Quantum Computing: A Threat to Blockchain Technology and Potential Solutions

R Durga[1*], Shapash Shaik[2]

[1*]Department of MBA, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India.

[2]Department of Computer Science and Engineering, RK College of Engineering, Vijayawada, Andhra Pradesh, India.

[1*]rdurga@gmail.com, [2]shapazshk@gmail.com

Corresponding Author E-mail ID: [1*]rdurga@gmail.com

Abstract

This article explores the potential implications of quantum computing in the field of blockchain technology. The inherent security and immutability of blockchain technology may be compromised by the future ability of quantum computers to undermine the cryptographic methods upon which its security is built. This article examines the potential impact of quantum computing on blockchain technology, specifically focusing on the vulnerabilities that may arise from the utilization of Grover's algorithm, which might potentially undermine the validity and integrity of the blockchain. Furthermore, the essay delves into the ongoing research and development endeavors in the fields of blockchain and quantum computing. It also examines prospective remedies to address the risks associated with quantum computing, such as the use of cryptographic algorithms that are resistant to quantum attacks. The conclusion underscores the significance of remaining abreast of the most recent advancements in this domain and adopting proactive strategies to mitigate the potential impact of quantum computing on blockchain technology.

Keywords: Classical computing, Quantum computing, Blockchain technology, Cryptographic algorithms, Security.

1. INTRODUCTION

Blockchain technology and quantum computing are two dynamic and swiftly progressing domains that hold significant potential to influence the trajectory of technology and yield noteworthy ramifications across many industries. Blockchain technology is a type of ledger that is distributed and decentralized, ensuring safe, transparent, and tamper-proof recording of transactions. Fundamentally, a blockchain refers to a digital ledger that records transactions in the form of distinct blocks, which are subsequently and permanently appended to a sequential chain of blocks. Every individual block is equipped with a distinct digital signature, referred to as a hash, that serves the purpose of safeguarding the integrity of the data encapsulated within it. The series of interconnected blocks is dispersed among a network of nodes, which collaboratively authenticate transactions and uphold the integrity of the ledger. The decentralized nature of blockchain technology is considered to be one of its primary features [1]. The elimination of a central authority can result in reduced transaction costs, heightened transparency, and improved security [2].

In addition to cryptocurrencies, blockchain technology [3, 4, 5] has a diverse array of potential applications, including but not limited to supply chain identity verification, chain management, and voting systems. The current state of technology is characterized by its early stages of development,

DoI: https://doi.org/10.63949/crinfo.v1i4.004

with several unresolved challenges remaining, including scalability and the establishment of regulatory frameworks.

Quantum computing leverages quantum-mechanical principles to manipulate and analyze data, exhibiting superior computational capabilities compared to traditional computers, enabling accelerated resolution of intricate issues. The potential ramifications of this development extend across a range of sectors, encompassing drug discovery, encryption, and finance. The potential of technology to bring about revolutionary changes in various sectors is evident, notably in the domain of optimization. Quantum computers exhibit remarkable efficiency in determining optimal solutions for intricate problems, a task that would require significantly more time for classical computers to accomplish.

2. BLOCKCHAIN TECHNOLOGY AND QUANTUM COMPUTING

The convergence of blockchain technology and quantum computing has garnered growing attention and apprehension due to the possible security risks posed by quantum computing to blockchain systems [6, 7]. Quantum computers possess the ability to compromise the cryptographic algorithms that serve as the foundation for blockchain technology, so exposing it to susceptibility and potential exploitation.

Scholars are currently engaged in extensive investigation to mitigate this potential risk, which involves the creation of cryptographic algorithms that are resistant to quantum attacks [8], as well as the examination of the integration of quantum computing into blockchain frameworks. In light of the ongoing evolution of these sectors, it is imperative to remain abreast of the most recent advancements and their ramifications for many businesses.

Public-key cryptography is a fundamental component of blockchain systems, wherein data is subjected to encryption and decryption processes employing a public key and a corresponding private key. The encryption technique employed in this method is founded upon mathematical issues that have been widely recognized for their inherent complexity, such as the factorization of huge numbers into their prime constituents. Classical computers employ methods such as RSA and Elliptic Curve Cryptography (ECC) for the implementation of public-key cryptography.

However, by employing Shor's algorithm [9], a quantum computer has the potential to rapidly surpass conventional methods, as it can factorize enormous numbers at an exponential rate compared to classical algorithms. Hence, the security of numerous blockchain systems may be compromised if a quantum computer possessing an adequate quantity of qubits can undermine the public-key cryptography employed in these systems.

An illustration of the potential impact of quantum computing on cryptographic systems may be observed through the scenario where a quantum computer possessing 4000 qubits is capable of compromising the RSA encryption, which typically employs a key length of 768 bits and finds widespread application in blockchain systems. Moreover, it is well acknowledged that the ECC method provides resistance against quantum attacks alone when employed with key lengths of 256 bits or greater. However, the feasibility of implementing such longer key lengths in certain blockchain applications may be hindered by the augmented computational resources that are necessitated.

Scholars are currently engaged in the development of cryptographic algorithms that possess the capability to withstand potential dangers posed by quantum computing. These algorithms rely on the utilization of mathematical problems that prove challenging for both classical and quantum computers to

DoI: https://doi.org/10.63949/crinfo.v1i4.004

Table 1: Comparison of Classical Computing, Quantum Computing, and Blockchain Technology

Aspect	Classical Computing	Quantum Computing	Blockchain Technology
Advantages	Well-established technology. Handles many real-world problems. Easy to program and debug.	Faster for certain types of problems. Can solve problems intractable for classical computers. Supports parallel computation.	Decentralized. Immutable. Transparent. Secure.
Disadvantages	Limited processing power for some problems. Can be slow for certain tasks. Security can be compromised by quantum computers.	Still in early stages of development. High error rates and low reliability. Expensive to build and maintain. Limited scalability and algorithms.	Limited scalability. Low transaction throughput. High energy consumption. Vulnerable to 51% attacks.
Potential Impact	Limited impact on blockchain technology. Useful for data analysis in blockchain applications.	Could break existing blockchain encryption. May enable new secure and scalable blockchain systems.	Enhances security and privacy. Enables decentralized applications and smart contracts.
Current Applications	Data processing. Machine learning. Image and speech recognition. Simulation and modeling.	Chemistry and materials science. Optimization and scheduling. Cryptography and security. Simulation and modeling.	Cryptocurrency and payments. Supply chain management. Identity and authentication. Decentralized applications.

solve. The algorithms encompassed within this category consist of Lattice-based cryptography, Hash-based cryptography, and Multivariate cryptography. The use of these algorithms within blockchain systems can effectively safeguard the system's security, even when confronted with the computational capabilities of a quantum computer. The current progress in the practical advancement of quantum computers, particularly those equipped with a substantial number of qubits, remains at a nascent phase. However, it is worth noting that quantum computing has the potential to overcome the cryptographic mechanisms utilized in blockchain systems at some point in the future. The widespread availability of such machines may need a significant amount of time, ranging from many years to even decades. This extended timeframe allows for sufficient opportunity to develop and deploy cryptographic methods that are resistant to quantum computing.

3. QUANTUM-RESISTANT CRYPTOGRAPHIC

Quantum-resistant cryptographic algorithms are founded upon distinct mathematical principles compared to current cryptographic methods. The latter relies on the computational complexity of certain mathematical problems, such as the factorization of large numbers, which can be efficiently handled by quantum computers employing Shor's algorithm. On the contrary, quantum-resistant algorithms are predicated upon mathematical challenges that are deemed arduous for both classical and quantum computers alike. The advancement of quantum-resistant cryptographic algorithms entails the exploration and formulation of novel protocols for key exchange, digital signatures, encryption, and other cryptographic operations. These protocols are specifically designed to withstand potential attacks from quantum computers. Various algorithms can employ diverse mathematical notions and principles, including code-based cryptography, lattice-based cryptography, and hash-based signatures.

Quantum-resistant cryptographic algorithms are specifically developed to ensure the security and integrity of blockchain technology, rather than aim to compromise its functionality. However, its primary purpose is to safeguard the integrity and confidentiality of blockchain networks by mitigating the vulnerabilities posed by quantum computers. The viability of blockchain technology in the long run is contingent upon the development of cryptographic algorithms that are resistant to quantum computing. The potential vulnerability of cryptographic methods utilized in blockchain systems to quantum computers could pose a significant risk to the security and integrity of blockchain-based applications. The potential consequences of this phenomenon extend to several domains such as financial systems, supply chain management, and other sectors that heavily depend on the utilization of blockchain technology.

Quantum-resistant cryptographic algorithms are specifically engineered to endure potential attacks from quantum computers, which hold the capability to compromise the security of existing cryptographic methods. The algorithms in question are constructed based on various mathematical principles that are well recognized as posing significant challenges for both classical and quantum computing systems. This attribute endows them with the capability to withstand attacks from both classical and quantum computers. Currently, there is ongoing research and development in the field of quantum-resistant cryptographic algorithms. Several instances of such algorithms are being explored and designed, including:

Lattice-based Cryptography: Lattice-based cryptography refers to cryptographic systems that are built upon the mathematical framework of lattices. The resistance of this system to quantum attacks is attributed to the perceived difficulty in solving the underlying mathematical issues, which is regarded to be challenging for both classical and quantum computers.

Hash-based Signatures: The utilization of hash functions as the foundation for digital signatures [10] Hash-based signatures are commonly referred to as fare in academic literature. It is widely postulated that their resistance to quantum attacks stems from the inherent complexity of the underlying mathematical issue, which is deemed challenging for both classical and quantum computing systems.

Code-based Cryptography: Code-based cryptography refers to a cryptographic system that relies on error-correcting codes as its underlying mechanism. The resistance of this system against quantum attacks is attributed to the perceived difficulty in solving the underlying mathematical issues for both classical and quantum computers.

The burgeoning field of research and concern revolves around the potential ramifications of quantum computing on blockchain technology. The security and tamper-proof nature of blockchain technology is commonly acknowledged; yet, the advent of quantum computers poses a possible threat to its security. The potential ramifications of quantum computing on blockchain technology encompass the emergence of cryptographic flaws. Numerous blockchain systems heavily depend on cryptographic techniques, such as RSA and elliptic curve encryption, which may face vulnerability to potential decryption by a quantum computer utilizing Shor's algorithm for factoring huge numbers. The potential consequences of this situation are jeopardizing the security of private keys utilized to sign and verify transactions.

DoI: https://doi.org/10.63949/crinfo.v1i4.004

In response to this imminent challenge, scholars are actively engaged in the development of cryptographic algorithms that are resilient against quantum computing, including lattice-based cryptography, hash-based signatures, and code-based encryption. The implementation of these algorithms within blockchain systems has the potential to enhance their security against quantum attacks. Nevertheless, it is imperative to acknowledge that the advancement of practical quantum computers, possessing an adequate quantity of qubits, is currently in its nascent phase. Consequently, it may take several years or perhaps decades before they are accessible on a widespread scale.

3.1 Security Risks

The potential vulnerability of blockchain systems arises from the hypothetical scenario in which quantum computers possess the capability to compromise the cryptographic algorithms employed by these systems. In such a situation, malevolent actors could exploit this weakness to illicitly appropriate funds or modify transactions [11, 12]. The potential consequences of this phenomenon extend to financial systems that heavily depend on blockchain technology, as well as other domains such as voting systems and supply chain management.

3.2 Need for Quantum-Resistant Cryptography

Dedicated efforts are being made by researchers to develop cryptographic algorithms that are immune to quantum attacks, to mitigate the risks associated with quantum computing. These algorithms are designed to provide security against conventional attacks as well as exhibit resistance against quantum algorithms such as Shor’s algorithm.

4. DEVELOPMENT OF QUANTUM-ENABLED BLOCKCHAINS

The potential impact of quantum computing on technology includes the development of blockchains that possess quantum capabilities. These blockchains utilize the computational power of quantum computing to improve both security and performance. The integration of quantum capabilities into blockchain technology has the potential to provide improved anonymity, accelerated transaction processing, and heightened resilience against quantum computer-based assaults.

The development of quantum-resistant cryptographic algorithms [13] is a crucial field of study aimed at addressing the potential vulnerability of conventional cryptographic algorithms to quantum computing. In the context of a computing environment that accounts for post-quantum advancements, the primary objective of these algorithms is to endure potential assaults from quantum computers while ensuring the utmost security of vital data and transactions.

The following are few fundamental elements of cryptographic methods that are resistant to quantum computing.

4.1 Mathematical Foundations

Quantum-resistant cryptographic algorithms are founded upon distinct mathematical principles in comparison to the prevailing cryptographic algorithms employed in the majority of blockchain systems. The reason for this is that Shor’s algorithm [14], which has the potential to be employed by quantum computers for solving specific mathematical problems such as factoring large numbers, is not contingent upon the complexity of existing methods. In contrast, quantum-resistant algorithms are dependent on

DoI: https://doi.org/10.63949/crinfo.v1i4.004

mathematical problems such as the shortest vector problem or lattice-based encryption, which are often regarded as difficult for both classical and quantum computers [15].

4.2 Key Exchange and Encryption

To ensure robust security against quantum computers, cryptographic algorithms that are resistant to quantum assaults must have both safe key exchange [16] and encryption techniques. This entails the formulation of novel protocols for key exchange and encryption that exhibit resistance against quantum attacks, exemplified by the New Hope algorithm and the NTRU algorithm.

4.3 Standardization

The establishment of industry-recognized and endorsed standards plays a vital role in promoting the widespread adoption of cryptographic algorithms that are resistant to quantum computing. The National Institute of Standards and Technology (NIST) is now spearheading a project aimed at standardizing post-quantum cryptography algorithms. The primary objective of this endeavor is to select a collection of algorithms that can effectively withstand attacks from both conventional and quantum means.

4.4 Implementation Challenges

The implementation of quantum-resistant cryptographic algorithms is a substantial barrier due to the necessity of modifying and upgrading the already utilized systems and protocols. This may include substantial modifications to blockchain systems, such as the adoption of novel cryptographic libraries or the formulation of innovative consensus procedures.

5. THREAT TO BLOCKCHAIN BY QUANTUM COMPUTING

The development of cryptographic algorithms that are resistant to quantum effects is crucial in ensuring the security of blockchain systems in a post-quantum computing age. The algorithms under consideration are founded on distinct mathematical principles and necessitate the development of novel protocols for key exchange and encryption that exhibit resilience against quantum attacks. The establishment of standards for post-quantum cryptographic algorithms and the resolution of implementation issues are of utmost importance in ensuring the broad adoption of these algorithms in blockchain systems.

The advent of quantum computing presents two notable challenges to the security guarantees provided by blockchain technology. One potential advantage of quantum computing is its potential to greatly decrease the computational complexity associated with hash inversion, a critical process for maintaining the integrity of the upstream blockchain. The strategy proposed by Grover [17] has the potential to expedite the process of finding pre-images for a given function value in a far more efficient manner compared to standard brute-force search methods. This advancement raises concerns regarding the integrity and reliability of blockchain entries. The algorithm presented herein possesses the capability to exploit the blockchain through two distinct methodologies: firstly, by seeking hash collisions to expeditiously substitute blocks without compromising the overall integrity of the blockchain; and secondly, by expediting the generation of nonces to rapidly recreate entire chains of records, while maintaining consistent modified hashes. The aforementioned approach is utilized in both instances to ascertain the pre-image of a particular value within a complex function.

Furthermore, it should be noted that quantum computers have the capability to circumvent the security

DoI: https://doi.org/10.63949/crinfo.v1i4.004

measures employed in public/private key cryptography, which is an integral component of blockchain systems. This includes the encryption of information during exchanges between various parties as well as the generation of digital signatures. The aforementioned secondary threat underscores the necessity of incorporating cryptographic algorithms that are resistant to quantum computing and investigating quantum-resistant approaches for safeguarding blockchain technology [18].

In addition to Quantum Key Distribution (QKD) [19], researchers are now investigating several concepts that have the potential to greatly influence blockchain-based systems. One particular concept entails the direct encoding and transmission of information into a quantum stream, rather than solely utilizing a quantum channel for key distribution. A further proposition is the creation of a "Quantum Bitcoin" system that incorporates conventional blockchain ledger technology while incorporating quantum methodologies for mining and validating a block. Moreover, within the realm of quantum systems, there exist established procedures for the encoding and storage of data, such as a ledger, with the primary objective of guaranteeing its resistance to tampering. Additional possibilities encompass quantum bit commitment methods, which may potentially function as a viable substitute for digital signature techniques [20]. Although these concepts show potential, their technology readiness levels are presently quite low, with numerous implementation hurdles that are equally as complex as quantum computing itself.

6. CONCLUSION

The advancement of quantum computing poses a substantial risk to the security and integrity of blockchain technology. The security of the blockchain is susceptible to compromise due to the potential ability of quantum computers to break the cryptographic methods employed, hence posing a threat to its integrity and compromising its dependability. Nevertheless, blockchain developers and users can adopt proactive strategies to mitigate this potential risk. These strategies may involve the adoption of quantum-resistant cryptographic algorithms, the exploration of alternative quantum-resistant solutions, and the continuous monitoring of advancements in scientific research and development within this domain. By implementing this approach, individuals may effectively safeguard the security and resilience of blockchain technology in response to the potential threats presented by quantum computing.

REFERENCES

[1] S. Nakamoto, B. Bit, *et al.*, “Bitcoin: A peer-to-peer electronic cash system,” *2008*, 2007.

[2] B. Marr, “How blockchain technology could change the world,” *Forbes, May*, vol. 27, 2016.

[3] C. Puviraj, B. Nikhil, S. Vishal, K. Tamizhanban, R. Dhanalakshmi, and S. Lakshmipriya, “Study of decentralized database network using concepts of blockchain,” in *2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM)*, pp. 1–5, IEEE, 2021.

[4] M. M. Amanullah, S. Arjun, and K. Leelasankar, “Fuzzy inference system based non fungible token forum application,” in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 881–884, IEEE, 2022.

DoI: https://doi.org/10.63949/crinfo.v1i4.004

[5] H. Singh and K. Leelasankar, “Ethereum-based p2p lending system (dao app): Qualitative review of a possible replacement for lending practices,” in *International Conference on Computing, Communication, Electrical and Biomedical Systems*, pp. 369–375, Springer, 2022.

[6] M. Mosca, “Cybersecurity in an era with quantum computers: Will we be ready?,” *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[7] R. Bansal, M. Khanna, and N. K. Rajput, “A qualitative evaluation of multiple quantum computing frameworks,” in *2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, vol. 1, pp. 1296–1302, IEEE, 2024.

[8] X. Peng, Z. Liao, N. Xu, G. Qin, X. Zhou, D. Suter, and J. Du, “Quantum adiabatic algorithm for factorization and its experimental implementation,” *Physical review letters*, vol. 101, no. 22, p. 220405, 2008.

[9] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[10] S. Krendelev and P. Sazonova, “Parametric hash function resistant to attack by quantum computer,” in *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 387–390, IEEE, 2018.

[11] A. Prakash, R. Krishnaveni, and R. Dhanalakshmi, “Continuous user authentication using multimodal biometric traits with optimal feature level fusion,” *International Journal of Biomedical Engineering and Technology*, vol. 34, no. 1, pp. 1–19, 2020.

[12] R. S. Ram, S. S. Murthi, R. S. Narayanan, R. Venkatesh, R. Dhanalakshmi, and S. Bairavel, “Application to filter unwanted messages from osn user walls,” in *2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM)*, pp. 1–5, IEEE, 2021.

[13] National Institute of Standards and Technology, “Workshop on cybersecurity in a post-quantum world.” `https://www.nist.gov/news-events/events/2015/04/workshop-cybersecurity-post-quantum-world`, Apr. 2015. Accessed: Nov. 2, 2019.

[14] P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer proc 35th ann symp found comp sci (ieee computer society, los alamitos, ca),” 1994.

[15] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, “Quantum attacks on bitcoin, and how to protect against them,” *arXiv preprint arXiv:1710.10377*, 2017.

[16] ETSI Technical Committee CYBER, “Quantum-safe cryptography (qsc); limits to quantum computing applied to symmetric key sizes,” Tech. Rep. ETSI GR QSC 006 V1.1.1, European Telecommunications Standards Institute (ETSI), 2016. Accessed: Nov. 2, 2025.

[17] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

DoI: https://doi.org/10.63949/crinfo.v1i4.004

[18] I. Abdikhakimov, “The interplay of quantum computing, blockchain systems, and privacy laws: Challenges and opportunities,” *Elita. uz-Elektron Ilmiy Jurnal*, vol. 2, no. 1, pp. 1–12, 2024.

[19] E. Dervisevic, A. Tankovic, E. Fazel, R. Kompella, P. Fazio, M. Voznak, and M. Mehic, “Quantum key distribution networks-key management: A survey,” *ACM Computing Surveys*, vol. 57, no. 10, pp. 1–36, 2025.

[20] Y. Baseri, A. Hafid, Y. Shahsavari, D. Makrakis, and H. Khodaiemehr, “Blockchain security risk assessment in quantum era, migration strategies and proactive defense,” *IEEE Communications Surveys & Tutorials*, 2025.

DoI: https://doi.org/10.63949/crinfo.v1i4.004