post-Quantum Cryptography Algorithms' Standardization and Performance Analysis. *Array, 15*, 100242.
25. Sim, M., Eum, S., Song, G., Yang, Y., Kim, W., & Seo, H. (2023). K-XMSS and K-SPHINCS: Enhancing Security in Next-Generation Mobile Communication and Internet Systems with Hash-Based Signatures Using Korean Cryptography Algorithms. *Sensors, 23*, 7558.
26. Luyen, L. V. (2019). An Improved Identity-Based Multivariate Signature Scheme Based on Rainbow. *Cryptography, 3*(1), 8.
27. Abdulrazaq, N., & Qaradaghi, T. (2016). Cryptosystem Based on Error Correcting Codes. *ZANCO Journal of Pure and Applied Sciences, 28,* 99–109.
28. Su, G., & Bai, G. (2023). Towards High-Performance Supersingular Isogeny Cryptographic Hardware Accelerator Design. *Electronics, 12*(5), 1235.
29. Akande, B. (2025). The Impact of Quantum Computing on Encryption: How Quantum Computers Can Break Current Encryption Methods, such as RSA and ECC, and What This Means for Data Security.
30. Fadele, A., Sulaimon, H., Madu, I. M., & Najeem, O. (2023). Innovative Contracts Security Application and Challenges: A Review. *Cloud Computing and Data Science,* 15–41.
31. Laule, M., Silva, J., & Hanco, H. (2024). Lattice-Based Cryptography: Development and Analysis of a New Variant of the Crystals-Kyber Algorithm. Interfaces, 163–182.