International Journal of Research in Engineering and Management Sciences (IJREMS)
E-ISSN: 3107-7439

Research Article
VOL.: 1, Issue: 2, July 2025

The Role of Quantum Computing in Strengthening Blockchain Security and Privacy Protocols

[1] Dr. Padmaja Pulicherla

*[*1] Department of Computer Science and Engineering,*
Hyderabad Institute of Technology and Management, Hyderabad, Telangana, India
Email: padmaja.j2ee@gmail.com
Orcid ID: https://orcid.org/0009-0006-6171-1238

ABSTRACT:

Blockchain is a huge component of decentralized systems, and it provides a safe and transparent way of carrying out transactions. It is though susceptible to quantum computing that could crack the RSA and ECC traditional encryption algorithms. This paper explains the risk of quantum computers and specifically of Shor Algorithm and the study of quantum- resistant cryptography, such as lattice-based cryptography, to secure blockchain systems. It also investigates quantum-enhanced encryption, e.g., quantum key distribution (QKD) which can make blockchain unbreakable encryption. The article substantiates the relevance of quantum-resistant solutions, which are being elaborated today to ensure the safety and confidentiality of blockchain in the future.

Keywords: Quantum Computing, Blockchain Security, Cryptography, Quantum-Resistant Algorithms, Privacy Protocols

Received Date: 5 July 2025**; Accepted Date:** 15 July 2025**; Published Date:** 20 July 2025.

Introduction

Since the inception of the blockchain technology, the decentralization and security in data management in the industries have witnessed a new dawn (Periyasamy et al., 2024). The fact that blockchain is a cryptography-based technology implies that it has security properties that could guarantee data integrity and eliminate the possibility of sensitive information leakage in the event of transactions processing (Periyasamy et al., 2024). The security of the blockchain networks is based on such cryptographic functions as RSA, ECC, and SHA because they provide the authentication, encryption, and data integrity options (Periyasamy et al., 2024). The transparency and immutability of blockchains can be useful to solve the issue of trusts with the help of the complex computational and cryptographic procedure of a decentralized data structure to establish a digital paradigm of trust (Periyasamy et al., 2024). However, one BIG thing is reversing all of that: the advent of quantum computing (Fernandez-Carames & Fraga-Lamas, 2020). Hypothetical quantum computers would have an exponentially faster computation speed than classical computers and hence will succeed in overwhelming the cryptographic schemes that blockchain is founded on (Ren et al., 2023). This quantum computing threat also extends to the classical communications network the quantum computer or quantum network would require because control signals and human-readable information is classical and vulnerable to cyber attacks (Peters et al., 2023).

Background of the Study

In particular, the emergence of e-commerce and e-services that are being popularized in the context of the COVID-19 outbreak have turned the security of transactions into the priority number one, and, therefore, the blockchain technology with its decentralized and distributed ledger design can be viewed as a possible solution (Sharma et al., 2023). The quantum computers present a vulnerability in blockchain systems because they can easily solve NP-hard or NP-complete problems on classical computers (Karpiinski et al., 2025). Quantum computers algorithms, e.g., Shor algorithm, are quick at factoring large integers and discrete logarithms, the Responsible problems on which many standard cryptographic systems, e.g., RSA and Ellptic Curve Cryptography, are founded (Peters et al., 2023). These weaknesses may result in the misuse of individual keys and, therefore, malicious users are capable of creating forged transactions and altering the information stored in blockchain and even launching 51 percent attacks, thus, affecting integrity and credibility of blockchain systems (Azad et al., 2025).

Justification

As the era of quantum computers approaches, it brings with it a conceptual shift in how computing is conducted and this presents both an opportunity and a challenge to the well- established systems of cryptography that blockchain technology specifically depends on. In such a way, the blockchain security mechanism is founded on the cryptographic algorithms, i.e., the hash functions and the public- key cryptography that are utilized to ensure the data integrity, authentication and confidentiality (Periyasamy et al., 2024). Such algorithms cannot be attacked classically, but with quantum computers, it is possible to reach an unknown vector and break the three basics of security in blockchain networks (FernandezCarames & FragaLamas, 2020). One of them is Shor algorithm, which offers a great threat to the majority of the public-key cryptosystems commonly in use such as RSA and Elliptic Curve Cryptography in offering security in blockchain transactions and digital signatures (Ren et al., 2023). Grover algorithms are less catastrophic than Shor, but they can speed up brute-force attacks on symmetric key algorithms and hash functions and, thus, violate immutability and integrity of blockchain data (Campagna et al., 2021). At that, the switch to quantum-safe cipher algorithms is compulsory to ensure the security and integrity of the blockchain technology when quantum computers emerge (Campagna et al., 2021).

Objectives of the Study

1. To look into how quantum computing can affect the security of the blockchain, specifically it will look at the weakness of classical cryptographic algorithms.
2. To study quantum-resistant cryptographic schemes, e.g., lattice-based cryptography, and the manner they may be integrated into blockchain protocols.
3. To analyse how quantum key distribution (QKD) contributes to better privacy and security of the blockchain.
4. To study the work and development in quantum-safe blockchain projects and protocols.
5. To offer future directions of blockchain security with regard to quantum computing.

Literature Review

It poses a threat and a potential of the blockchain technology since quantum computing can break the cryptography the security of the blockchain is built on, and, in its turn, it can also provide the means of enhancing its integrity (Ren et al., 2023). The security of blockchain systems is based on the cryptographic primitives (i.e., public-key cryptography and hash functions) the applicability of which has acquired a new dimension than ever before with the outbreak of

e-commerce and e-services (Sharma et al., 2023). Only with such cryptography tools, the authentication of data will be supported and the integrity of the stored transactions in the decentralized data system ensured (Periyasamy et al., 2024). Nevertheless, these classical cryptography protocols remain absolutely susceptible to the recently developed quantum computers, which can execute sophisticated algorithms within a short time (Dey et al., 2022).

Material and Methodology The study is based on the comprehensive review of the state of knowledge in the area of quantum computers and security of blockchain and quantum-resistant cryptography algorithms. Several research reports, cases, and academic articles have been read to get a first impression of the situation in quantum-safe blockchain protocols and the proposed cryptographic tools. In addition, a theoretical framework was created to assess the quantum-resistant cryptography and QKD addition to blockchain systems. The framework addresses the feasibility of the quantum-safe cryptography

limitations

The increasing popularity of e-commerce and e-services demonstrated the highest importance of safe methods of transactions, and the blockchain technology was regarded as an appealing option due to the decentralized and distributed ledger architecture (Sharma et al., 2023). Being a paradigm shift in computing, quantum computing with its capabilities founded on the laws of quantum mechanics can both enable and crack the existing cryptographic systems that serve as the backbone of blockchain security (Ren et al., 2023). The problem of interaction between quantum computing and blockchain technology is diversified and multidimensional since it must systematically analyze the quantum vulnerabilities that quantum algorithms introduce blockchain platforms already begin to implement it. QKD has already shown itself capable of providing additional security to communications, as well, and may be able to provide a modest degree of additional security to sensitive transactions on a blockchain.

Although quantum-resistant solutions integrated into blockchain systems sound very promising, the process is not flawless. They are computational overhead of the quantum-safe algorithms, scalability of the QKD systems and the need of the global standards in quantum cryptography and develop practical quantum-resistant cryptography (Dey et al., transition in the real blockchain networks, which are currently based on the classic cryptography algorithms.

Result and Discussion

Quantum computing is one of the threats to the security of blockchain networks. The pervasive nature of vulnerability of blockchain applications to quantum computers could be real, as the latter holds the promise of cracking classic cryptographic hashes, which are deployed to secure crypto transactions, supply chains, as well as digital identity systems.

Still, the solutions to these issues may be quantum-resistant cryptography and QKD. In particular, lattice-based cryptography already shows the gigantic promise to become a quantum-resistant algorithm, and certain

2022). After all, since its original introduction to Bitcoin in 2008, blockchain technology became a relevant method of seeking the solutions to the trust-related problems through computationally and cryptographically challenging means in a decentralized data structure to provide a digital analog of trust (Periyasamy et al., 2024). Nevertheless, the more actively the blockchain technology is being realized in a wide range of spheres of activities, the greater is the concern that its defense should be strengthened as a result of emerged quantum computational attacks. The decentralization model canceles the necessity of the central governing body and is more safe and transparent, as the database is saved in numerous nodes (Kiktenko et al., 2018).

Future Scope

The security of the current blockchain ecosystems has been compromised with the invention of quantum computing, and quantum- resistant cryptography tools will have to be envisioned and implemented (Fernandez- Carames and Fraga-Lamas, 2020). The question of how to actually deploy quantum-resistant blockchain systems needs to become the subject of future works and there are a couple of areas that are particularly important to target so that the process of migration could be secure and high- performance (Sharma et al., 2023). It so happens that one of the potential areas of interest is the scalability of quantum-safe algorithms to blockchain networks, specifically (Dey et al. 2022). The introduction of quantum-resistant algorithms into the blockchain technology would not affect the performance and throughput of the system because the latter is designed on the basis of intensive computational and cryptographic techniques to establish the trust (Periyasamy et al., 2024). That is the study, and future optimization, of post-quantum cryptography algorithms which will not be practical to attack with a quantum computer, but whose computational overhead will be modest (Peters et al., 2023). Besides it, the introduction of the Quantum Key Distribution into blockchain standards is also considered the method of ensuring superior security in the future (Marcozzi & Mostarda, 2021). QKD, which is based on the quantum mechanics that facilitates the secure transmission of encryption keys, is highly sensitive to Eavesdropping and provides privacy of blockchain transaction (Ren et al., 2023).

Conclusion

It is possible to note that quantum computing poses a significant threat to the security and privacy of blockchain networks and, in turn, there are new possibilities to improve the security of blockchain networks using quantum-resistant cryptography and quantum key distribution. As the evolution of the quantum technology is ongoing, it is provided that the blockchain systems will be forced to incorporate the quantum-safe solutions that will guarantee the security and privacy in future. One can quantum-proof blockchain networks by just fast- forwarding and introducing quantum-resistance Cryptographic processes to welcome the quantum age.

References

1. Adhikari, P., Hamal, P., & Baidoo, F. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive,13(1), 1457. https://doi.org/10.30574/ijsra.2024.13.1.1860
2. Kurshan, E., Mehta, D., Bruss, B., & Balch, T. (2024). AI versus AI in Financial Crimes and Detection: GenAI Crime Waves to Co-Evolutionary AI. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2410.09066
3. Paramesha, M., Rane, N., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: a comprehensive review [Review of Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: a comprehensive review]. SSRN Electronic Journal. RELX Group (Netherlands). https://doi.org/10.2139/ssrn.4855893
4. Sowmya, G. S., & Sathisha, H. K. (2023). Detecting Financial Fraud in the Digital Age: The AI and ML Revolution. International Journal For Multidisciplinary Research, 5(5). https://doi.org/10.36948/ijfmr 2023.v05i05.6139
5. Yesare, P. (2023). AI vs. Fraud: How Smart Algorithms are Reshaping Financial Security. International Journal of Innovative Research in Science Engineering and Technology, 12(5). https://doi.org/10.15680/ijirset.2023.1205507
6. Dasaklis, T. K., Casino, F., & Patsakis, C. (2021). SoK: Blockchain Solutions for Forensics. In Security informatics and law enforcement (p. 21). Springer International Publishing. https://doi.org/10.1007/978-3- 030-69460-9_2
7. Hossain, M. Z. (2023). Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4450488
8. Turner, A., McCombie, S., & Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. Frontiers in Computer Science, 2. https://doi.org/10.3389/fcomp.2020.600596
9. Billard, D. (2019). Blockchain-Based Digital Evidence Inventory. Journal of Advances in Information Technology, 10(2), 41. https://doi.org/10.12720/jait.10.2.41-47
10. 10. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavue, C. (2019). Blockchain Solutions for Forensic Evidence Preservation in

IoT Environments. 110. https://doi.org/10.1109/netsoft.2019.8806675

11. Chen, Y.-H. (2023). Integrating Explainable Artificial Intelligence and Blockchain to Smart Agriculture with Decision Making and Improved Security. https://doi.org/10.2139/ssrn.4446597
12. Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44. https://doi.org/10.1016/j.diin.2019.01.002 Yuan, F., Zuo, Z., Jiang, Y., Shu, W., Tian,
13. Z., Ye, C., Yang, J., Mao, Z., Huang, X., Gu, S., & Peng, Y. (2025). AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection. Algorithms, 18(5), 263. https://doi.org/10.3390/a18050263
14. Adel, N. (2024). The Impact of Digital Literacy and Technology Adoption on Financial Inclusion in Africa, Asia, and Latin America. Heliyon, 10(24). https://doi.org/10.1016/j.heliyon. 2024.e40951
15. Mytnyk, B., Tkachyk, O., Shakhovska, N., Федушко, С., & Syerov, Y. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data and Cognitive Computing, 7(2), 93. https://doi.org/10.3390/bdcc7020093
16. Luo, B., Zhen, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2023). AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2308.15992
17. Sharma, V., Pandey, B., & Kumar, V. (2016). Importance of Big Data in financial fraud detection. International Journal of Automation and Logistics, 2(4), 332. https://doi.org/10.1504/ijal.2016.080339
18. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber⋆, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications. Sensors, 21(5), 1594. https://doi.org/10.3390/s21051594