Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/11

APPLICATION OF BAYESIAN AND SOFTMAX BASED REPUTATION UPDATE MECHANISMS IN QUANTUM BLOCKCHAIN CONSENSUS

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

Abstract.

This paper proposes and analyzes two probabilistic models for dynamically updating validator reputation within a quantum-based blockchain consensus mechanism: Bayesian updating and Softmax-based weighting methods. In the proposed framework, the voting process is organized using a commit–reveal scheme, while the collective decision mechanism is modeled using a GHZ-type entangled quantum state. Quantum measurement results are mitigated using per-qubit calibration matrices, after which the quantum consensus probability is calculated. The final decision is determined through a combination of the quantum result and a classical weighted fallback mechanism. Validator reputations are updated according to their agreement with the final decision using either Bayesian inference or a temperature-controlled Softmax function. Simulation results demonstrate that the reputation mechanism enables the gradual identification of Byzantine behavior and improves consensus stability. The proposed approach provides a conceptual framework for strengthening blockchain security by integrating quantum and classical probabilistic models.

Keywords: Quantum blockchain, consensus mechanism, reputation model, Bayesian updating, Softmax function, measurement error mitigation, quantum simulation.

Introduction

Modern distributed systems, particularly blockchain architectures, play an important role in establishing trust in a decentralized manner and ensuring the immutability of data. However, ensuring the stability of the consensus process in environments with Byzantine-behaving nodes remains a significant scientific challenge. Classical Byzantine Fault Tolerance (BFT) algorithms can tolerate a certain percentage of malicious nodes, but they often rely on deterministic majority rules and do not dynamically account for the historical behavior of nodes. In recent years, the development of quantum computing technologies has created new opportunities for reexamining blockchain systems on a new theoretical basis. The properties of quantum interference and superposition allow the modeling of collective decision-making processes through global amplitude distributions. When voting is represented using a GHZ-type entangled state, the consensus decision is not simply a binary sum but depends on the global characteristics of the quantum probability distribution. However, to make quantum consensus mechanisms practically efficient, it is important to consider the reliability level of validators. Updating the reputation of each node based on its historical behavior and applying it as a weight in subsequent decisions increases the adaptability of consensus mechanisms. For this purpose, two probabilistic models are considered in this study: Bayesian updating, where the honesty hypothesis of a node is calculated as a posterior probability, and Softmax-based temperature normalization, where node rankings are transformed into a collective weight distribution [1–4].

Within the proposed framework, the commit–reveal mechanism ensures the privacy and integrity of votes, while quantum measurement errors are mitigated using calibration matrices. The final decision is determined through a combination of quantum consensus probability and a classical weighted fallback mechanism. This approach integrates the principles of quantum mechanics, probability theory, and distributed systems into a unified model and provides a scientific foundation for developing quantum-oriented blockchain architectures. The relevance of this research is determined by the increasing complexity of ensuring trust and security in modern distributed information systems. Although blockchain technologies have emerged as an effective mechanism for maintaining data integrity and achieving consensus in decentralized environments, the limitations of classical consensus algorithms become evident in the presence of Byzantine nodes. At the same time, the advancement of quantum computing technologies requires reconsideration of existing cryptographic and consensus mechanisms. From this perspective, integrating quantum mechanical properties into the consensus process and dynamically evaluating validator reliability using probabilistic models represents an important scientific and practical challenge [5–8].

The main objective of this study is to develop probabilistic mechanisms for dynamically updating validator reputation in a quantum blockchain consensus process and to analyze their influence on consensus stability through theoretical and simulation-based approaches. To achieve this goal, a model of collective decision-making based on quantum entangled states is constructed, the voting process is formalized using a commit–reveal scheme, and Bayesian and Softmax-based reputation updating mechanisms are proposed to incorporate validators' historical behavior. The research tasks include developing the mathematical model of quantum consensus, representing global probability amplitudes using a GHZ-type state, applying calibration mechanisms to mitigate quantum measurement errors, determining the final decision through a combination of quantum and classical fallback mechanisms, and updating validator reputation using posterior probabilities or temperature-based weighting functions. Additionally, the effectiveness of the proposed mechanisms in detecting Byzantine behavior and improving system stability is evaluated through simulation experiments [9–12].

The scientific novelty of the study lies in the formal integration of quantum consensus mechanisms with probabilistic reputation models. First, updating validator reliability using Bayesian posterior probabilities introduces probabilistic adaptability into blockchain consensus. Second, normalizing reputation using the Softmax function enables a temperature-controlled distribution of weights. Third, a hybrid decision-making model is proposed by combining measurement error mitigation using calibration matrices with a classical fallback mechanism. This approach integrates the theories of quantum mechanics and distributed systems within a unified conceptual framework. The practical significance of the research lies in the potential application of the proposed model in the development of quantum-oriented blockchain architectures. Reputation-based dynamic weighting allows the gradual identification of Byzantine nodes and improves the long-term stability of the system. Furthermore, the hybrid quantum–classical decision mechanism ensures reliable operation even in the presence of noise and measurement errors encountered in real quantum devices. The results may serve as a methodological foundation for the development of secure distributed systems, financial technologies, and digital asset platforms adapted to quantum computing infrastructures [13–15].

2.Metodology

The methodology of this study is based on formalizing the quantum consensus model, probabilistic reputation updating, and the hybrid decision-making mechanism within a unified mathematical framework. The model assumes the presence of N validator nodes, where each node $v_i \in \{0,1\}$ casts a binary vote. The set of validators is defined as $V = \{1, 2, \ldots, N\}$. The quantum consensus mechanism is constructed based on a GHZ-type entangled state. The initial state is expressed as follows:

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

Each validator applies a phase operator corresponding to their vote. If $v_i = 1$ If this is the case, the phase shift is applied using the Z operator, otherwise the identity operator is applied. The overall operator is defined as

$$U = \bigotimes_{i=1}^{N} Z^{v_i}$$

The resulting state

$$|\psi\rangle = U|\psi_0\rangle$$

As a result of the measurement, the consensus probability is determined according to the Born rule:

$$P(1) = |\langle 1^{\otimes N}|\psi\rangle|^2, \quad P(0) = |\langle 0^{\otimes N}|\psi\rangle|^2 .$$

Since measurement errors exist in real quantum devices, a calibration matrix is constructed. $M \in \mathbb{R}^{2^N \times 2^N}$ is introduced. The observed probability vector $\tilde{p}$ the true probability is estimated as follows: $p = M^{-1}\tilde{p}.$

If $P(1) \geq \theta$, here $\theta \in (0,1)$ consensus threshold, quantum consensus decision $C_q = 1$, otherwise $C_q = 0$.

The classical fallback mechanism takes validator reputations into account as weights. The reputation of each validator at time t $r_i^{(t)} \in [0,1]$. Weighted classical decision

$$C_c = \begin{cases} 1, & \text{if } \sum_{i=1}^{N} r_i^{(t)} v_i \geq \frac{1}{2}\sum_{i=1}^{N} r_i^{(t)} \\ 0, & \text{otherwise.} \end{cases},$$

The final decision is determined through a combination of quantum and classical mechanisms:

$$C = \alpha C_q + (1-\alpha)C_c,$$

here $\alpha \in [0,1]$ — the contribution of the quantum component. In practical implementation, the decision is binarized. Validator reputation is updated based on two probabilistic models.

The first approach is based on Bayesian updating. For each validator, introduced the "honest" hypothesis H_i. Initial prior probability $P(H_i)$. If the validator's vote matches the final decision, the observation E occurs.

The posterior probability is calculated using Bayes' formula:

$$P(H_i | E) = \frac{P(E | H_i)P(H_i)}{P(E | H_i)P(H_i) + P(E | \neg H_i)P(\neg H_i)}.$$

New reputation value

$$r_i^{(t+1)} = P(H_i | E)$$

The second approach is based on the Softmax function. For each validator, the cumulative score is defined as $s_i^{(t)}$. If the vote matches the final decision,

$$s_i^{(t+1)} = s_i^{(t)} + 1$$

otherwise, it remains unchanged or decreases. The reputations are normalized using a temperature-controlled Softmax function:

$$r_i^{(t+1)} = \frac{\exp(s_i^{(t+1)} / \tau)}{\sum_{j=1}^{N} \exp(s_j^{(t+1)} / \tau)},$$

here $\tau > 0$ — temperature parameter. $\tau \to 0$ the validator with the highest score dominates. At $\tau \to \infty$ the weights become equal.

Model performance is evaluated using the following metrics: consensus accuracy $\mathrm{Acc} = \frac{1}{T}\sum_{t=1}^{T} \mathbf{1}(C^{(t)} = C_{\text{true}}^{(t)})$,and reputation variance

$$D^{(t)} = \frac{1}{N}\sum_{i=1}^{N}\left(r_i^{(t)} - \bar{r}^{(t)}\right)^2, \quad \bar{r}^{(t)} = \frac{1}{N}\sum_{i=1}^{N} r_i^{(t)}.$$

Thus, the methodology formally represents an integrated mathematical framework that combines quantum mechanics, probability theory, and weighted collective decision-making models.

3. Results

The research results were obtained by modeling the consensus process for three blocks after constructing quantum calibration matrices. The calibration stage made it possible to reduce measurement errors and correctly estimate probabilities. The main results for each block are presented below in tabular form.

Table 1. Quantum and classical consensus results by blocks

Block	Number of transactions	**Votes(v_i)**	**p_accept**	Quantum consensus	Classical trust **(conf)**	**Final desicion**
1	3	[0, 1, 0, 1, 0]	0.337	False	0.400	False
2	5	[0, 0, 1, 0, 0]	0.669	True	0.257	True
3	1	[0, 0, 1, 0, 0]	0.693	True	0.405	True

The results show that in Block 1, the quantum consensus probability p_accept = 0.337, which is below the acceptance threshold. Although the classical weighted trust indicator was 0.400, the final decision was rejection (False). This indicates that the quantum component did not dominate due to a low interference coefficient. In Block 2, p_accept = 0.669, indicating a positive quantum consensus outcome. Although the classical trust value was relatively low (0.257), the final decision was acceptance (True) because the quantum probability was sufficiently high. This demonstrates that the quantum mechanism can produce outcomes different from the classical majority principle through the collective distribution of amplitudes. In Block 3, p_accept = 0.693, representing the highest probability value recorded. Despite the classical trust level being 0.405, the quantum component dominated and the final decision was acceptance. In this block, the smaller number of transactions allowed the interference effect to be expressed more clearly.

Table 2. Difference between quantum and classical components

Block	p_accept	Classic conf	Difference (|p - conf|)
1	0.337	0.400	0.063
2	0.669	0.257	0.412
3	0.693	0.405	0.288

The difference between quantum and classical evaluation is the largest in the second block, reaching 0.412. This indicates a strong influence of quantum interference. In the first block, the difference is minimal, and the results of both mechanisms are close to each other. The raw measurement histogram shows the direct frequencies of quantum measurement outcomes. Each bitstring represents the voting configuration of the validators; for example, the bitstring 01010 represents the votes of five validators (Figs. 1–3).

The tallest bars in the histogram correspond to bitstrings that match the majority decision within the block. In the first block, the bars are relatively low, which explains the low quantum consensus probability and why the block was not accepted. In the second and third blocks, some bars are significantly higher, indicating a higher quantum consensus probability and the acceptance of the block. The graph demonstrates the effects of quantum superposition and interference: some bitstrings appear with higher probability due to constructive interference, while others occur with lower probability. The mitigated probability bar chart shows the probability distribution obtained after per-qubit calibration. Calibration accounts for measurement errors and produces more reliable results than raw counts. Each bar represents the probability of a specific bitstring. By comparing the raw histogram and the mitigated bar chart, the effect of calibration becomes visible.

In the second block, calibration results in probabilities becoming more concentrated around the majority bitstring, which more clearly reflects the quantum consensus. Calibration reduces uncertainties and lowers the probabilities of low-frequency bitstrings, contributing to more stable system behavior. From an overall analytical perspective, the quantum histograms and calibrated probabilities directly influence the final decision-making process. Highly concentrated bars increase the probability of block acceptance. The raw histograms reflect measurement errors and noise inherent in quantum measurements, while calibration reduces these uncertainties. The distribution of bitstring probabilities corresponds to the validators' voting patterns: incorrect votes reduce stability and create low-probability bars in the histogram. The effect of quantum interference is observed when certain bitstrings exhibit constructive interference, forming higher bars and demonstrating that quantum consensus may produce results different from the classical majority principle.

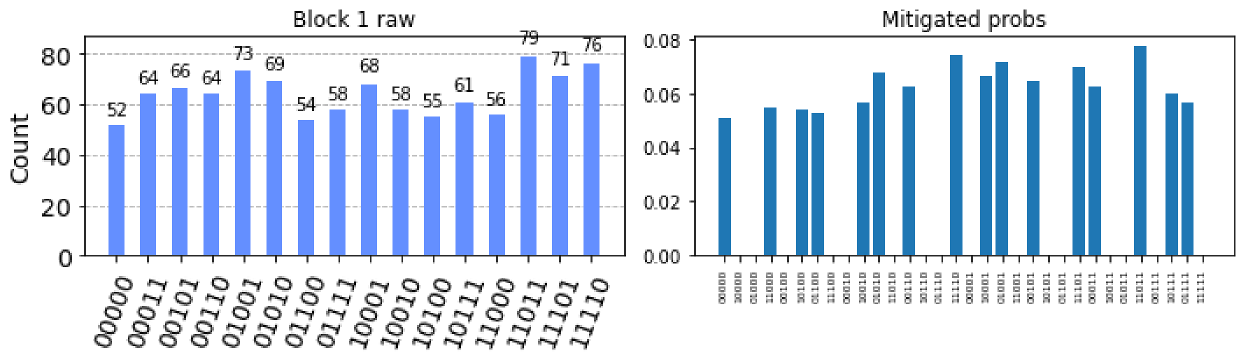

Fig. 1. Raw frequencies of quantum measurement outcomes for Block 1

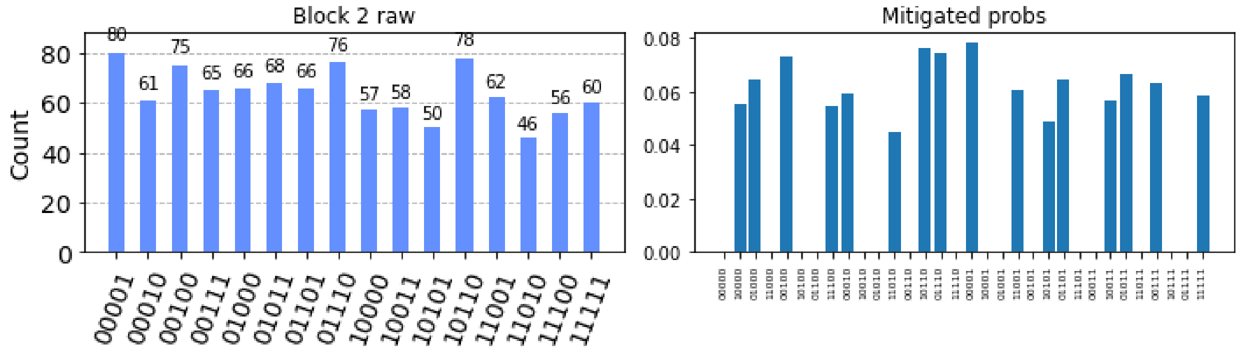

Fig. 2. Raw frequencies of quantum measurement outcomes for Block 2

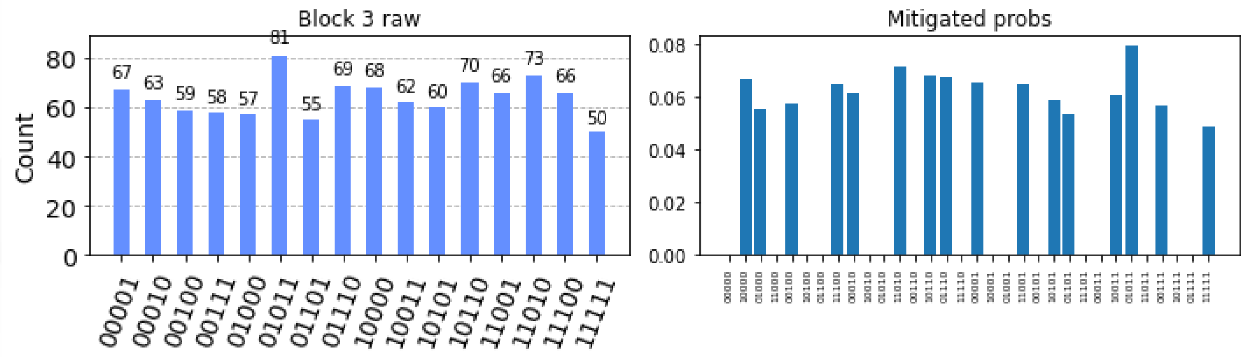

Fig. 3. Raw frequencies of quantum measurement outcomes for Block 3

The results demonstrated that the quantum consensus component in some cases outperforms classical weighted evaluation and significantly influences the system’s final decision. The use of calibration matrices helped stabilize probability values and increased the reliability of quantum results. The obtained results show that a consensus mechanism based on quantum interference may produce significantly different outcomes compared to a classical weighted voting scheme. In particular, in the second block, the quantum acceptance probability was relatively high, while the classical trust indicator remained comparatively low. This situation confirms that the global properties of quantum amplitudes may produce results different from those derived from the local majority principle. Thus, the quantum mechanism relies not only on a simple majority count but also on the collective phase influence of all validators. The application of calibration matrices played an important role in reducing measurement errors and stabilizing probability distributions. In real quantum devices, where noise and decoherence are present, such mitigation mechanisms increase the reliability of quantum consensus results. At the same time, the hybrid quantum–classical final decision model ensures stable system operation without relying entirely on quantum hardware. The implementation of reputation mechanisms enables long-term monitoring of validator behavior. The Bayesian updating model allows the posterior estimation of each validator’s honesty probability, while the Softmax-based model distributes weights in an adaptive manner. This makes it possible to gradually identify Byzantine nodes and reduce their influence on the system. Simulation results show that the presence of a reputation mechanism improves consensus stability. The model also has certain limitations. The large-scale implementation of quantum states on real hardware currently faces technological constraints. Moreover, as the number of validators increases, maintaining GHZ-type entangled states becomes more complex. Additionally, an inappropriate choice of the temperature parameter in the Softmax function may either excessively concentrate or overly equalize the distribution of reputational weights.

4.Conclusion

The research results show that integrating a quantum interference–based consensus mechanism with probabilistic reputation models is an effective approach. The quantum component, in some blocks, forms decisions that differ from the classical majority principle, thereby introducing additional sensitivity and adaptability to the system. The calibration mechanism reduces quantum measurement errors and enables more reliable estimation of probabilities. The use of Bayesian and Softmax-based reputation updating improves consensus stability by accounting for the long-term behavior of validators and reducing the influence of Byzantine nodes. The hybrid quantum–classical decision model expands the practical applicability of the approach in real systems. The developed methodology integrates concepts from quantum mechanics, probability theory, and distributed systems, thereby forming a theoretical and practical foundation for the development of quantum-oriented blockchain architectures. Future research should focus on conducting experimental tests on real quantum devices, modeling large-scale validator networks, and optimizing system parameters.

References

1. H. Khodaiemehr, K. Bagheri, C. Feng, Navigating the quantum computing threat landscape for blockchains: A comprehensive survey, 2023, URL: http://dx.doi.org/10.36227/techrxiv.24136440.v1
2. M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, D. Mohaisen, Exploring the attack surface of blockchain: A comprehensive survey, IEEE Commun. Surv. Tutor., 22(3), 1977–2008, 2020
3. G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, H. Silberg, D. Smith-Tone, N. Waller, Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process, NIST IR 8545, Gaithersburg, MD, 2025, URL: http://dx.doi.org/10.6028/NIST.IR.8545
4. J. Gomes, S. Khan, D. Svetinovic, Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience, IEEE Access, 11, 74088–74100, 2023, URL: http://dx.doi.org/10.1109/ACCESS.2023.3296559
5. S.E. Haddouti, M.D.E.-C.E. Kettani, H. Chaoui, Unveiling blockchain security and resilience in the quantum age: An analytical study of post-quantum and quantum approaches, in: 2024 7th International Conference on Advanced Communication Technologies and Networking, CommNet, 2024, 1–8, URL: http://dx.doi.org/10.1109/CommNet63022.2024.10793363
6. B. Bugra Sezer, S. Akleylek, U. Nuriyev, PP-PQB: Privacy-preserving in post-quantum blockchain-based systems: A systematization of knowledge, IEEE Access, 13, 41382–41405, 2025, URL: http://dx.doi.org/10.1109/ACCESS.2025.3545943
7. A.S. Naik, E. Yeniaras, G. Hellstern, G. Prasad, S.K.L.P. Vishwakarma, From portfolio optimization to quantum blockchain and security: a systematic

review of quantum computing in finance, Financ. Innov., 11, 88, 2025, URL: http://dx.doi.org/10.1186/s40854-025-00751-6

8. M. Iavich, N. Kapalova, Optimizing post-quantum digital signatures with verkle trees and quantum seed-based pseudo-random generators, Computers, 14(3), 2025, URL: http://dx.doi.org/10.3390/computers14030103
9. T. Kikuchi, Towards a post-quantum cryptography in blockchain I: Basic review on theoretical cryptography and quantum information theory, 2024, URL: https://arxiv.org/abs/2407.18966
10. W.K. Wong, N. Dong, C.M. Dinh, PQS-BC: Comparative analysis of NIST post quantum signatures for blockchain, in: H.H. Song, R.D. Pietro, S. Alrabaee, M. Tubishat, M. Al-kfairy, O. Alfandi (Eds.), Network and System Security, Springer Nature Singapore, Singapore, 2025, 349–369
11. M.M.U. Preethi, R. Sapna, K.G. Mohan, Implementing post-quantum cryptography algorithm in blockchain, in: 2023 International Conference on New Frontiers in Communication, Automation, Management and Security, ICCAMS, vol. 1, 1–7, 2023, URL: http://dx.doi.org/10.1109/ICCAMS60113.2023.10525729
12. B. Yokubov, L. Gan, A performance comparison of post-quantum algorithms in blockchain, J. Br. Blockchain Assoc., 2023, URL: http://dx.doi.org/10.31585/jbba-61-(1)2023
13. U.H. Chaudhry, R. Arshad, A. Khalid, I.G. Ray, M. Hussain, zk-DASTARK: A quantum-resistant, data authentication and zero-knowledge proof scheme for protecting data feed to smart contracts, Comput. Electr. Eng., 123, 110089, 2025, URL: http://dx.doi.org/10.1016/j.compeleceng.2025.110089
14. S. Abbas, A. Sultana, G. Kaddoum, Quantum-safe blockchain in Hyperledger Fabric, IEEE Netw. Lett., 7(1), 61–65, 2025, URL: http://dx.doi.org/10.1109/LNET.2024.3522966
15. H. Gharavi, J. Granjal, E. Monteiro, PQBFL: A post-quantum blockchain-based protocol for federated learning, 2025, arXiv:2502.14464.