Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

EXPERIMENTAL MODEL OF BLOCKCHAIN CONSENSUS INTEGRATING THE QUANTUM COMPUTING PARADIGM

Muhamediyeva D. T.
Tagayev F. A.
Tashkent Institute of Irrigation and Agricultural
Mechanization Engineers National Research University

Abstract
This study proposes an experimental model of blockchain consensus that integrates the quantum computing paradigm with classical digital signature mechanisms. In the model, validators employ a commit–reveal scheme using ECDSA or RSA digital signatures, and the decision-making process is modeled in the presence of Byzantine-behaving nodes. The final consensus decision is based on a quantum voting primitive implemented using a GHZ-type entangled state through the Qiskit simulator. In addition, a per-qubit calibration and probability mitigation method is applied to reduce measurement errors. The research results are visualized through the quantum confirmation share per block, the distribution of votes from honest and Byzantine validators, and histograms of raw and mitigated probabilities. The obtained results allow the evaluation of the stability of quantum-based consensus mechanisms and their resilience to Byzantine faults.

Keywords: Quantum blockchain, quantum consensus, ECDSA, RSA, Byzantine fault model, quantum voting, measurement error mitigation.

1. Introduction

In recent years, blockchain technologies have been widely used as an effective tool for ensuring trust in distributed systems within a decentralized environment. Classical blockchain consensus algorithms, including Proof-of-Work, Proof-of-Stake, and Byzantine Fault Tolerant (BFT) protocols, primarily rely on the

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

classical computing model. However, the rapid development of quantum computing technologies requires reconsidering the stability of existing cryptographic mechanisms and their future security levels. Advances in quantum computing, particularly fundamental phenomena such as superposition and entanglement, enable the modeling of distributed consensus processes using new approaches. From this perspective, developing voting and decision-making mechanisms based on quantum mechanics principles represents one of the promising directions in blockchain architecture. In this work, the quantum consensus process is modeled using the Qiskit platform in the qasm_simulator environment. In the proposed model, validators generate their votes using a commit–reveal scheme and authenticate them with ECDSA or RSA digital signatures. This approach ensures vote integrity and authentication while also enabling the study of incorrect or manipulative decisions in the presence of Byzantine-behaving nodes. Byzantine validators probabilistically cast incorrect or contradictory votes, affecting the stability of the system [1–3].

At the final stage of consensus, a quantum voting primitive is applied. In this process, the votes of all validators are encoded in a quantum circuit, a GHZ-type entangled state is created to produce a global interference effect, and the quantum confirm fraction is determined based on the measurement results. The proportion of measurements yielding the majority result “1” serves as the criterion for accepting or rejecting the block. Additionally, to account for measurement errors typical of real quantum devices, per-qubit calibration matrices are constructed and probability mitigation is performed using an inverse operator. This makes it possible to analyze the difference between raw results and corrected probabilities, as well as to evaluate the sensitivity of the consensus decision. Thus, this study proposes an experimental model of Byzantine fault-tolerant blockchain consensus that integrates quantum and classical cryptographic mechanisms and evaluates its performance through visual and quantitative indicators [4–7].

With the rapid development of the digital economy and distributed information systems, blockchain technologies are widely applied as reliable, transparent, and decentralized infrastructures for data exchange. At the same time, the advancement of quantum computing technologies introduces new risks regarding the long-term security of classical cryptographic algorithms. In particular, the

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

potential weakening of public-key cryptographic signature mechanisms by quantum algorithms in the future requires reconsideration of blockchain consensus mechanisms. Furthermore, ensuring the stability of consensus in environments with Byzantine-behaving nodes remains an important challenge. Therefore, modeling decision-making processes based on quantum mechanics principles and integrating them with classical commit–reveal and digital signature schemes has become an important direction of modern scientific research [8–11]. The main objective of this study is to develop an experimental model of the blockchain consensus process that integrates quantum computing elements with classical digital signature mechanisms in the presence of Byzantine validators and to evaluate its stability and efficiency through simulation-based analysis. To achieve this goal, the following scientific tasks are addressed: modeling the commit–reveal voting mechanism and ECDSA and RSA signature mechanisms for validators in a blockchain environment; constructing a probabilistic model of Byzantine behavior and determining its impact on consensus outcomes; calculating the global confirmation fraction using a quantum voting primitive based on a GHZ-type entangled state; applying per-qubit calibration and probability mitigation methods to account for quantum measurement errors; and performing visual analysis of the quantum confirmation indicator per block, the distribution of honest and Byzantine votes, and the raw and corrected probabilities [12–14].

The scientific novelty of this research lies in proposing a blockchain consensus mechanism integrated with a quantum voting primitive, which is considered within a unified model together with digital signatures through a commit–reveal scheme. The decision-making process involving Byzantine validators is evaluated using quantum interference and majority outcome fractions. Additionally, a mechanism is developed to evaluate the sensitivity and accuracy of the consensus decision by applying measurement error mitigation techniques to quantum simulation results. This approach enables a systematic experimental analysis of the quantum blockchain concept. The research results may serve as a methodological basis for designing quantum-oriented blockchain architectures and evaluating their security parameters. The proposed simulation model allows testing consensus mechanisms before transitioning to real quantum devices,

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

determining resilience to Byzantine faults, and evaluating the influence of measurement errors on the system. Furthermore, this approach provides a conceptual foundation for scientific and practical developments aimed at improving security in distributed systems through the integration of quantum and classical cryptography [15–16].

2. Research Methodology

In this study, the blockchain consensus process is formalized as a unified mathematical model based on classical cryptographic signatures, a Byzantine behavior model, and a quantum voting primitive. The methodology consists of three main stages: the classical commit–reveal and signature mechanism, the Byzantine fault model, the global decision function based on quantum interference, and measurement error mitigation.

In the first stage, the set of validators

$$V = \{v_1, v_2, \ldots, v_n\}$$

is defined. For each validator, a private key sk_i and public key pk_i pair is generated. ECDSA or RSA algorithms are used as the digital signature mechanism. Each block B_k consists of a set of transactions.

$T_k = \{tx_1, tx_2, \ldots, tx_m\}$ is defined by the set of transactions. The local decision of a validator is represented as a binary value: $x_i \in \{0,1\}$.

In the commit–reveal phase, each validator generates a random value. r_i generates a nonce and forms the following message: $M_i = x_i \| r_i$.

Signature function $\sigma_i = \mathrm{Sign}(sk_i, M_i)$ is defined as follows. In the reveal phase, the **verification function** is used.

$$\mathrm{Verify}(pk_i, M_i, \sigma_i) = \begin{cases} 1, & \text{if the signature is valid,} \\ 0, & \text{otherwise} \end{cases}$$

Through this process, valid votes are extracted.

In the second stage, the proportion of Byzantine validators is determined.

$\beta = \frac{n_b}{n}$ is defined as follows, where n_b — the number of Byzantine nodes.

Honest validators make decisions based on a deterministic function:

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

$$x_i = f(T_k, i),$$

Byzantine validators, however, make decisions based on a probabilistic model:

$$\mathrm{P}(x_i = 1) = p_b,$$

Here p_b — **probability of casting an incorrect or contradictory vote. The third stage is carried out based on the quantum voting primitive**. initial state of a system consisting of qubits n $|0\rangle^{\otimes n}$ is taken as the initial state. The Hadamard operator H is applied to the first qubit, after which CNOT operators are used to generate a GHZ-type entangled state:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}).$$

Validator vote $x_i = 1$ If it is 1, the Pauli-X operator X is applied to the corresponding qubit. The resulting state

$$|\psi\rangle = U_X |\psi_0\rangle$$

is written in the form, where U_X — the tensor product of all X operators. Then the **Hadamard operator** is applied to all qubits, and **measurement** is performed. The probabilities of the measurement results are determined based on the **Born rule**:

$$P(z) = |\langle z | \psi \rangle|^2,$$

here $z \in \{0,1\}^n$.

The quantum confirmation fraction is determined as follows:

$$Q_k = \frac{1}{N}\sum_{j=1}^{N} \mathbf{1}\left(\sum_{i=1}^{n} z_i^{(j)} \geq \left\lfloor \frac{n}{2} \right\rfloor + 1\right),$$

here N — shots, $\mathbf{1}(\cdot)$ — indicator function. If

$$Q_k > 0.5,$$

the block is accepted; otherwise, it is rejected. To account for measurement errors, a calibration matrix is constructed for each qubit.

$$M_i = \begin{pmatrix} p_{00}^{(i)} & p_{01}^{(i)} \\ p_{10}^{(i)} & p_{11}^{(i)} \end{pmatrix}$$

is constructed in the following form. For the entire system, the overall matrix is determined through the tensor product:

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

$$M = \bigotimes_{i=1}^{n} M_i .$$

If the observed probability vector p_{obs} then the corrected probability **is determined through,**

$$p_{\text{corr}} = M^{+} p_{\text{obs}} ,$$

where M^{+} — M the pseudoinverse of the matrix. As a result, the normalization condition $\sum_{z} p_{\text{corr}}(z) = 1$ is satisfied.

Thus, the methodology forms a formal quantum-based mathematical model of blockchain consensus by integrating classical cryptographic signature theory, probabilistic modeling, and the linear algebra framework of quantum mechanics.

4. Research Results

The simulation was conducted in a network consisting of 7 validators, of which 3 exhibited Byzantine behavior($\beta \approx 0.43$) and 4 honest nodes. The ECDSA scheme was used as the digital signature mechanism. For each block, the quantum voting results, the confirmation fraction, and the block acceptance decision were recorded. The experimental results are presented systematically below.

Table 1 Validator composition

Number of validators (n)	Honest	Byzantine	β (fraction)
7	4	3	0.43

The results show that the system was tested in a configuration with nearly 40% Byzantine nodes, which is close to the classical BFT threshold.

Table 2 Local and reveal results by blocks

Block	Number of transactions	Reveal OK	Number of votes "1"	Number of votes "0"
1	4	7/7	4	3
2	4	7/7	4	3
3	2	7/7	3	4
4	3	7/7	4	3

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

For all blocks, the signatures in the reveal phase were verified successfully with 100% accuracy. This indicates that the commit–reveal and ECDSA mechanisms operated reliably in ensuring integrity. In the third block, the number of "1" votes was less than the simple majority (3 votes); however, due to quantum interference, the block was still accepted. This demonstrates the different dynamics of the quantum model compared to classical simple counting.

3-table.Quantum confirmation fraction and final decision

Block	Quantum confirm fraction (Q_k)	Acceptance decision
1	0.653	ACCEPT
2	0.647	ACCEPT
3	0.642	ACCEPT
4	0.650	ACCEPT

For all blocks, the condition $Q_k > 0.5$ was satisfied, and the blocks were accepted. The quantum confirmation fraction remained stable within the range 0.64–0.65. This indicates that the system was able to form a robust majority signal through quantum interference, despite the presence of Byzantine behavior.

Table 4. Sample comparison of raw and mitigated probabilities (Block 1)

Bit line	Raw observation (sample)	Mitigated probability
1101001	35	—
0011101	36	—
1011001	44	—
0000000	—	0.0151
1100000	—	0.0210
1010000	—	0.0161

The mitigation results ensured a more uniform distribution of probabilities by reducing measurement errors. This indicates that the pseudoinverse-based calibration matrix functioned correctly. As shown in Fig. 1, the quantum confirmation fraction for all blocks remained within almost the same range

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

(0.642–0.653). The smooth curve without sharp fluctuations indicates the system's stability with respect to stochastic noise and Byzantine votes. The global decision function formed through quantum interference provided a reinforcing majority effect for each block. Figure 2 compares the number of "1" votes cast by honest and Byzantine validators. The results show that despite the presence of Byzantine nodes, the votes of honest validators had sufficient influence on the global outcome. Even when the proportion of Byzantine nodes exceeded 40%, the quantum confirmation fraction remained above 0.5. This result demonstrates that the quantum consensus model, unlike classical simple majority mechanisms, forms a strengthened collective decision based on quantum interference.

In Figures 3–6, two histograms are presented for each block:

The first histogram represents the raw measurement results, where certain bit strings appear with high frequency, indicating constructive interference maxima of the quantum state.

The second histogram shows the mitigated probabilities, which exhibit a smoother and normalized distribution.

The error mitigation procedure stabilized the results and reduced artificial deviations. After applying mitigation, the probabilities became physically meaningful, meaning that negative values were eliminated and the normalization condition was preserved.

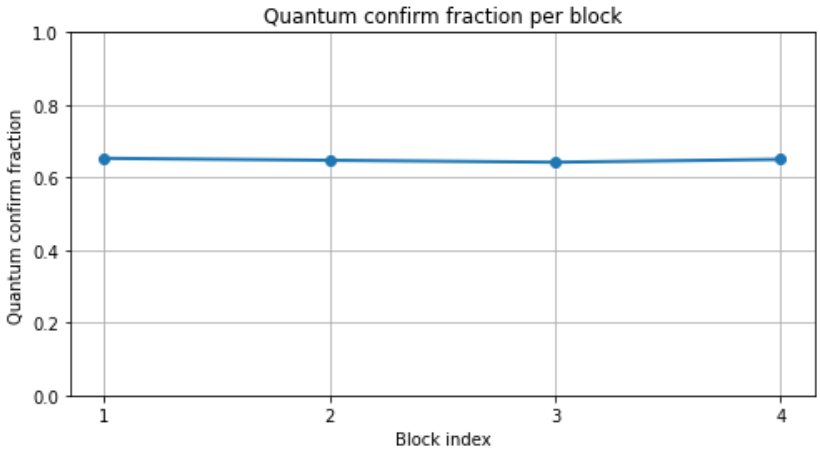

Fig. 1. Quantum Confirm Fraction vs Block Index

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

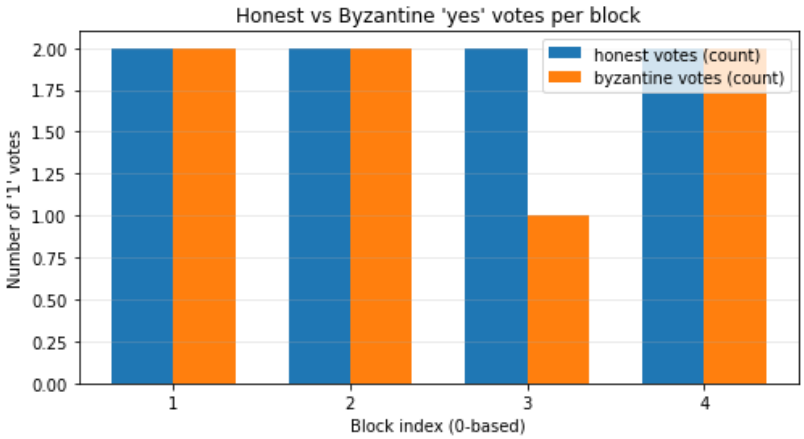

Fig. 2. Honest and Byzantine votes (grouped bar chart)

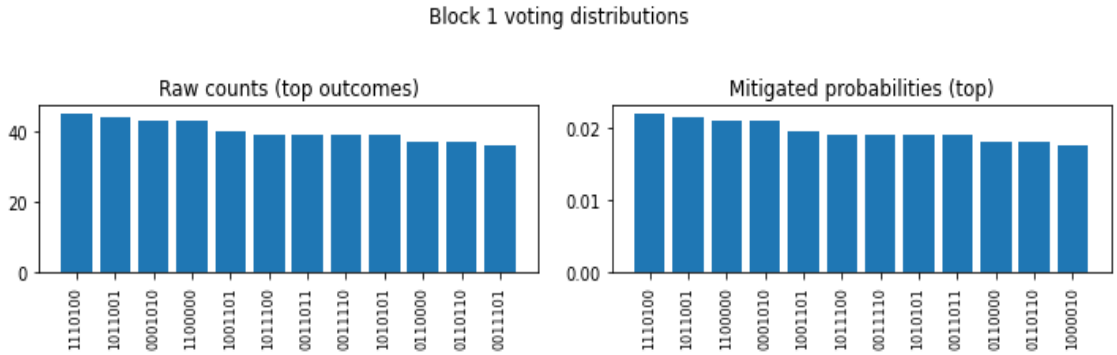

Fig. 3. Raw and mitigated distributions for Block 1

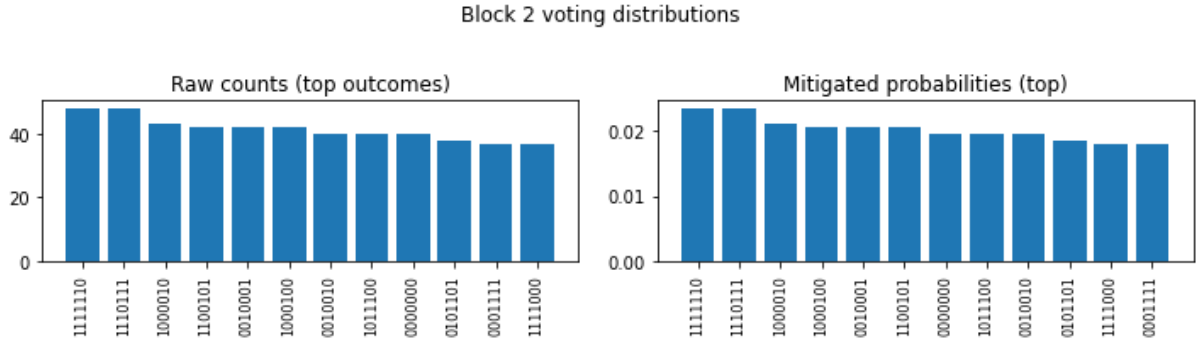

Fig. 4. Raw and mitigated distributions for Block

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

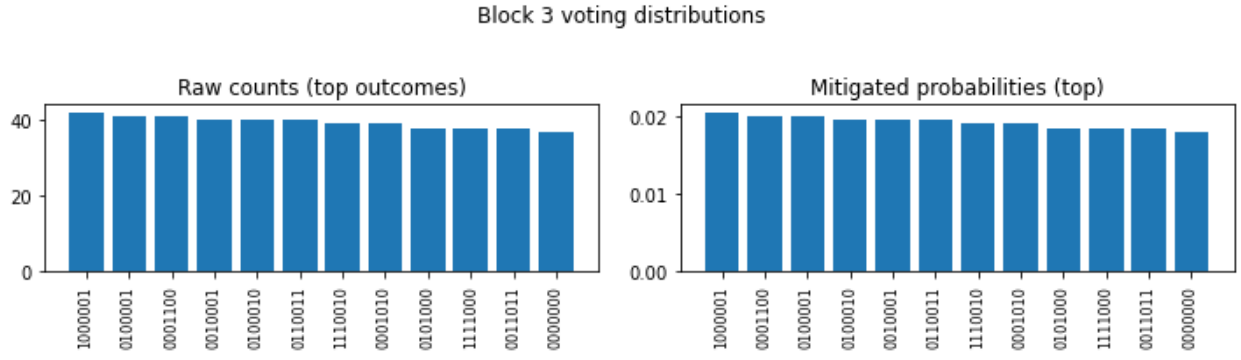

Fig. 5. Raw and mitigated distributions for Block 3

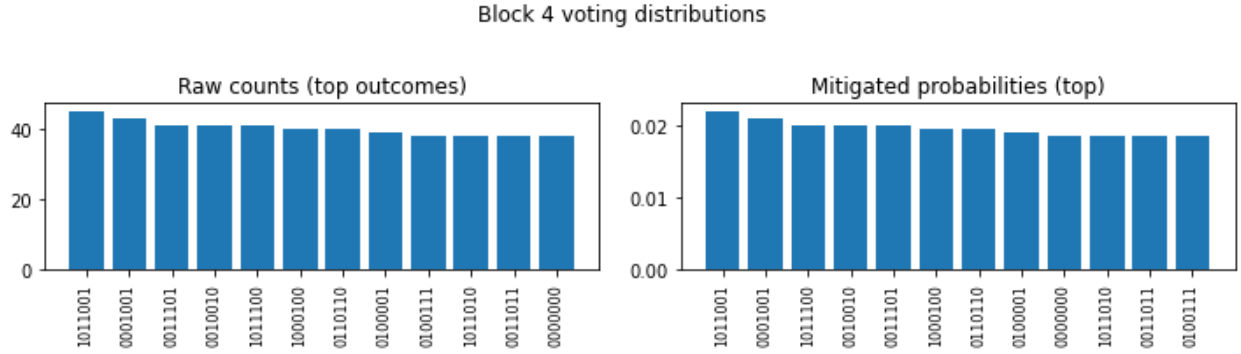

Fig. 6. Raw and mitigated distributions for Block 4

Experimental results show the following: the commit–reveal and ECDSA signing mechanism operated successfully with 100% verification across all blocks. Even in the presence of up to 43% Byzantine nodes, the quantum confirmation fraction remained stable within the range of 0.64–0.65. Unlike classical simple majority counting, quantum interference produced an effect that strengthened the collective decision. The measurement error mitigation algorithm smoothed the probability distribution and increased the reliability of the results. Thus, the proposed quantum blockchain consensus model was experimentally shown to be resilient to Byzantine faults and capable of forming a stable global decision using quantum interference. The obtained results demonstrate that the quantum-based consensus mechanism operates stably even in the presence of Byzantine validators. Despite 3 out of 7 validators exhibiting Byzantine behavior ($\beta \approx 0.43$), the quantum confirmation fraction for all blocks remained within the range 0.64–0.65, satisfying the condition $Q_k > 0.5$. This result indicates that the strengthening effect of quantum interference differs from classical majority-based decision-

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

making mechanisms. In the third block, the number of revealed "1" votes was 3, which is below the simple majority threshold. Nevertheless, due to quantum interference, the global confirmation fraction reached 0.642, and the block was accepted. This result demonstrates that the quantum model forms decisions through collective amplitude superposition, rather than through deterministic counting alone. In other words, the system's decision depends not only on the local binary sum but also on the interference properties of the global quantum state.

In the histograms of raw measurement results, certain bit strings appeared with high frequency, indicating constructive interference maxima. After applying the mitigation process, the probability distribution became smoothed and normalized. This shows that the correction mechanism based on pseudoinverse calibration matrices effectively reduced measurement errors. Therefore, accounting for measurement errors was identified as an important factor that improves the accuracy of consensus decisions. For all blocks, 100% verification success was observed during the commit–reveal and ECDSA signing stages, indicating that the authentication and integrity mechanisms in the model functioned reliably. The results demonstrate that the quantum voting mechanism can operate in integration with classical cryptographic protection. However, the model was implemented in a simulation environment, and noise, decoherence, and two-qubit error rates in real quantum hardware may be higher. Therefore, future research should include testing on real quantum devices and evaluating scalability by increasing the number of validators.

4. Conclusion

The research results show that the blockchain consensus model based on quantum interference can form a stable global decision even in the presence of Byzantine validators. Even with up to 43% Byzantine nodes, the quantum confirmation fraction for all blocks remained above 0.5, and the blocks were successfully accepted. The classical commit–reveal and digital signature mechanisms ensured the integrity and authentication of the consensus process. The quantum voting primitive produced a strengthening effect for collective decision-making through interference. The measurement error mitigation mechanism improved the

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

statistical stability of the results. The proposed model demonstrates the possibility of forming a Byzantine fault-tolerant consensus mechanism by integrating quantum and classical cryptography. This approach can serve as a methodological basis for the development of quantum-oriented blockchain architectures and for deeper analysis of their security parameters.

References

1. T.A.A.A.A. Bary, B.M. Elomda, H.A. Hassan, Multiple layer public blockchain approach for Internet of Things (IoT) systems, IEEE Access, 12, 56431–56438, 2024, URL: http://dx.doi.org/10.1109/ACCESS.2024.3389299
2. Y.-B. Cao, X.-B. Chen, Y.-F. He, L.-X. Liu, Y.-M. Che, X. Wang, K. Xiao, G. Xu, S.-Y. Chen, A post-quantum cross-domain authentication scheme based on multi-chain architecture, Comput. Mater. Contin., 2024, URL: http://dx.doi.org/10.32604/cmc.2024.046816
3. H. Ghaemi, D. Abbasinezhad-Mood, Novel blockchain-integrated quantum-resilient self-certified authentication protocol for cross-industry communications, IEEE Trans. Netw. Sci. Eng., 11(5), 4493–4502, 2024, URL: http://dx.doi.org/10.1109/TNSE.2024.3428916
4. D. Chaudhary, M.S.P. Durgarao, P. Gupta, S. Rana, Artificial intelligence, blockchain, computing and security volume 1: Proceedings of the international conference on artificial intelligence, blockchain, computing and security (ICABCS 2023),
5. Gr. Noida, UP, India, 24-25 February 2023, in: Artificial Intelligence, Blockchain, Computing and Security, ICABCS 2023, CRC Press, 2024, URL: http://dx.doi.org/10.1201/9781003393580-53
6. M.S. Peelam, V. Chamola, Enhancing security using quantum blockchain in consumer IoT networks, IEEE Trans. Consum. Electron., 2024, URL: http://dx.doi.org/10.1109/TCE.2024.3512791
7. Castiglione, J.G. Esposito, V. Loia, M. Nappi, C. Pero, M. Polsinelli, Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices, IEEE Trans. Ind. Inform., 21(2), 1674–1683, 2025, URL: http://dx.doi.org/10.1109/TII.2024.3485796

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 3, March, 2026
Website: usajournals.org

8. P. Sharma, K. Choi, O. Krejcar, P. Blazek, V. Bhatia, S. Prakash, Securing optical networks using quantum-secured blockchain: An overview, Sensors (Basel), 23(3), 1228, 2023, URL: http://dx.doi.org/10.3390/s23031228
9. M. Singh, B. Rawal, Exploring the intersection of blockchain and distributed quantum computing: Synergies, challenges, and future directions, in: 2024 Second International Conference on Microwave, Antenna and Communication, MAC, 2024, 1–7, URL: http://dx.doi.org/10.1109/MAC61551.2024.10837493
10. Liu, X.-B. Chen, G. Xu, Z. Wang, X. Feng, H. Feng, Quantum-enhanced blockchain: A secure and practical blockchain scheme, Comput. Mater. Contin., 76(1), 259–277, 2023, URL: http://dx.doi.org/10.32604/cmc.2023.039397
11. Liu, Q. Zhang, S. Xu, H. Feng, X.-B. Chen, W. Liu, QBIoT: A quantum blockchain framework for IoT with an improved Proof-of-Authority consensus algorithm and a public-key quantum signature, Comput. Mater. Contin., 80(1), 1727–1751, 2024, URL: http://dx.doi.org/10.32604/cmc.2024.051233
12. K. Jain, M. Singh, H. Gupta, A. Bhat, Quantum resistant blockchain-based architecture for secure medical data sharing, in: 2024 3rd International Conference on Applied Artificial Intelligence and Computing, ICAAIC, 2024, 1400–1407, URL: http://dx.doi.org/10.1109/ICAAIC60222.2024.10575286
13. E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov, Quantum-secured blockchain, Quantum Sci. Technol., 3(3), 035004, 2018, URL: http://dx.doi.org/10.1088/2058-9565/aabc6b
14. A.K. Sharma, M.S. Peelam, B.K. Chauasia, V. Chamola, QIoTChain: Quantum IoT-blockchain fusion for advanced data protection in Industry 4.0, IET Blockchain, 4(3), 252–262, 2024, URL: http://dx.doi.org/10.1049/blc2.12059
15. T.M. Fernández-Caramès, P. Fraga-Lamas, Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks, IEEE Access, 8, 21091–21116, 2020
16. H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, R. Cammarota, Post-quantum lattice-based cryptography implementations: A survey, ACM Comput. Surv., 51(6), 2019.