Investigating How Quantum Cryptographic Techniques Can Enhance the Security of Blockchain-Based Artificial Intelligence (AI) Models

Afroja Akther
Emporia State University

Tanzina Sultana
University of the Cumberlands

Ayesha Arobee
Emporia State University

Md Bahauddin Badhon
Emporia State University

Farhad Akter
Emporia State University

Nafiz Eashrak
Emporia State University

The integration of blockchain and artificial intelligence (AI) has revolutionized secure, transparent, and decentralized applications. However, the security of blockchain-based AI models remains reliant on classical cryptographic techniques, such as RSA and ECC, which are increasingly vulnerable to emerging quantum computing threats. This study investigates how quantum cryptographic techniques can enhance the security and resilience of blockchain-based AI applications. Specifically, it explores the role of Quantum Key Distribution (QKD) in securing key exchanges, post-quantum cryptographic (PQC) algorithms in fortifying data encryption, and quantum hashing techniques in protecting blockchain consensus mechanisms. The research evaluates the feasibility, implementation challenges, and performance implications of quantum-enhanced security frameworks for AI-driven blockchain networks. By addressing these concerns, this study establishes a foundation for developing quantum-secured blockchain infrastructures that safeguard AI transactions against future quantum threats while ensuring trust, transparency, and scalability in decentralized applications.

Keywords: blockchain, artificial intelligence, quantum cryptography, quantum key distribution, post-quantum cryptography

INTRODUCTION

Blockchain technology has emerged as a revolutionary solution for ensuring decentralized, tamper-proof data storage, making it highly suitable for AI-driven applications that require secure, transparent, and immutable records (Akter et al., 2024b; Das, 2025). By leveraging distributed ledger technology (DLT), blockchain enhances the trustworthiness of AI models by ensuring that transactions and data exchanges are secure and verifiable. However, the security of blockchain-based AI systems fundamentally depends on classical cryptographic techniques such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) (Zeydan et al., 2024). These encryption methods rely on the computational difficulty of problems like integer factorization and discrete logarithms, which provide security against conventional computing attacks. The advent of quantum computing introduces significant security risks to these cryptographic systems. Shor's Algorithm, a quantum algorithm developed by Peter Shor, has demonstrated that quantum computers can efficiently solve integer factorization and discrete logarithm problems, rendering classical cryptographic techniques vulnerable (Nkulenu, 2024). If large-scale quantum computers become practical, they could decrypt blockchain transactions that rely on current cryptographic standards, leading to severe data breaches, loss of integrity, and breakdown of trust in AI-driven applications. Therefore, it is imperative to explore quantum-resistant security mechanisms to protect blockchain-based AI systems from future quantum threats. Quantum cryptographic techniques, particularly Quantum Key Distribution (QKD), offer a promising solution by leveraging the principles of quantum mechanics to establish provably secure encryption keys that cannot be intercepted or compromised without detection (Sahu & Mazumdar, 2024).

AI-driven applications increasingly rely on blockchain to ensure the integrity and security of their transactions, particularly in finance, real state, healthcare, supply chain, luxury industries and autonomous systems (Rane et al., 2023; Hossain et al., 2025). AI models require secure data transmission, validation, and storage mechanisms, as they often handle sensitive personal and business information. Ensuring the confidentiality, integrity, and authenticity of AI-generated transactions is essential for preventing data breaches, adversarial manipulation, and unauthorized modifications (Joshi, Pandey & Kumari, 2025). However, the emerging threats posed by quantum computing challenge the effectiveness of classical encryption standards used in blockchain. Without adopting quantum-resistant security measures, blockchain-based AI applications could become susceptible to decryption attacks, allowing malicious actors to alter or compromise data integrity. One of the most promising approaches to counter quantum threats is Quantum Key Distribution (QKD), which enables two parties to share cryptographic keys securely using quantum mechanics principles such as quantum superposition and entanglement (Imran et al., 2024). Unlike traditional encryption schemes, which rely on computational complexity, QKD provides information-theoretic security, meaning that even an adversary with unlimited computational power cannot break it without being detected. This makes QKD a compelling solution for securing AI transactions on blockchain networks. Additionally, exploring other quantum-resistant cryptographic methods, such as lattice-based cryptography and quantum-resistant digital signatures, could help fortify blockchain networks against quantum-enabled cyber threats.

Given the rapid advancements in quantum computing, AI, and blockchain, there is an urgent need to study how quantum cryptographic techniques can enhance blockchain security while maintaining efficiency and scalability (Chahar, 2025). This research aims to address this gap by investigating how Quantum Key Distribution (QKD) and quantum-resistant cryptographic techniques can be effectively integrated into blockchain-based AI models. Additionally, it seeks to evaluate the impact of quantum-enhanced security measures on the performance of AI-driven smart contracts, ensuring that blockchain networks remain resilient against evolving cyber threats.

This study seeks to answer three key research questions. First, it explores how Quantum Key Distribution (QKD) can be integrated into blockchain-based AI models, focusing on secure key exchange, encryption for AI model interactions, and quantum-resistant blockchain consensus mechanisms. Second, it examines the performance implications of quantum cryptography on AI-driven smart contracts, evaluating factors such as transaction processing speed, computational overhead, and scalability challenges. Finally,

the research investigates how quantum-resistant blockchain ensures trust, immutability, and security for AI transactions, emphasizing the role of quantum-secure digital signatures, fraud prevention mechanisms, and quantum-safe consensus protocols. By addressing these research questions, this study aims to establish a comprehensive security framework for AI-driven blockchain applications, ensuring that they remain resilient in the face of emerging quantum threats. This research will contribute to the development of next-generation secure blockchain ecosystems, enabling safe AI transactions while maintaining trust, transparency, and data integrity in an era of quantum computing.

LITERATURE REVIEW

Security Challenges in Blockchain-Based AI

Blockchain technology has been widely adopted in AI-driven applications due to its ability to provide decentralization, transparency, and immutability (Rane, Choudhary & Rane, 2023). However, as blockchain networks heavily rely on classical cryptographic methods for securing transactions and smart contracts, they are increasingly vulnerable to quantum computing threats. Vulnerabilities in classical cryptography arise because AI models using blockchain depend on asymmetric encryption techniques such as RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard) (Chahar, 2025). These encryption methods rely on computationally hard mathematical problems like integer factorization and discrete logarithms, which classical computers struggle to solve efficiently. However, with the advent of quantum computing, algorithms like Shor's Algorithm can efficiently solve these problems, rendering existing cryptographic protections ineffective (Akter et al. 2024a). If quantum computers reach practical implementation, they could break blockchain security, exposing AI-driven transactions to cyber threats such as unauthorized modifications, data breaches, and identity fraud.

Another significant challenge is privacy concerns in AI models, which rely on blockchain for secure data transactions and decision-making (Nassar et al., 2020; Akther et al. 2025). AI-powered systems often process sensitive user information, including financial data, medical records, and business intelligence, necessitating stringent confidentiality measures. Traditional blockchains operate on a transparent model where transaction details are accessible to all participants within the network (Nguyen et al., 2020). While privacy-enhancing techniques like zero-knowledge proofs (ZKPs) and homomorphic encryption have been proposed, they are computationally expensive and may not be entirely resistant to quantum attacks (Zhou et al., 2024). The integration of AI and blockchain further complicates security, as AI models require frequent data exchanges, which can be exploited by adversaries if the cryptographic mechanisms are compromised.

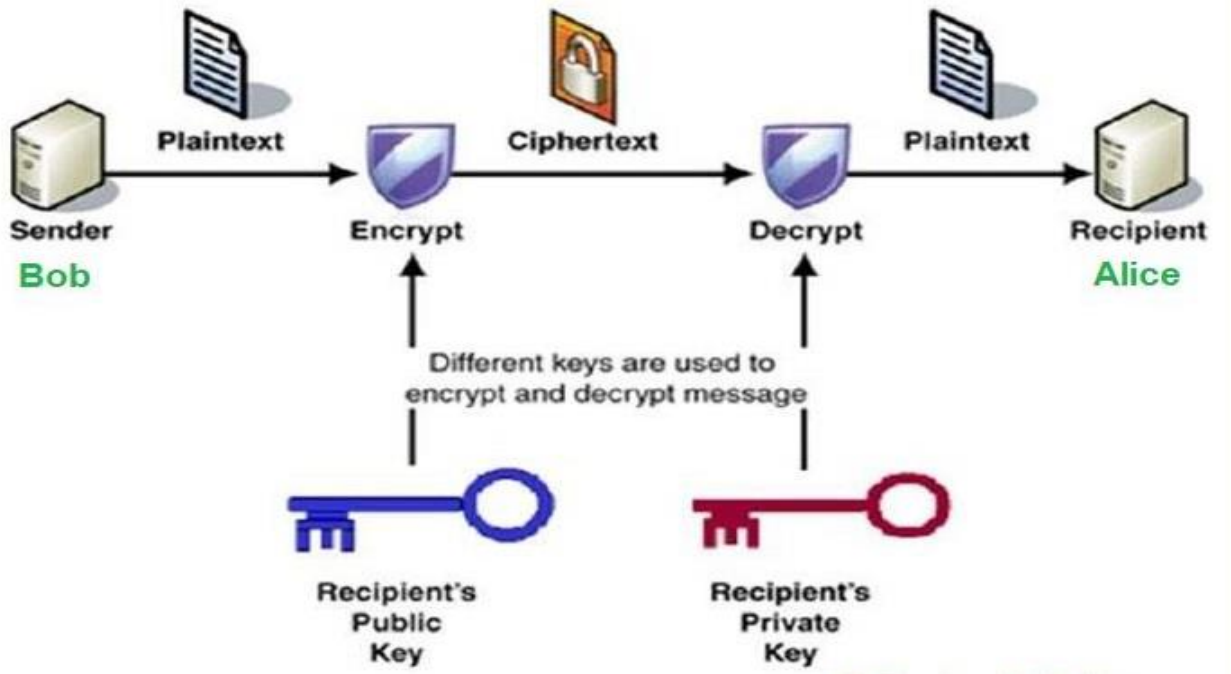
Additionally, scalability and security trade-offs present challenges in blockchain-based AI applications. Most blockchain security models emphasize data integrity and authentication, but they often struggle to balance transaction speed with cryptographic robustness (Albshaier, Budokhi & Aljughaiman, 2024). Public blockchains like Ethereum and Bitcoin face issues related to high computational costs and slower transaction processing times due to complex encryption and consensus mechanisms (Ferdous, Chowdhury & Hoque, 2021). AI-driven applications demand real-time decision-making and high transaction throughput, but current cryptographic protections often introduce delays. The need for post-quantum cryptographic solutions that provide strong security without compromising speed is becoming increasingly critical. Blockchain networks must adapt to quantum-resistant encryption techniques that not only mitigate security risks but also enhance the overall efficiency and scalability of AI-integrated blockchain ecosystems.

Quantum Cryptographic Techniques

To counteract the security challenges posed by quantum computing, several quantum cryptographic techniques (Figure 1) have been explored to enhance blockchain security for AI-driven applications. One of the most promising solutions is, in Figure 2, Quantum Key Distribution (QKD), which leverages the principles of quantum mechanics to facilitate unbreakable encryption (Sonko et al., 2024). Unlike classical key exchange protocols, which rely on mathematical complexity for security, QKD uses quantum

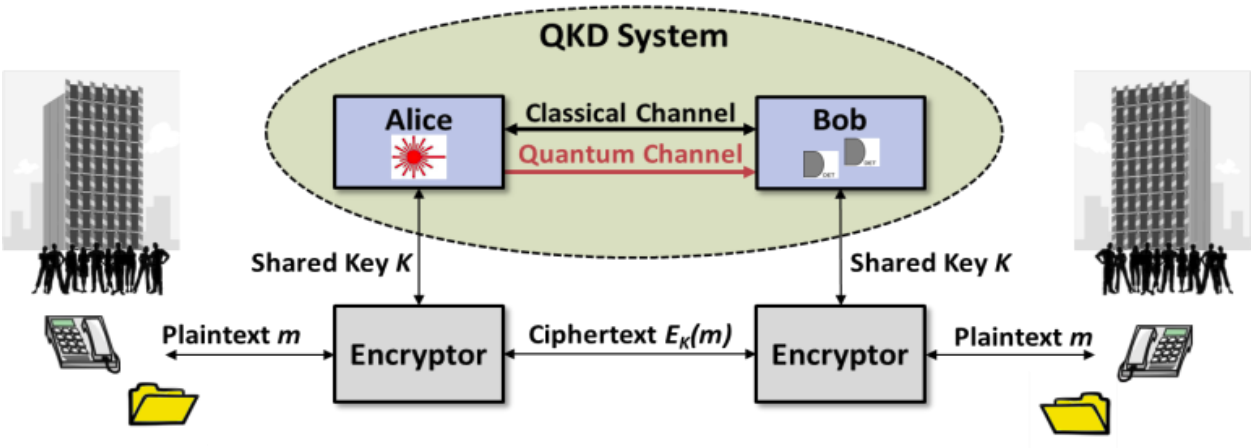
superposition and entanglement to generate and distribute encryption keys between parties securely. The most widely studied QKD protocols include BB84 and E91, which enable two communicating parties to detect any eavesdropping attempts by measuring quantum states (Ain et al., 2025). If an adversary attempts to intercept the key exchange, the quantum state collapses, alerting the users to the presence of an attacker. This inherent security property makes QKD an ideal solution for securing AI model communications, blockchain-based smart contracts, and distributed AI transactions. However, QKD requires specialized quantum hardware, including single-photon detectors and quantum repeaters, which presents implementation challenges for large-scale blockchain networks.

FIGURE 1
QUANTUM CRYPTOGRAPHY – THE PLAIN AND SIMPLE EXPLANATION



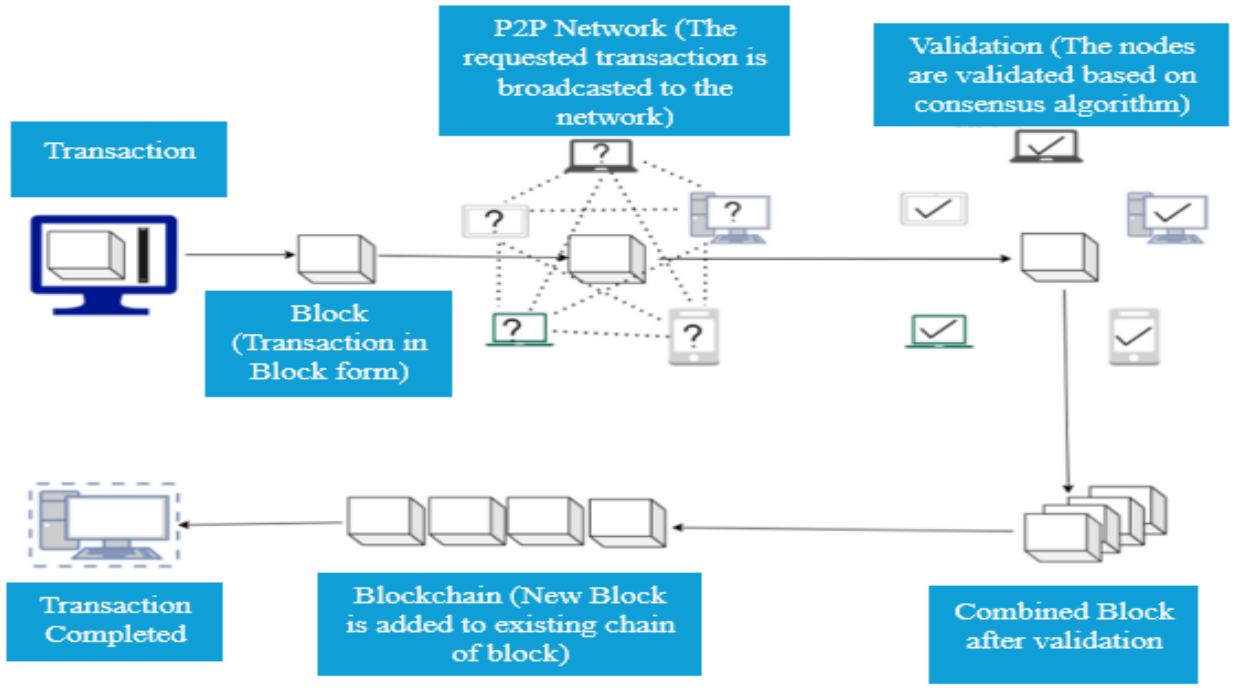
Another important quantum-resistant cryptographic approach is Post-Quantum Cryptography (PQC), which involves developing classical cryptographic algorithms that can withstand quantum attacks. Unlike QKD, which requires quantum infrastructure, PQC relies on mathematical problems that remain computationally hard even for quantum computers. Some of the most promising post-quantum cryptographic techniques include lattice-based cryptography, multivariate cryptography, and hash-based cryptography. Lattice-based encryption, for instance, is based on the difficulty of solving lattice problems such as the Learning with Errors (LWE) problem, which is resistant to both classical and quantum attacks (Sabani, Savvas & Garani, 2024). PQC is particularly attractive for blockchain-based AI applications because it does not require specialized quantum communication channels, making it a more practical solution for immediate adoption. Many blockchain platforms and cybersecurity organizations are actively researching PQC to ensure that blockchain transactions, smart contracts, and AI-driven computations remain secure in the post-quantum era (Ren et al., 2025).

FIGURE 2
QUANTUM KEY DISTRIBUTION (QKD) SYSTEM



In addition to QKD and PQC, Quantum Hashing has been proposed as a method to strengthen blockchain consensus mechanisms against quantum adversaries. Blockchain relies on cryptographic hashing functions to ensure data integrity and immutability. Current hash functions like SHA-256 and Keccak-256 are widely used in blockchain mining and transaction verification. However, quantum computers could exploit Grover's Algorithm to accelerate hash function inversion, weakening blockchain security. Quantum hashing techniques aim to develop quantum-resistant hash functions that prevent adversarial manipulation of blockchain records. These quantum-resistant hashing functions could be used in proof-of-work (PoW) and proof-of-stake (PoS) mechanisms to maintain blockchain integrity even in a quantum computing environment (Baseri et al., 2025).

FIGURE 3
POST-QUANTUM CRYPTOGRAPHY (PQC) SYSTEM



Quantum cryptographic techniques such as QKD, post-quantum cryptography, and quantum hashing represent essential advancements for securing blockchain-based AI transactions against future quantum threats. The integration of these technologies into blockchain networks will ensure that AI-driven applications continue to operate securely while maintaining data confidentiality, transaction integrity, and network resilience. Future research will need to address the implementation challenges associated with quantum cryptography, including hardware scalability, computational efficiency, and integration with existing blockchain frameworks. By developing quantum-secure blockchain solutions, AI-powered systems can achieve a higher level of trust and reliability in an era where quantum computing is expected to disrupt conventional cybersecurity paradigms.

METHODOLOGY

This study employs secondary data analysis, synthesizing existing research on quantum cryptography, blockchain security, and AI integration to propose a quantum-enhanced blockchain model. The research reviews QKD-based key management, post-quantum cryptographic techniques, and quantum-secure digital signatures (e.g., lattice-based cryptography) to enhance AI-driven blockchain transactions. Additionally, literature on quantum-enhanced consensus mechanisms is examined to assess their role in securing AI models on blockchain networks. To evaluate the feasibility of quantum-resistant blockchain, findings from simulation-based studies are analyzed, focusing on security robustness, transaction latency, and cryptographic efficiency. Comparative assessments of classical vs. quantum encryption models provide insights into performance trade-offs. A case study approach is used to review existing AI-driven healthcare blockchain applications, assessing how quantum-enhanced security improves patient data protection and ensures secure AI model interoperability in medical data exchange. This methodological approach provides a theoretical foundation for developing quantum-resistant AI blockchain applications based on validated research findings.

Enhancing Security in MediBloc's AI-Driven Blockchain Healthcare System with Quantum Cryptography

MediBloc is a decentralized blockchain-based healthcare data platform that allows patients to securely store, manage, and share their medical records with healthcare providers. The platform integrates Artificial Intelligence (AI) for predictive analytics, data processing, and personalized healthcare recommendations. MediBloc ensures data integrity, privacy, and security using blockchain, reducing the risks of unauthorized access and data tampering. However, the platform relies on classical cryptographic techniques such as RSA and ECC, which are vulnerable to quantum computing attacks. As quantum technology advances, MediBloc faces potential threats to data confidentiality and authentication mechanisms, which could expose sensitive medical records to cyber threats.

Challenges in Current Security Implementation

1. **Vulnerability to Quantum Attacks:** MediBloc's encryption methods rely on computationally hard problems (RSA, ECC) that quantum computers could easily break using Shor’s Algorithm, potentially exposing sensitive patient data.
2. **Interoperability Risks:** AI models integrated into MediBloc require secure interoperability to exchange medical data between hospitals, insurers, and researchers without security breaches.
3. **Scalability Concerns:** While blockchain ensures data immutability, secure key management and real-time AI processing introduce latency issues, making it challenging to integrate quantum-safe encryption.

Quantum-Enhanced Security Solution

To address these challenges, MediBloc could integrate Quantum Key Distribution (QKD) and Post-Quantum Cryptographic (PQC) techniques, enhancing its blockchain security –

1. **Quantum Key Distribution (QKD) for Secure Communication:** QKD enables tamper-proof encryption key exchange between patients and healthcare providers, ensuring that any eavesdropping attempts are immediately detectable. By implementing BB84 or E91 protocols, hospitals can securely transmit medical data, enhancing patient confidentiality in blockchain-based AI healthcare systems.
2. **Post-Quantum Cryptography (PQC) for Long-Term Data Protection**: To protect patient records from quantum-enabled decryption, MediBloc can adopt lattice-based cryptography (e.g., NTRUEncrypt, Kyber) instead of RSA and ECC. PQC ensures future-proof encryption and digital signatures without requiring specialized quantum hardware, making it a practical and scalable security solution.
3. **Quantum-Secure AI Model Interoperability**: AI-driven medical data exchange between patients, hospitals, and insurers requires quantum-resistant hashing to prevent tampering. Quantum-secure smart contracts can authenticate and validate patient data access requests while protecting AI-based decision-making from quantum threats.

By integrating QKD, PQC, and quantum-secure AI interoperability, MediBloc can establish a future-proof security framework, ensuring safe, private, and resilient AI-driven blockchain healthcare transactions.

Impact of Quantum Cryptographic Integration

Integrating Quantum Cryptography into MediBloc's AI-driven blockchain healthcare system ensures long-term data security and quantum-resilient interoperability. By adopting QKD and PQC, MediBloc can safeguard patient records against quantum threats while maintaining AI-driven decision-making integrity. Table 1 focuses on the limitations of current blockchain security mechanisms in AI-driven healthcare systems and presents quantum-enhanced solutions to mitigate these risks. Traditional encryption methods, such as RSA and ECC, are susceptible to quantum attacks, while classical PKI-based key exchanges lack resilience against future threats. Additionally, AI model transactions and cryptographic hashing face vulnerabilities that could compromise data integrity and interoperability in blockchain healthcare platforms. By integrating Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), and quantum hashing techniques, AI-driven blockchain networks can achieve stronger security, tamper resistance, and future-proof protection against evolving quantum cyber threats.

TABLE 1
COMPARISON OF CURRENT BLOCKCHAIN SECURITY VS. QUANTUM-ENHANCED SOLUTIONS IN AI-DRIVEN HEALTHCARE

Security Aspect	Current Blockchain Implementation	Quantum-Enhanced Solution
Data Encryption	RSA, ECC (vulnerable to quantum attacks)	Post-Quantum Cryptography (Lattice-based, Hash-based)
Key Management	Classical PKI key exchange	Quantum Key Distribution (QKD)
Interoperability	AI model transactions rely on traditional blockchain encryption	Quantum-secure AI interoperability using quantum-resistant hashing
Tamper-Resistant AI	Standard cryptographic hashing	Quantum hashing for blockchain consensus mechanisms

FINDINGS AND DISCUSSIONS

The findings of this study highlight the potential of quantum-enhanced blockchain models in securing AI-driven transactions against quantum threats. The discussion is structured around three key areas: the design of a quantum-resistant blockchain model, the evaluation of Quantum Key Distribution (QKD) for blockchain security, and the guidelines for implementing quantum-secure AI transactions. These findings

are grounded in existing theoretical frameworks and research on quantum cryptography, blockchain security, and AI integration.

A Quantum-Resistant Blockchain Model

A quantum-resistant blockchain model integrates Quantum Key Distribution (QKD), post-quantum cryptographic (PQC) algorithms, and quantum hashing techniques to enhance the security of AI-driven blockchain transactions. Traditional blockchain security mechanisms rely on asymmetric cryptography (e.g., RSA, ECC, and AES), which are vulnerable to quantum attacks due to Shor's Algorithm's ability to efficiently solve their underlying mathematical problems. In contrast, QKD leverages quantum superposition and entanglement to establish provably secure encryption keys that cannot be intercepted or compromised without detection. This eliminates a major security vulnerability in blockchain-based AI transactions.

The theoretical analysis also suggests that quantum-enhanced consensus mechanisms can improve the scalability and efficiency of blockchain networks. Current blockchain models face trade-offs between security and transaction processing speed, with complex encryption protocols often introducing delays. Quantum hashing techniques can address this issue by ensuring fast and secure transaction validation while preventing quantum adversaries from manipulating blockchain records. A hybrid quantum-blockchain architecture, which combines QKD for key exchange, lattice-based encryption for data security, and quantum hashing for consensus mechanisms, presents a robust solution for securing AI-generated transactions while maintaining high processing efficiency.

Evaluation of QKD for Blockchain Security

The integration of Quantum Key Distribution (QKD) into blockchain networks significantly enhances security by ensuring information-theoretic encryption, meaning that no computational attack, even from quantum computers, can decrypt the exchanged keys without detection. Theoretical research on BB84 and E91 QKD protocols confirms that quantum-secured key exchange eliminates traditional cryptographic vulnerability and enhances blockchain security, particularly for AI-driven applications where sensitive data, smart contracts, and automated transactions require a high degree of confidentiality and trust.

However, the practical implementation of QKD in blockchain security presents several challenges. QKD-based security models require quantum communication infrastructure, including single-photon detectors, quantum repeaters, and secure optical fiber channels, making them costly and complex to deploy. Moreover, blockchain networks currently operate on classical cryptographic infrastructures, requiring a gradual transition toward quantum-resistant protocols. Theoretical models suggest that a hybrid cryptographic approach, combining QKD for key management with post-quantum cryptographic techniques for data encryption, could provide a pragmatic solution for integrating quantum security into blockchain systems without requiring a complete infrastructure overhaul.

From a performance standpoint, the implementation of QKD-enhanced blockchain security has been evaluated in simulation-based studies, showing that it outperforms classical cryptographic methods in preventing data breaches and unauthorized access. However, scalability and efficiency remain critical concerns, as QKD introduces additional computational overhead and network requirements. Future research should focus on optimizing quantum-safe blockchain protocols to minimize these limitations while maintaining high levels of security.

Quantum-Secure AI Transactions

To ensure the long-term security of AI transactions on blockchain networks, it is essential to follow a structured quantum-security implementation strategy. The findings suggest three primary guidelines for deploying quantum-resistant AI blockchain applications –

1. **Adoption of Hybrid Cryptographic Models:** AI-powered blockchain applications should implement a dual-layer security approach that combines QKD for key exchange and post-quantum cryptographic (PQC) algorithms for data encryption. This ensures that even if quantum computers become capable of breaking traditional cryptographic methods, AI

transactions remain protected through quantum-resistant encryption techniques such as lattice-based cryptography, multivariate cryptography, and hash-based cryptographic schemes.

2. **Implementation of Quantum-Secure Digital Signatures:** The findings indicate that quantum-resistant digital signatures, such as lattice-based and hash-based signatures, are essential for securing AI-driven smart contracts and blockchain transactions. These cryptographic techniques prevent adversarial manipulation of AI models and ensure secure authentication and verification in blockchain-based decision-making processes. Replacing classical digital signatures (e.g., ECDSA and RSA) with quantum-safe alternatives will enhance the integrity and trustworthiness of AI-driven transactions.
3. **Regulatory Standardization and Compliance:** Ensuring the adoption of quantum-secure blockchain technologies requires global standardization efforts for post-quantum cryptographic protocols. Theoretical research highlights the need for regulatory frameworks that define best practices for secure AI transactions in finance, healthcare, supply chain management, and autonomous systems. Collaboration among government agencies, technology firms, and research institutions is necessary to develop universal quantum security standards, ensuring that AI-powered blockchain applications remain interoperable and resilient against quantum cyber threats.

Ensuring quantum-secure AI transactions requires a structured hybrid cryptographic approach, adoption of quantum-resistant digital signatures, and global regulatory standardization. These insights contribute to the development of next-generation secure blockchain ecosystems, ensuring that AI-driven transactions remain tamper-proof, efficient, and resilient against quantum-enabled cyberattacks.

CONCLUSION

This research outlines a blueprint for integrating quantum cryptographic techniques into AI-driven blockchain transactions, ensuring resilience against quantum threats. By combining Quantum Key Distribution (QKD), post-quantum cryptography (PQC), and quantum hashing, a secure and scalable blockchain framework can be established. Future work will focus on the real-world deployment of QKD in blockchain networks, addressing scalability, cost, and infrastructure challenges. Additionally, optimizing quantum-resistant consensus mechanisms and establishing global security standards will be key to ensuring widespread adoption. This study sets the foundation for next-generation quantum-secure AI transactions, advancing blockchain security in a quantum computing era.

ACKNOWLEDGEMENT

The authors would like to thank everyone, just everyone!

REFERENCES

Akther, A., Arobee, A., Adnan, A.A., Auyon, O., Islam, A.J., & Akter, F. (2025). *Blockchain as a platform for Artificial Intelligence (AI) Transparency*. arXiv. https://doi.org/10.48550/arXiv.2503.08699

Ain, N.U., Waqar, M., Bilal, A., Kim, A., Ali, H., Tariq, U.U., & Nadeem, M.S. (2025). A Novel Approach Based on Quantum Key Distribution Using BB84 and E91 Protocol for Resilient Encryption and Eavesdropper Detection. *IEEE Access*.

Akter, S., Bhuiyan, M., Badhon, M., Hasan, H., Akter, F., & Islam, M. (2024a) Quantum-Edge Cloud Computing for IoT: Bridging the Gap between Cloud, Edge, and Quantum Technologies. *Advances in Internet of Things*, *14*, 99–120. doi: 10.4236/ait.2024.144006.

Akter, S., Hussain, M.I., Bhuiyan, M.K.I., Sumon, S.A., Hossain, M.I., & Akhter, A. (2024b). *Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach*. http://dx.doi.org/10.2139/ssrn.5041397

Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A review of security issues when integrating IOT with cloud computing and blockchain. *IEEE Access*.

Baseri, Y., Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense. *arXiv preprint arXiv:2501.11798*.

Chahar, S. (2025). Exploring the future trends of cryptography. In *Next Generation Mechanisms for Data Encryption* (pp. 234–257). CRC Press.

Das, S.R., Jhanjhi, N.Z., Asirvatham, D., Rizwan, F., & Javed, D. (2025). Securing AI-Based Healthcare Systems Using Blockchain Technology. In *AI Techniques for Securing Medical and Business Practices* (pp. 333–356). IGI Global.

Ferdous, M.S., Chowdhury, M.J.M., & Hoque, M.A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, *182*, 103035.

Hossain, M.I., Hussain, M.I., Arobee, A., Zim, M.N.F., Badhon, M.B., & Akter, S. (2025). Balancing Innovation and Sustainability: Learn the Potential Impact on the Environment of Bitcoin Mining. *Journal of Knowledge Management Practice*, *25*(1). https://doi.org/10.62477/jkmp.v25i1.487

Imran, M., Altamimi, A.B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum Cryptography for Future Networks Security: A Systematic Review. *IEEE Access*.

Joshi, R., Pandey, K., & Kumari, S. (2025). Generative AI: A Transformative Tool for Mitigating Risks for Financial Frauds. *Generative Artificial Intelligence in Finance: Large Language Models, Interfaces, and Industry Use Cases to Transform Accounting and Finance Processes*, pp. 125–147.

Nassar, M., Salah, K., ur Rehman, M.H., & Svetinovic, D. (2020). Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(1), e1340.

Nguyen, D.C., Pathirana, P.N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, *166*, 102693.

Nkulenu, G. (2024). *Quantum Computing: The Impending Revolution in Cryptographic Security.*

Rane, N., Choudhary, S., & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. *Available at SSRN 4644253*.

Ren, X., Xu, M., Niyato, D., Kang, J., Xiong, Z., Qiu, C., . . . Wang, X. (2025). Building Resilient Web 3.0 Infrastructure With Quantum Information Technologies and Blockchain: An Ambilateral View. *Proceedings of the IEEE*.

Sabani, M.E., Savvas, I.K., & Garani, G. (2024). Learning with Errors: A Lattice-Based Keystone of Post-Quantum Cryptography. *Signals*, *5*(2), 216–243.

Sahu, S.K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in Physics*, *12*, 1456491.

Sonko, S., Ibekwe, K.I., Ilojianya, V.I., Etukudoh, E.A., & Fabuyide, A. (2024). Quantum cryptography and US digital security: a comprehensive review: Investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. *Computer Science & IT Research Journal*, *5*(2), 390–414.

Zeydan, E., Blanco, L., Mangues-Bafalluy, J., Arslan, S.S., Turk, Y., Yadav, A.K., & Liyanage, M. (2024). Blockchain-based self-sovereign identity: Taking control of identity in federated learning. *IEEE Open Journal of the Communications Society*.

Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P.C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*, 103678.