Systems and Soft Computing 9 (2026) 200624

Contents lists available at ScienceDirect

Systems and Soft Computing

journal homepage: www.journals.elsevier.com/soft-computing-letters

Quantum-adaptive cryptography and adaptive multi-consensus layer for future-proof blockchain security and scalability

Jermin Jeaunita T. C [a], Panimozhi K [b], Sangeetha Francelin Vinnarasi F [c], Upendra Kumar [d], Haiter Lenin Allasi [e,g,*], Sasikumar P [f]

[a] Department of Computer Science and Engineering, Loyola Institute of Technology and Science, Thovalai, 629302, Nagercoil, India
[b] Department of Computer Science and Engineering, B.M.S College of Engineering, Bangalore, India
[c] Department of Information Technology, St. Joseph's Institute of Technology, OMR, Chennai, India
[d] Department of Computer Science and Engineering, Birla Institute of Technology Mesra Ranchi, Jharkhand, India
[e] Department Mechanical Engineering, WOLLO University, Kombolcha Institute of Technology, Post Box No: 208, Kombolcha, Ethiopia
[f] School of Computing and Innovative Technologies, British University Vietnam, Ecopark, Hung Yen, Vietnam
[g] School of Engineering and Applied Sciences, Kampala International University, Box 20000, Kampala, Uganda

ARTICLE INFO

Keywords:
Quantum-adaptive blockchain
Post-quantum cryptography
Crystal-dilithium
Quantum threat detection
Consensus algorithms
Bayesian optimization

ABSTRACT

Quantum computing is an emerging technology that could easily break cryptographic algorithms and threaten transaction integrity in blockchain networks. Existing blockchain consensus mechanisms remain static, and they are not capable of adapting to dynamic security requirements, performance, and energy consumption. To address these limitations, this study proposes a Quantum-Adaptive Cryptography and Adaptive Multi-Consensus blockchain framework that dynamically responds to evolving quantum threats and network conditions. The framework employs an AI-driven decision tree model to classify quantum threat levels using features derived from the QM9 quantum chemical dataset. The decision tree classifier classifies quantum threat levels into either low, high, or moderate, which then triggers one of the cryptographic schemes of Elliptic Curve Digital Signature Algorithm (ECDSA), Crystal-Dilithium 3, or Hybrid ECDSA with Crystal-Dilithium, respectively. In parallel, a Bayesian optimization-based multi-consensus layer dynamically selects the most suitable consensus protocol (Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), or democratic Byzantine Fault Tolerance (dBFT)) based on network load, validator behavior, and security requirements. Experimental results demonstrate that the proposed framework achieves zero-downtime cryptographic switching, improved transaction throughput, stable block finality, and enhanced quantum resilience. The proposed approach ensures a secure, scalable, and future-proof blockchain architecture that adapts to emerging quantum computing threats. The approach also has practical implications for building scalable, resilient, and quantum-secure blockchain systems applicable to decentralized finance, supply chain, and critical infrastructure applications.

1. Introduction

Security infrastructure is crucial in blockchain for its decentralized and distributed features, which include various mechanisms such as cryptographic algorithms, network architecture, consensus protocols, and smart contract execution [1,2]. These mechanisms are vulnerable due to the development of quantum computing and powerful quantum computers [3]. Quantum computing is evolving to be the new technology that efficiently solves the mathematical challenges today. Quantum computers execute any operations at high speed, which enables the ability to perform any modern algorithms of the extensive cryptographic infrastructures [4,5]. Large quantum computers have the ability to break the traditional cryptographic algorithms Rivest, Shamir, Adleman (RSA) and Elliptic Curve Cryptography (ECC), which is known as a quantum threat. This quantum threat presents a multifaceted and highly complex challenge for security in blockchain [6,7]. Quantum computers solve these problems in polynomial time. However, classical computers take an exponential time, which hugely compromises the security of these cryptographic systems [8,9]. This poses a risk for data under these systems. This vulnerability pressures the essential need to operate

* Corresponding author.
E-mail addresses: jerminjeaunita@lites.edu.in (J.J.T. C), panimozhi.cse@bmsce.ac.in (P. K), sangeethaf@stjosephstechnology.ac.in (S.F.V. F), upendrakr@bitmesra.ac.in (U. Kumar), haiterlenina@gmail.com (H.L. Allasi), sasikumar.p@buv.edu.un (S. P).

https://doi.org/10.1016/j.sasc.2026.200624
Received 25 September 2025; Received in revised form 8 August 2026; Accepted 4 September 2026
Available online 5 September 2026
2772-9419/© 2026 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Post-Quantum Cryptography (PQC), which is strong enough to withstand any cryptographic attack developed by quantum computing [10,11].

PQC algorithms enhance the security of conservative blockchains and speed up the transaction verifications [12,13]. However, PQC with blockchain affects the transaction processing speed, slower signing and verification time, transaction throughput, and computational efficiency across the network. This impacts the delay in network transactions and the verification and validation process of blockchain [14,15]. The consensus algorithms solve these problems in quantum computing through the contributions of network nodes. Consensus algorithms enable the network to be secure and reliable to resist quantum attacks, and enhance transaction and verification speed [16,17]. This ensures PQC to develop cryptographic methods to secure against quantum attacks, and consensus algorithms integrate PQC to attain network agreement securely without delays [18].

Thus, analyzing the existing studies, most approaches adopt static cryptographic configurations and depend on a single, fixed consensus mechanism. These solutions cannot be dynamically scaled to changing quantum threat levels and other changing network conditions. Furthermore, the integration of real-time quantum threat assessment with adaptive cryptographic switching and multi-consensus selection remains unexplored. However, this gap hinders the long-term security and scalability of existing blockchain systems. This study proposed a Quantum-Adaptive Cryptography and Adaptive Multi-Consensus framework to solve these problems. This approach provides a future-proof solution for secure and scalable blockchain systems.

The proposed pipeline combines quantum feature extraction, AI threat classification, adaptive cryptography and dynamic consensus selection to ensure secure blockchain operation. The quantum derived features are preprocessed, normalized and converted to composite threat scores through threat mapping and Weighted Linear Combination (WLC). A Decision Tree Classifier detects a quantum threat level and automatically switches on the appropriate cryptographic scheme: Elliptic Curve Digital Signature Algorithm (ECDSA), hybrid ECDSA and Crystal-Dilithium or Crystal-Dilithium 3. The parameters of the network are monitored continuously using the JSON-RPC and Cosmos SDK telemetry modules and the best consensus protocol, such as Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and democratic Byzantine Fault Tolerance (dBFT), are determined using the Bayesian optimization method. This built-in pipeline offers adaptability in real time, quantum resilience, seamless cryptographic switching and enhanced blockchain scalability. The major contributions of the work are as follows:

- **Quantum-adaptive blockchain framework:** This study develops a quantum-adaptive cryptography and adaptive multi-consensus blockchain framework that integrates AI-driven threat modeling, quantum-resistant cryptography switching, and adaptive consensus algorithm selection.
- **AI-driven quantum threat classification:** This study employs an AI-driven Decision Tree Classifier (DTC) that classifies the quantum threat levels into low, high, or moderate, and triggers cryptographic scheme switching.
- **Post quantum cryptographic signing system:** The proposed framework employs a signing system that utilizes the ECDSA, Crystal-Dilithium 3, and hybrid ECDSA with Crystal-Dilithium, and signatures based on quantum threat assessment.
- **Adaptive consensus algorithm selection:** This study utilizes Bayesian optimization for optimal consensus algorithm selection based on network and energy parameters. This builds an adaptive multi-consensus layer on Cosmos SDK with hot-swappable modules supporting multiple consensus protocols.

The remaining portion of this paper is organized as follows. Section 2 discusses the related studies in the concerned domain. Section 3 explains the methodology of the proposed model. Section 4 provides the experimental results, and Section 5 summarizes the objective of the study, implementation, and results.

2. Literature survey

In this section, we review the existing works on PQC algorithms and consensus algorithms related to blockchain security. Recent works have shown the efficiency of intelligent optimization and adaptive computational techniques for system improvement in various fields. However, these methods are mainly focused on optimization accuracy, control efficiency, or computational intelligence, rather than the emerging challenge of quantum threats in the blockchain environment.

Sun et al. [19] integrated PQC algorithms and signature schemes to secure signatures, particularly for user authentication within the same node. The approach leverages the accuracy of logic programming to make smart contracts verify fewer errors. Revanthi and Suganthi [20] developed an encryption technique, Crystals-Kyber, with a Falcon and Crystal-Dilithium signature PQC algorithm. The PQC algorithms are embedded into the smart contract and communication layers of Hyperledger Fabric to prevent quantum attacks. Similarly, Reddy et al. [21] suggested a quantum-resistant QuantumShield-blockchain framework that integrated PQC algorithm Crystal-Dilithium for digital signatures and quantum key distribution to resist quantum decryption. The framework provided a confidential and tamper-proof transaction in post-quantum environment, although limited in scalability and efficiency of the framework. Aramide [22] evaluated how quantum algorithms break classical cryptographic schemes and highlighted the need for PQC in quantum-resistant algorithms to ensure long-term confidentiality, authenticity, and integrity. Nwaga and Idima [23] identified suitable PQC algorithms that effectively replaced vulnerable classical schemes, the RSA and the ECC algorithms, in blockchain and cloud infrastructures. The approach explored PQC integration in blockchain networks through digital signatures, key exchanges, transaction verification, and smart contract execution. However, the future enhancements depended on global cooperation and regulatory enforcement.

Frikha et al. [24] developed a lightweight and efficient blockchain consensus algorithm enabling secure and decentralized operations. The approach reduced computational overhead and latency while maintaining security. Liu et al. [25] developed a Quantum-Enhanced Blockchain Architecture for Internet of Things (QBIoT) for secure data sharing and introduced a Proof of Authority with Random Election (PoARE) for new block creation. This approach provided an efficient solution for quantum security problems in a post-quantum environment. Ktari et al. [26] presented a consensus algorithm in blockchain technology to increase the security in quantum attacks. This study utilized the Field-Programmable Gate Arrays (FPGAs) and PQC algorithms to improve the security and efficacy of blockchain consensus mechanisms. Qin et al. [27] developed a Weighted Practical Byzantine Fault Tolerance (WPBFT) consensus algorithm to assign weights to consortium blockchain nodes and balanced the system based on behavior and activity. The algorithm improved efficiency, scalability, and security in consortium blockchain systems. Still, the algorithm needed further testing to improve its adaptability in a real consortium blockchain application. Tian et al. [28] introduced a Verifiable Secure Sharing (VSS) with the Raft protocol consensus algorithm to create a zero-trust framework for blockchain consensus. The algorithm enhanced blockchain security under zero-trust principles that prevent malicious manipulation. However, the study needed improvements in strengthen the security to ensure the safety of the data transmission process.

2.1. Research gaps identified

The recent research investigated PQC algorithms and consensus algorithms in a blockchain setting, where, most of the available solutions depend on static security configurations and fixed consensus

mechanisms. This restricts the capability to respond to changing quantum threats and changing network conditions. Existing post-quantum blockchain approaches primarily focus on cryptographic replacement or hybrid signature schemes. This lack of adaptability creates a significant gap in the development of future-proof blockchain systems. Thus, an approach is required for maintaining long-term security, scalability, and operational continuity in quantum-evolving environments.

3. Methodology

The proposed quantum-adaptive blockchain framework is illustrated in Fig. 1. The methodology utilizes the quantum chemical dataset QM9 [29]. Five specific features are extracted namely, HOMO-LUMO gap ($\Delta\varepsilon$), HOMO energy (εHOMO), LUMO energy (εLUMO), Dipole moment (μ), and Polarizability (α) from the dataset. The forward fill imputation technique is used to handle missing values. Then, the feature engineering process is continued to compute first difference values for each property, and z-score normalization is used to normalize the features. The feature augmentation technique uses the threat mapping to compute the composite score and Δ composite score using normalized features and Δ normalized features, respectively. The Artificial Intelligence (AI)-based decision tree classifier categorizes the quantum threat levels into low, high, or moderate. The detected threat levels activate corresponding cryptographic schemes. If the threat is low, this activates the ECDSA cryptographic algorithm, if the threat is high, this activates the PQC algorithm Crystal-Dilithium 3, and if the threat is moderate, the hybrid algorithm that combines the properties of ECDSA and the Crystal-Dilithium algorithm is activated.

In parallel, the Ethereum fork activates JSON-RPC monitoring agents and Cosmos SDK telemetry modules in the network to provide real-time data on transaction load, validator behavior, and consensus health. Based on this, a Bayesian optimizer evaluates consensus candidates (Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), democratic Byzantine Fault Tolerance (dBFT)) using a multi-objective function, balancing, throughput, latency, security, and post-quantum compatibility. The Cosmos SDK's hot-swappable modules enable seamless runtime consensus switching.

3.1. Dataset description

In this study, we utilize the QM9 dataset containing 133,885 quantum chemical properties of small organic molecules as training data for quantum threat level detection. Each molecule is collected from a group of chemical elements such as Carbon, Chlorine, Hydrogen, Nitrogen, and Oxygen. The QM9 dataset provides the molecular properties that are mapped to proxies of quantum hardware performance, which helps to detect the quantum threats. The QM9 dataset provides well-structured quantum chemical properties that are mapped to proxies of quantum hardware capability. In this dataset, we only selected the features such as Highest Occupied Molecular Orbital (HOMO)-Lowest Unoccupied

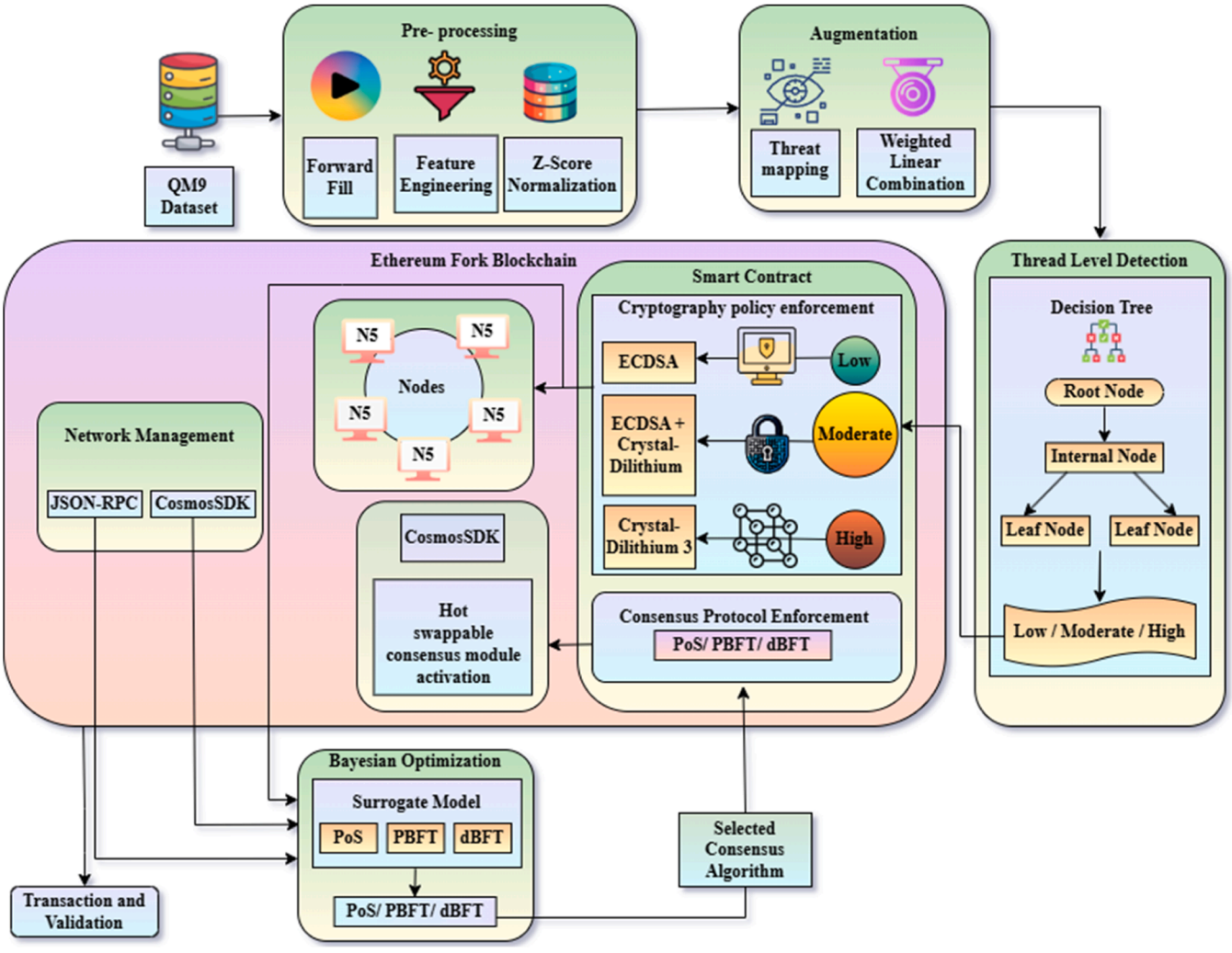


Fig. 1. Schematic diagram of the proposed quantum-adaptive blockchain framework.

Molecular Orbital (LUMO) gap, HOMO energy, LUMO energy, dipole moment, and polarizability were selected. This reflects computational stability, energy transitions, and coherence-related characteristics, making them suitable indicators for quantum threat modeling in this study.

3.2. Enhancing the dataset

From the 15 properties of the QM9 dataset, we utilized five specific properties using the feature extraction technique. The five selected properties have the clearest correspondence to hardware performance and blockchain risk. The selected features are HOMO-LUMO gap ($\Delta\varepsilon$), HOMO energy (εHOMO), LUMO energy (εLUMO), Dipole moment (μ), and Polarizability (α) that have the proxies for quantum hardware capabilities. Then, we utilize the preprocessing techniques to prepare the QM9-derived quantum hardware proxy data as input features. The forward fill technique [30] handles missing values and maintains continuity across the molecular sequence. The missing value is replaced using the last observed value in the series. Feature engineering process [31] computes first differences (Δ) to capture increasing or decreasing quantum hardware performance trend features for each property. The raw features and Δ features are normalized using Z-sore normalization, which standardizes feature scales [32]. This improves interpretability and stability in threshold-based classification. This normalization is applied separately to raw features and Δ features to the standardized scale as expressed in equation (1).

$$Z = \frac{Y - \mu}{\alpha} \tag{1}$$

where Z represents the normalized feature, μ denotes mean and α signifies the standard deviation of Y.

3.3. Feature augmentation through threat mapping for computing composite threat score

The normalized features and Δ normalized features are converted into threat scores through sign inversion based on domain knowledge. This mapping ensures that, across all features, higher values consistently represent a higher quantum threat. Then, we applied the Weight Linear Combination (WLC) [33] approach to compute the composite threat score using domain-specific weights. The threat mapping ensures consistent semantic interpretation, and the higher feature values represent higher quantum risk. The WLC approach was selected to aggregate multiple indicators into a single composite threat score. The weights are assigned based on the relevance of features in blockchain security. In $\Delta\varepsilon$, the weight is assigned 30% based on the strongest indicator of computational power, εHOMO with 25% reflects gate error rates which is relevant for maintaining stability. εLUMO with 25% is directly tied to coherence time, μ with 10%, influences the hardware recalibration frequency, and α with10% indicates long-term hardware stability. Then, we compute the composite threat score and Δ composite threat score using the threat-mapped features and assign weights as denoted in equations (2) and (3).

$$CS = (0.3 * \Delta\varepsilon_m) + (0.25 * \varepsilon\mathrm{HOMO}_m) + (0.25 * \varepsilon\mathrm{LUMO}_m) + (0.1 * \mu_m) + (0.1 * \alpha_m) \tag{2}$$

$$\Delta CS = (0.3 * \Delta(\Delta\varepsilon)) + (0.25 * \Delta\varepsilon HOMO) + (0.25 * \Delta\varepsilon LUMO) + (0.1 * \Delta\mu) + (0.1 * \Delta\alpha) \tag{3}$$

where, m represents the mapped features, CS is the composite score that represents the current threat magnitude, and ΔCS represents the rising, stable, or falling threat trend directions. These results are passed to the AI classifier decision tree for adaptive cryptographic response.

3.4. Quantum threat level classification using AI decision tree

After the augmentation process, we employ an AI model decision tree classifier [34] to categorize the quantum computer's threat level. A DTC is selected due to its low inference latency, interpretability, and rule-based structure. This is critical for real-time security adaptation in blockchain environments. The DTC is based on a training model that predicts the class based on the learning rules. The trained DTC classifier uses the threshold learned from $\Delta\varepsilon$, εHOMO, εLUMO, μ, and α features to divide the feature space into regions corresponding to low, high, or moderate threat. The decision tree's decision rules map these scores into threat levels as expressed in equation (4).

$$TL = \begin{cases} Low, CS \leq -0.3252 \, or \, \Delta CS < -0.05 \\ High, CS > 0.2893 \\ Moderate, otherwise \, (if \, -0.3252 < CS \leq 0.2893 \, and \, \Delta CS \geq -0.05) \end{cases} \tag{4}$$

where TL represents the threat level. If the CS values are less than or equal to -0.3252 or ΔCS values are less than -0.05, threat level is classified as low threat. The CS values are greater than 0.2893 which is classified as high threat, otherwise classified as a moderate threat. Based on these threat levels, we dynamically configure the Ethereum fork to apply an appropriate cryptographic scheme.

3.5. Cryptographic scheme enforcement on ethereum fork

This rule-based classification allows the Ethereum fork blockchain to react dynamically through the smart contracts [35]. If the threat is low this selects the ECDSA algorithm only. If the threat is high the algorithm selects the PQC algorithm Crystal-Dilithium 3 only. If the threat is moderate the hybrid algorithm that combines the properties of ECDSA and Crystal-Dilithium algorithm. Fig. 2 describes the quantum-adaptive blockchain process. As shown in this figure, initially user submits a transaction then Ethereum node enquires the cryptographic switching for active mode based on the threat levels. Adaptive consensus protocol engine proposes the validated transaction. JSON-RPC and cosmos SDK are sent to the Bayesian optimizer, that returns the optimal consensus algorithm. Then, the block is finalized, and the transaction is confirmed to the user.

3.5.1. ECDSA for low threat

In this study, the ECDSA algorithm [36] is used to ensure security from low threat scenarios. This technique signs and verifies digital transactions securely in the blockchain. The ECDSA generates a digital signature from the use of elliptical curves that provides a sender authentication and data integrity-based confidence. The algorithm uses two functions such as *GenerateSignature*() and *VerifySignature*(). The *GenerateSignature*() approach obtains the hashed Region of Interest (hRoI) and a private key (t). The digital signature generation process is denoted in equations (5) and (6).

$$DS = c_1 \ mod \ m, \left(g^{-1} * hRoI + s * t\right)) \ mod \ m) \tag{5}$$

$$DS = d_1 \ mod \ m, \left(g^{-1} * hRoI + r * t\right)) \ mod \ m) \tag{6}$$

Where (c_1, d_1) represents the computed elliptical curve points, s and r are computed based on the selected random value g, m represents the order of the elliptical curve, $hRoI$ and t denotes the parameters of the elliptic curve. The digital signature process is illustrated in equation (7).

$$V = [(hRoI * \vartheta) * F + (s * \vartheta) * t] \ mod \ m == (s \ mod \ m) \tag{7}$$

Where s and r are extracted from DS, ϑ and (c_1, d_1) are calculated using the parameter m, the $hRoI$, t, and previously derived values. This ensures the integrity of transactions through incorporating a digital signature.

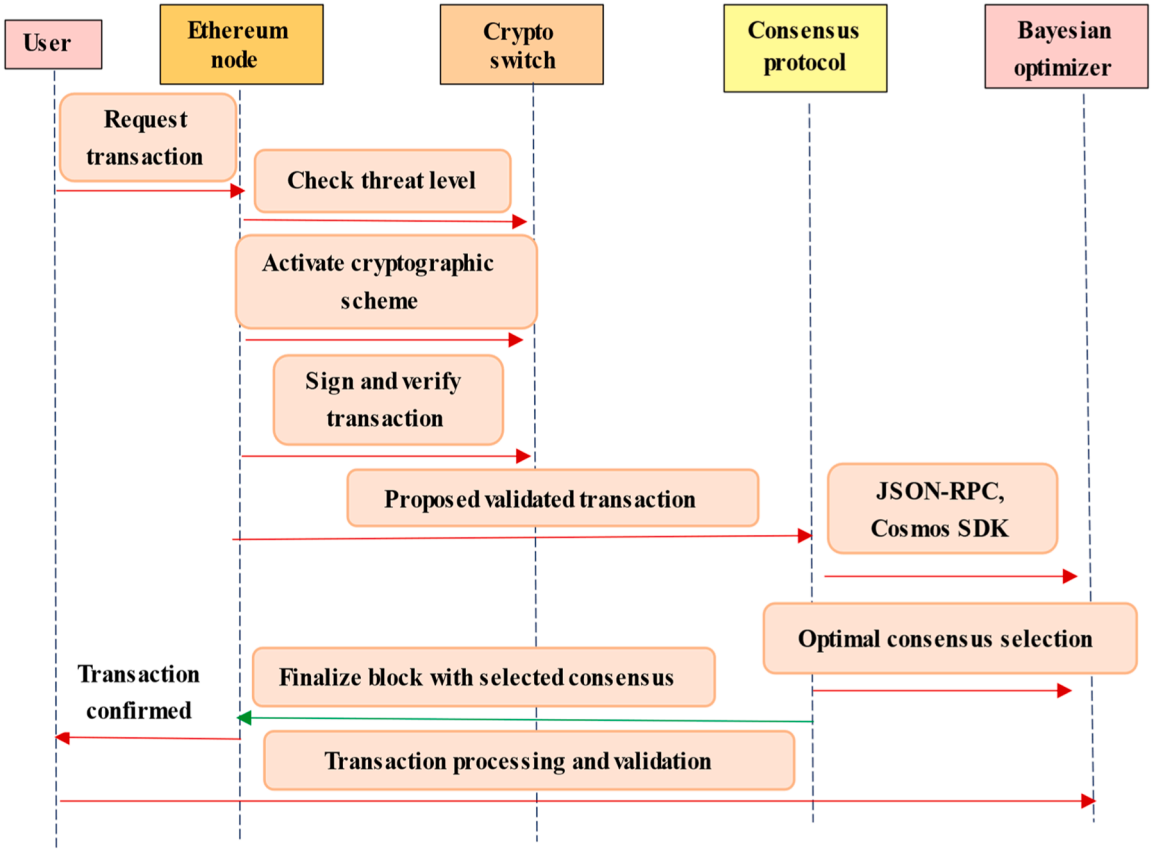


Fig. 2. Sequence diagram for the quantum-adaptive blockchain process.

3.5.2. Crystal-dilithium 3 for high threat

The Crystal-Dilithium 3 signature algorithm is utilized to ensure security from quantum attacks in high-threat scenarios. It maintains integrity and trust among data while performing transactions in blockchain. The process of Crystal-Dilithium 3 is illustrated in Algorithm 1. The algorithm produces two polynomials, p_1 and p_2 to generate the secret key. These polynomials are utilized to calculate the public key as expressed in equation (8).

$$\textit{Public key}\ (l) = K \times p_1 + p_2 \tag{8}$$

where K denotes the publicly known matrix allowing others to validate signatures without compromising the secret key. When signing a file, the algorithm takes the data m as input and produces a nonce γ from it to confirm individuality of the signature. Then computes polynomial a that depends on γ and l, and merged with p_1 and p_2 to create the signature. This signature is securely connected to the definite data and the signer's identity. At the verification process time, the integrity of the data and the validity of the signer are complete through checking the signature against the l and the data m. The successful verification represents that the data has not been tampered with and originate from the requested sender. This guarantees the integrity and confidentiality of sensitive data, enabling secure transactions. Crystal-Dilithium delivers a nonce establishment, which is secured separately for the data and the secret key of the sender. This ensures the immutability and trustworthiness of the transactions and provides the highest level of reliability.

3.5.3. Hybrid ECDSA with crystal-dilithium 3 for moderate threat

The hybrid ECDSA with Crystal-Dilithium signature algorithm is utilized to ensure security from quantum attacks in moderate threat scenarios. The hybrid ECDSA with Crystal-Dilithium scheme combines classical ECDSA with post-quantum signatures (Dilithium) [37]. It requires both signatures to be verified for each transaction. This approach is better as it has high security confidence than the ECDSA algorithm. This dual-signature process introduces computational and storage overhead. Validators perform two verifications per transaction, and

Algorithm 1
Pseudocode of crystal-dilithium 3.

Input: (data m, signature $(a, a\backsim[p_1, p_2], l)$

Output: data m, signature $(a, a\backsim[p_1, p_2])$
1: Produce p_1 and p_2 with least coefficients
2: Calculate $l) = K \times p_1 + p_2; l \leftarrow M_p$
3: Signing process
4: Produce nonce γ from m
5: Calculate a that depends on γ and l
6: Verify $a \rightarrow (l, m)$
7: If successful
8: Signature is valid
9: Else
10: Signature is invalid

block sizes increase due to carrying both signatures. It offers a transitional path for adoption of PQC. The hybrid approach is less efficient than Crystal-Dilithium-3, which achieves the same quantum resistance with lower latency and smaller verification costs.

3.6. Network monitoring and parameter gathering

In this phase, Ethereum fork continuously monitor key network parameters such as network load, transaction volume, validator performance metrics, and consensus health indicators. For this phase, we utilize the JSON-RPC monitoring agents and Cosmos SDK telemetry modules. In the Ethereum fork, JSON-RPC monitoring agents collect real-time metrics such as pending transaction counts, gas usage distribution, block production times, stale block rates, network load, and the latency of signature validation for both ECDSA and Crystal-Dilithium 3. In parallel, the Cosmos SDK telemetry module captures validator-centric and consensus-related data, including validator uptime, availability, signed vote rates, slashing events, proposal outcomes, block propagation delays, and participation levels across different consensus protocols (PoS, PBFT, dBFT). Also, monitors the efficacy and transition overhead of hot-swappable consensus modules, tracking memory usage and protocol switch latency. This monitoring system generates a rich, continuous dataset of blockchain state, validator behavior, and cryptographic performance, which is then fed into the Bayesian optimizer to select secure, real-time decision-making under varying quantum threat conditions.

3.7. Bayesian optimization for consensus protocol selection

The Bayesian Optimization [38] for Consensus Protocol Selection process enables the blockchain to dynamically choose the most suitable consensus mechanism (PoS, PBFT, dBFT) based on real-time network conditions and quantum threat levels. Bayesian optimization is selected to handle the multi-objective nature of consensus performance optimization, considering throughput, latency, validator behavior, and security. It enables efficient exploration of consensus options with minimal runtime overhead. The Bayesian optimization uses the Gaussian Process (GP) to predict how each consensus protocol will perform under given conditions.

In Proof of Stake (PoS) consensus algorithm [39], validators are chosen to propose and validate block transactions according to their stake values. It performs well under normal load conditions with large validator sets and has good throughput when the network is stable. The validators are essential to stake a certain number of their tokens to present them with a chance of being selected to validate transaction blocks, and get a reward for validating the blocks. However, it is vulnerable to long-range attacks if cryptography is weak. This algorithm is selected when the network has low to moderate load and validator participation is high, ensuring cost-effective and scalable operation. In the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm [40], coordinating all nodes in the network, decide on the order of transaction requests. Consensus is reached through rounds of transaction exchanges among validators, tolerating up to $\frac{n-1}{3}$ malicious nodes in a network. Once a block is confirmed, it cannot be returned. It is maintained very safely in smaller, permissioned validator environments and confirms strong protection against forks and malicious behavior. However, it faces challenges in high communication overhead, and it is not ideal for large-scale, high-throughput public blockchains. This algorithm is selected when security and fault tolerance are prioritized over throughput, for instance, under moderate to high quantum threat levels and when validator reliability is uncertain. In the democratic Byzantine Fault Tolerance (dBFT) consensus algorithm [41], token holders vote for validators, and these validators participate in the consensus process. The block confirmation is achieved when consensus is reached among the selected validators. This algorithm is faster than classical PBFT due to fewer active participants, high throughput, and good scalability, and provides the response immediately. However, it depends on the trust calculated for selected validators, which introduces centralization risks, and it is vulnerable if validator selection becomes biased or compromised. This algorithm is selected when the system needs a balance between scalability and security, especially under high transaction volume with moderate validator diversity.

The proposed Bayesian Optimization strategy is designed for adaptive consensus selection. The effectiveness of the optimization is evaluated in terms of its ability to discover high performing consensus configurations under different blockchain conditions. The exploration and exploitation process based on surrogates allows efficient choices of consensus mechanisms and saves unnecessary evaluations, ensuring the scalability. This consensus algorithm approach enables blockchain-based systems to achieve a dynamic, context-aware balance between throughput, security, latency, and post-quantum cryptography compatibility that is crucial for robust operation in adversarial quantum computing environments.

3.8. Hot-swappable consensus module activation in cosmos SDK

This phase utilizes the selected consensus protocol decision that activates consensus modules with support for seamless switching. This maintains consistent state, synchronization, and validator consensus on protocol switch. This produces an active consensus protocol that ensures optimal security and efficiency. The Bayesian optimizer controls the optimal protocol for current conditions. The corresponding consensus module is activated within the Cosmos SDK. The Cosmos SDKs is selected to support seamless runtime switching between PoS, PBFT, and dBFT consensus protocols. Hot-swappable modules eliminate downtime and maintain ledger consistency, which is essential for adaptive blockchain systems. The system ensures that all validators are synchronized on the switch decision and that the blockchain state is consistently maintained across the network during the transition. To achieve this, the consensus engine checkpoints the current state, activates the new consensus module, and resumes block production under the new rules. This allows the blockchain to respond adaptively to changes in network load, validator behavior, and quantum threat levels, maintaining both efficiency and security. The system achieves seamless transitions, eliminating downtime and enabling context-aware consensus selection as an integral part of the blockchain strategy.

4. Results and discussion

This section presents the experimental outcomes of the proposed quantum-adaptive blockchain framework. The QM9 dataset is split into 70% for training, 20% testing, and 10% for validation. The system specifications used for the proposed work are Intel(R) HD Graphics, CPU- Intel Core i5-6500 CPU @3.20 GHz, MEMORY -16.0 GB DDR3, Python 3.12, remix idev0.71.0, Solidity v0.8.30, Web3.js v4.16.0OS Windows 10, TensorFlow - 2.17.

4.1. Performance analysis of the proposed model

This section presents the performance analysis of the proposed model through the analysis of the decision tree threat detection module, Ethereum fork implementation results, analysis of cryptographic switching performance, analysis of consensus algorithm selection, scalability analysis, and ablation study analysis.

4.1.1. Performance analysis of the threat detection module

The decision tree model for quantum threat level classification uses the criterion, minimum samples in node, and the maximum depth for the hyperparameters. The hyperparameter tuning results are illustrated in Table 1. In Table 1, the top fifteen combinations of criterion, minimum samples, and the maximum depth as hyperparameters are represented

Table 1
Hyperparameter tuning results of the decision tree based on the top fifteen combinations. At the Gini criterion, minimum samples in the node ten, and a maximum depth of three, attained a better mean accuracy.

No	Criterion	Min samples in the node	Maximum depth	Score
1	Gini	2	2	84.93
2	Gini	2	3	99.99
3	Gini	5	2	84.93
4	Gini	5	3	99.99
5	Gini	10	2	84.93
6	**Gini**	**10**	**3**	**99.99**
7	Entropy	2	2	84.93
8	Entropy	2	3	99.98
9	Entropy	2	5	99.99
10	Entropy	5	2	84.93
11	Entropy	5	3	99.98
12	Entropy	10	2	84.93
13	Entropy	10	3	85.9
14	Entropy	10	5	99.7
15	Entropy	10	10	99.98

with rank-one combination as the Gini criterion, ten minimum samples in the node, and three for maximum depth, providing a mean accuracy score of 99.9%.

Fig. 3 illustrates the normalized features and the normalized first difference Δ features of the HOMO-LUMO gap, HOMO energy, LUMO energy, Dipole moment, and Polarizability characteristics. In this figure, each violin shape shows the probability density of the data for that feature. Wider regions represent more data points at that value, and narrower regions represent fewer data points. The white dot in the center symbolizes the average, and the thick bar shows the interquartile range. This highlights that the features are properly normalized and balanced. Table 2 denotes the normalized features of the HOMO-LUMO gap, HOMO energy, LUMO energy, Dipole moment, and Polarizability characteristics. The dataset includes 133885 normalized molecule IDs. We only listed the 10, 20, 30, 40, and 50 molecule ID's normalized values in the table. This highlights the feature with different scales and improves tree-split quality, enabling thresholds to be interpretable across features.

Fig. 4 shows the normalized molecular features and their corresponding threat-mapped features. This graph shows, how different features are distributed across the dataset after normalization. The normalized features and threat-mapped features highlight the significance of reinterpreting features. This combination of features enables the classification more robust, interpretable, and resilient against threats. This helps the decision tree classifier for early detection of quantum threats. This highlights how normalization, threat mapping,

Table 2
Calculated sample normalized features of the extracted HOMO-LUMO gap, HOMO energy, LUMO energy, Dipole moment, and Polarizability features.

Molecule ID	HOMO-LUMO Gap	HOMO energy	LUMO energy	Dipole moment	Polarizability
10	0.56	0.31	0.57	0.12	0.095
20	0.46	0.54	0.62	0.11	0.11
30	0.48	0.51	0.62	0.02	0.17
40	0.53	0.50	0.69	0.045	0.16
50	0.38	0.69	0.61	0.063	0.19

and delta features together contribute to the decision tree classification.

Fig. 5 demonstrates the composite threat score and the Δ composite threat score through the threat mapping approach. It calculates the threat score based on the molecule IDs. The negative value represents the lower potential quantum threat, and the positive value denotes the higher potential quantum threat. The threat mapping process computes consistently across the dataset. The threat mapping features and the weighted sum of features are utilized to calculate the composite threat score and Δ composite threat score. The sample composite threat score and Δ composite threat score is based on the molecule IDs 10, 20, 30, 40, and 50 and are listed in Table 3. The overlap of Composite and Δ Composite highlights that both capture the same general risk distribution, making it useful for the AI decision tree classifier to detect rising or falling threat levels. This highlights how composite threat scores and Δ composite scores are calculated and distributed. Together, they improve the Decision Tree's input, activating quantum-resistant blockchain defenses.

Fig. 6 illustrates the distributions of quantum threat levels using the AI decision tree classifier. As shown in this figure, the decision tree classifier has classified 45.4% threats as low threat, 33.4% threats as high threat, and 21.1% threats as moderate threat. These classified threat levels are used to activate the cryptographic scheme enforcement in Ethereum fork, as denoted in Fig. 7.

4.1.2. *Ethereum fork implementation results*

Table 4 illustrates the metrics-based analysis of the Ethereum fork node such as throughput, block time, latency, fork rate, data propagation, and peer counts, based on the normalized performance. The experimental results indicate that the Ethereum fork implementation achieves a high transaction throughput of 855 TPS, demonstrating strong scalability under the evaluated network conditions. The Dilithium signature latency of 12ms, making it suitable for high-performance blockchain environments. The system experiences a limited number of fork events (6 occurrences). A data propagation delay

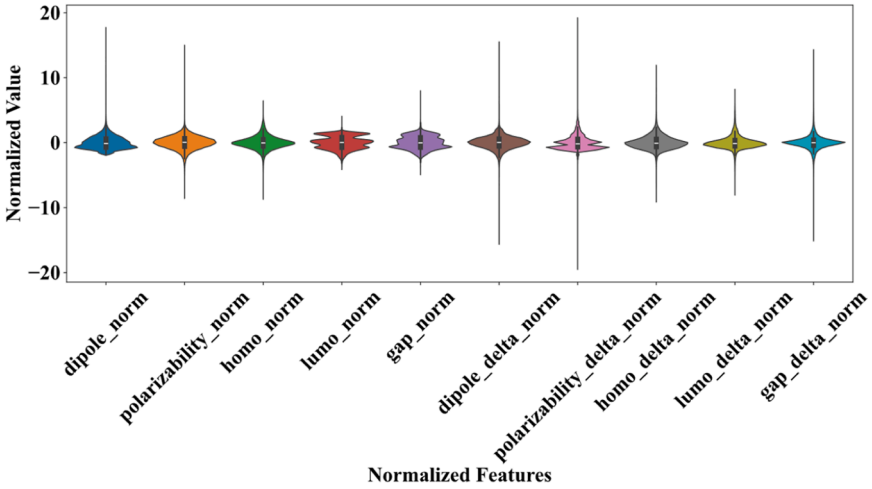


Fig. 3. Visualization of the normalized features and Δ normalized features through the z-score normalization technique.

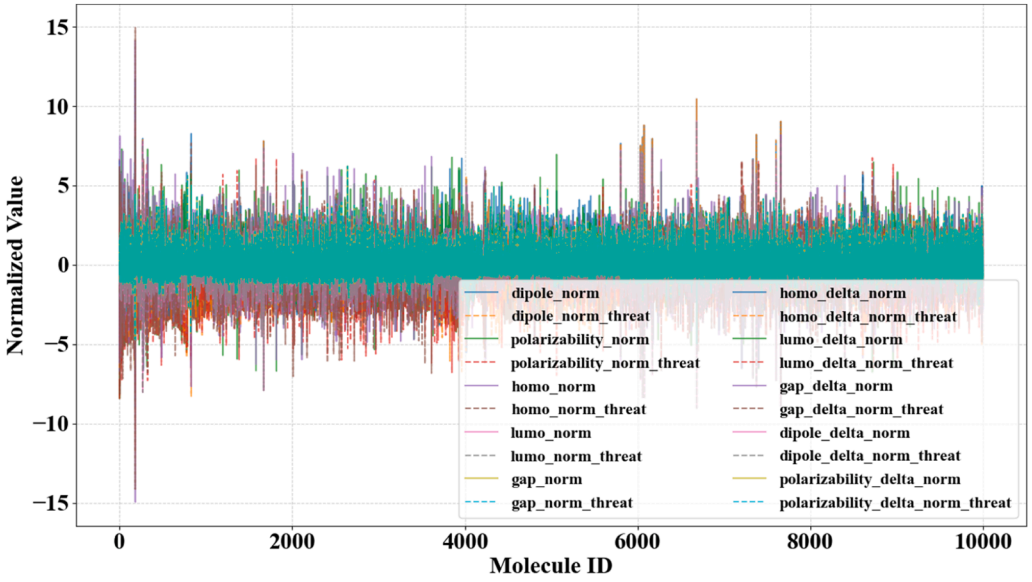


Fig. 4. Visualization of normalized features and threat-mapped features for the composite score calculation.

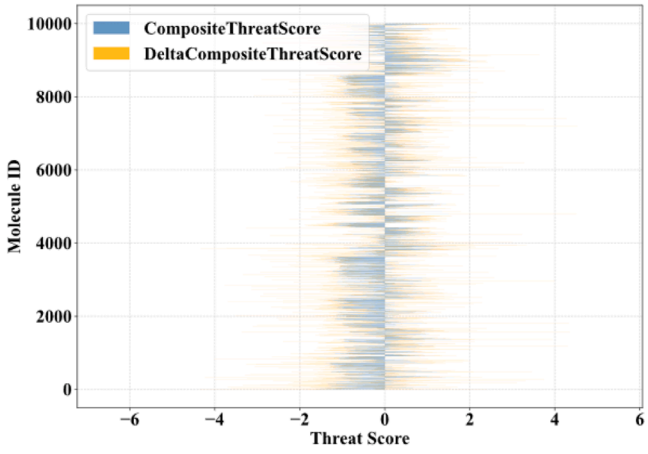


Fig. 5. Visualization of the composite threat score and Δ composite threat score based on the 10000 molecule IDs.

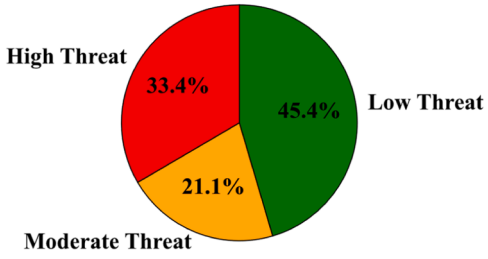


Fig. 6. Quantum threat level classification as low, high, or moderate threat.

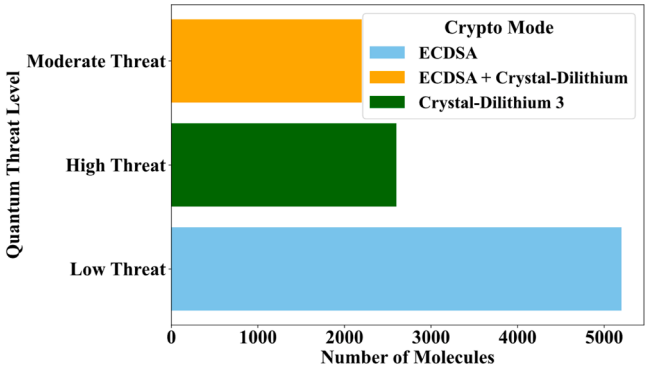


Fig. 7. Cryptographic scheme enforcement based on the detected quantum threat levels: low, high, and moderate threats.

Table 3
Calculated sample composite scores and Δ composite scores from the threat mapping score and WLC approach.

Molecule ID	Composite score	Δ composite score
10	1.17667754667072	0.494470301094402
20	-0.725141233208579	-0.765141233208579
30	-1.23887308515879	-3.62692429048569
40	-1.11425162609476	-2.49025288558827
50	-0.59399085655054	1.52378532997306

of 120ms suggests efficient distribution of blocks and transactions across the network. The average block time of 2.4 seconds highlights the capability of the forked Ethereum network to achieve faster block confirmation compared to public Ethereum deployments.

Fig. 8 demonstrates the operational performance of the Ethereum fork nodes based on the throughput and average block time. The y-axis represents the values of the throughput and average block time. Block finality represent that a block of transactions is permanently added to the blockchain and cannot be reversed or altered. This graph shows that if one node has high throughput but long block times, it is overloaded. If

Table 4
Performance analysis of the Ethereum fork nodes.

Metrics	Measured Value
Throughput (TPS)	855
Dilithium Signature Latency (ms)	12
Fork Events	6
Data Propagation Delay (ms)	120
Average Peer Count (nodes)	42
Average Block Time (s)	2.4

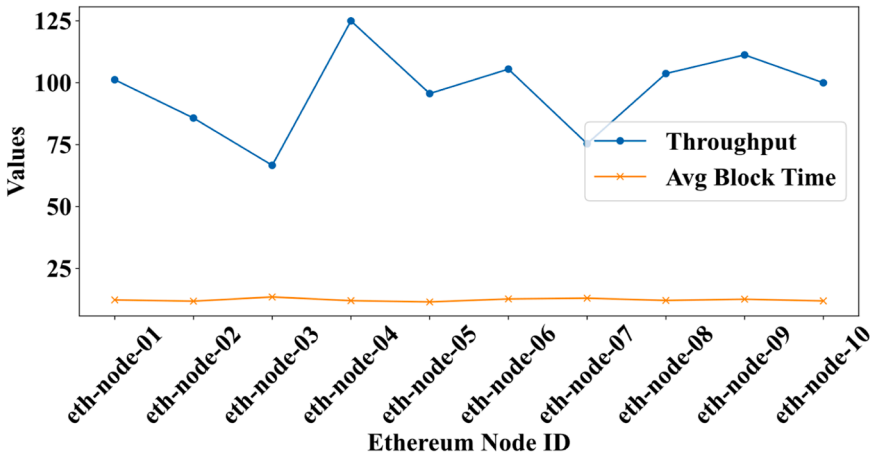


Fig. 8. Throughput and average block time measured across Ethereum fork nodes under varying network conditions.

a node has balanced throughput and block time, it represents an optimal configuration. This helps identify bottleneck nodes in the network. This highlights that the proposed blockchain framework sustains greater than 90 throughputs across most nodes while block finality is stable with 12s.

4.1.3. Analysis of cryptographic switching performance

Table 5 demonstrates the cryptographic switching performance of the quantum threat levels as low, high, and moderate. This examines the performance of the model with different cryptographic schemes and different threat levels. The average signature validation time (ms) calculated by measuring the past time required to verify each cryptographic signature during transaction validation. The switching time **(s)** represents the duration required to transition from one cryptographic scheme to another. The switching efficiency (%) quantifies the effectiveness of the cryptographic transition and is computed as the ratio of successfully processed transactions during the switching period. The transaction success rate (%) is calculated as the percentage of transactions that are successfully validated, committed, and included in the blockchain in the evaluation period. The downtime during switch measures the total duration for which the blockchain network is unable to process or finalize transactions during cryptographic transitions. The low, high, and moderate threats obtain a better average signature validation time of 57.02ms, 27.21ms, and 43.81ms with respect to their cryptographic schemes. The low, high, and moderate threats obtain a transaction success rate of 100%, 99.41%, and 99.95% respectively. These highlights switching between schemes occurred with zero downtime, proving feasibility of seamless post-quantum adoption through hot-swappable consensus modules.

4.1.4. Analysis of consensus algorithm selection

Table 6 illustrates the consensus algorithm's performance with the metrics of throughput, latency, and security score based on the randomly selected five scenarios. Each row in the table represents different simulated situation through the Bayesian optimizer that results in the suitable consensus algorithm and expected performance. The scenarios S1-S5 represent the test case representing possible real-world network state. As shown in this table, Bayesian optimization selects a PoS under low-threat high-uptime, dBFT when throughput spikes, PBFT when security substances most.

Table 7 illustrates the hot-swappable consensus module activation in Cosmos SDK module performance. It analyses the observed system behavior during a live transition of consensus protocols within the Cosmos SDK, when the blockchain is switched from PoS to PBFT. The entire switching process is completed in 1.2s, demonstrating the efficiency of the hot-swappable consensus module without causing service downtime. The switch from one consensus protocol to another is triggered by the Bayesian optimizer, which monitors three categories of telemetry such as network load, validator behavior, and threat level. The use of PoS, PBFT, and dBFT provides adaptability. This enables blockchain to optimize for the right balance of throughput, latency, and security at runtime. This makes the blockchain resilient, efficient, and future-proof in a quantum-threat environment. This table proves that Cosmos SDK's hot-swappable consensus module allows the blockchain to change consensus protocols while maintaining ledger integrity, validator agreement, quantum security readiness, and near-continuous throughput, with only minor resource overhead. Table 8 investigates the performance of security logging of the proposed model. It shows the signature latency, Transactions per Second, Consensus Transitions, and Validator Participation of the proposed model. This highlights the

Table 5
Cryptographic switching performance analysis based on the quantum threat levels.

Threat level	Active cryptography scheme	Avg. signature validation time (ms)	Switching time (s)	Switching efficiency (%)	Transaction success rate (%)	Down time during switch
Low	**ECDSA**	**57.02**	**1.2**	**90.33**	**100**	**No**
	Crystal-Dilithium 3	61.20	1.1	83.91	99.46	No
	ECDSA with Crystal-Dilithium	61.28	1.5	66.67	99.61	No
High	ECDSA	48.72	1.8	85.56	99.21	No
	Crystal-Dilithium 3	**43.81**	**1.3**	**96.92**	**99.95**	**No**
	ECDSA with Crystal-Dilithium	47.31	1.6	62.51	99.30	No
	ECDSA	29.55	1.3	76.92	99.06	No
Moderate	Crystal-Dilithium 3	29.63	1.2	73.33	99.25	No
	ECDSA with Crystal-Dilithium	**27.21**	**1.1**	**83.43**	**99.41**	**No**

Table 6
Consensus algorithm selection performance based on the five scenarios.

Scenario ID	Network Condition (tx/s, validator_uptime, threat)	Chosen Consensus Algorithm	Expected TPS	Latency (s)	Resource Utilization (%)	Security Score
S1	~94 tx/s, 99% uptime, Low threat	PoS	~92	~6.0	65	0.71
S2	~120 tx/s, 98% uptime, Moderate threat	PBFT	~115	~5.5	72	0.78
S3	~150 tx/s, 97% uptime, High threat	dBFT	~140	~6.0	80	0.75
S4	~80 tx/s, 99.5% uptime, High threat	PBFT	~78	~5.2	70	0.77
S5	~100 tx/s, 96% uptime, High threat	PBFT	~95	~5.0	74	0.79

Table 7
Performance of hot-swappable consensus module activation in Cosmos SDK.

Metric	Value
Previous Consensus Protocol	PoS
Selected Consensus Protocol (Activated)	PBFT
Mode Transition Time	1.2 sec
State Synchronization Status	Successful
Validator Agreement	98% participation confirmed the switch
CPU Usage	45% → 52%
Memory Usage	320 MB → 360 MB
Throughput	95.1 tx/sec
Avg Block Finality Time	5.2 sec
Fork Events	0 (during the interval)
Quantum Resistance Readiness	Maintained (Dilithium-3 validation stable ~12.9ms)

Table 8
Performance of security logging of the proposed model.

Metric / Category	Details
Signature Latency	ECDSA: ~2.5ms Dilithium: ~12.9ms
TPS (Transactions per Second)	~95.1 tx/sec after PBFT activation
Consensus Transitions	PoS → PBFT Switch time: 1.2 sec
Validator Participation	~98%
Alerts	No anomalies detected
Feedback Loop	Logs and alerts feed directly into Bayesian Optimization engine, guiding adaptive protocol selection in subsequent intervals

assurance of robustness and alerting context of the proposed model.

Table 9 presents the transaction processing and validation performance of the proposed quantum-aware blockchain framework. The transaction processing shows all transactions submitted during the interval were confirmed, validated, and immutably recorded on the blockchain. Block Production represents blocks that achieve deterministic finality, meaning once a block is committed, it cannot be reverted. The state consistency indicates all validators were synchronized to an identical ledger state, and no inconsistencies occurred during the consensus switch.

4.1.5. Scalability analysis of the proposed model

Fig. 9 illustrates the throughput and average block time performance across 451 Ethereum fork nodes. This graph evaluates the scalability and stability of the Ethereum fork system. In this figure, variable node environments for most validators sustain high throughput. Block times remain reliable despite throughput changes. The deviation between

Table 9
Performance of transaction processing and validation.

Category	Details
Transaction Processing	Confirmed and secured transactions recorded on the blockchain
Block Production	Finality Time: ~5.2 sec (PBFT, post-switch)
Quantum Resistance	Maintained (Dilithium validation ~12.9ms)
State Consistency	All validators synchronized with identical ledger state

throughput variability and stable block time illustrates how the Bayesian optimizer dynamically adjusts consensus selection.

Table 10 represents the decision tree's performance based on the synthesized molecular dataset. The QM9 dataset includes 133885 molecule IDs. We synthesized datasets to analyze the scalability of the model. This highlights the proposed model scales linearly with dataset size and maintains predictive quality. This also ensures it can handle large-scale molecule-derived datasets.

Table 11 investigates the transaction throughput under the large molecular dataset. The transaction was tested across consensus algorithms PoS, dBFT, and PBFT. The PoS consensus algorithm reduces throughput gradually but remains efficient. The dBFT attains the highest throughput with large validator sets, and PBFT drops throughput due to quadratic message overhead, but ensures highest safety under high threat Table 12.

4.1.6. K-fold cross-validation

The 5-fold cross-validation results of the proposed proposed Quantum-adaptive cryptography and adaptive multi-consensus blockchain framework on the QM9 dataset are presented in Table 2. The performance is consistently high across all folds. The last row defines the mean and standard deviation of the all folds. This highlights the consistency and reliability of the model. This proves the generalizability of the proposed model for enhanced the blockchain resilience under evolving quantum threats and network conditions.

4.1.7. Ablation study

We have performed ablation analysis under two categories: Ablation study 1 and Ablation study 2. Ablation study 1 analyses the decision tree's classification performance with each component of the proposed model as illustrated in Table 13. This proves normalization is essential, and without normalization, accuracy drops by 10%. Threat mapping is significant, and without threat mapping, the decision tree misinterprets, and the accuracy decreases. Without WLC, the accuracy drops nearly 7% and with WLC, it improves the robustness of the model. By replacing the decision tree with a random forest, the performance of the random forest is slightly better. However, it utilizes more time for threat reaction. This highlights that the decision tree has better performance in threat level classification with an accuracy of 91.34%.

Table 14 evaluates the various configurations on the proposed framework with metrics including average throughput (TPS), average latency (s), consensus selection optimality (%), cryptographic switch downtime (s), threat reaction time (s), validator recovery time (s), and Quantum Resilience Score (QRS) (0–1). The static cryptographic switching and static consensus algorithm attained a lower performance compared to the proposed quantum-adaptive blockchain framework. This highlights that the proposed framework attains better performance with cryptographic switching mechanism, adaptive consensus algorithm selection, and hot-swappable mechanisms.

4.2. Comparative analysis

This section compares the proposed framework with the existing approaches Falcon and Crystal-Dilithium, Crystal-Dilithium, Blockchain consensus algorithm, and QBIoT approaches, as represented in Table 15. The comparative evaluation conducted using the same benchmark

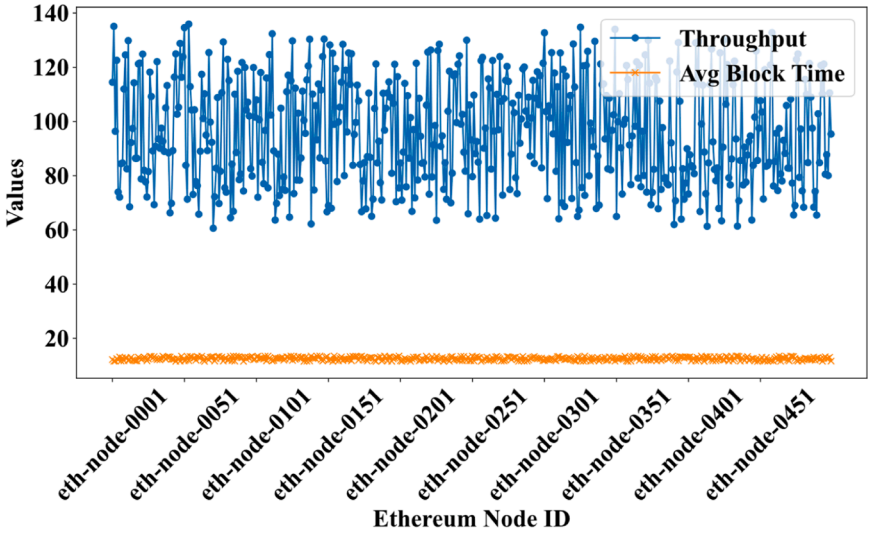


Fig. 9. Throughput and average block time across Ethereum fork nodes for scalability analysis.

Table 10
Decision tree's performance based on the synthesized dataset.

Dataset Size	Training Time (s)	Total Inference Time (ms)	Inference Time per sample (ms)	Accuracy (%)	F1 Score (%)
133,885	0.898	15.660	0.000585	91.34	91.01
140,000	0.950	16.200	0.000590	91.70	91.40
150,000	1.050	17.000	0.000600	92.10	91.80
160,000	1.180	18.100	0.000605	92.45	92.20
170,000	1.300	19.200	0.000610	92.80	92.55

Table 11
Analysis of blockchain transaction scalability.

Validator Count	PoS (TPS)	dBFT (TPS)	PBFT (TPS)
100	90.2	110.5	95.1
200	88.0	107.3	93.4
300	85.7	104.6	91.8
400	83.5	101.2	90.0
500	81.0	98.7	88.5

Table 12
Cross-validation performance of the proposed framework on the QM9 dataset.

Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Fold 1	91.28	90.61	91.12	90.86
Fold 2	91.46	90.82	91.31	91.06
Fold 3	91.31	90.69	91.08	90.88
Fold 4	91.39	90.75	91.24	90.99
Fold 5	91.26	90.58	91.05	90.75
Mean ± SD	**91.34 ± 0.08**	**90.69 ± 0.09**	**91.16 ± 0.11**	**90.91 ± 0.11**

datasets and identical experimental conditions for both the proposed method and the compared approaches. The existing approaches attained a TPS value of 94.2, 93.45, 92.31, 92.6, while the proposed model attained a Throughput (TPS) value of 95.1 with a latency of 5.2s. This shows the effectiveness of the proposed model in quantum-adaptive blockchain environments.

4.3. Discussion

The experimental results of the proposed Quantum-adaptive cryptography and adaptive multi-consensus blockchain framework

Table 13
Ablation study 1-analysis of decision tree classifier.

Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Threat Reaction Time (s)
Without Normalization	82.95	81.10	80.85	80.97	1.32
Without Threat Mapping	83.42	81.65	81.22	81.43	0.31
Without WLC	84.08	82.40	82.13	82.25	1.30
Random Forest (With normalization + threat mapping + WLC)	88.57	86.95	87.41	87.17	0.00110
Decision tree (With normalization + threat mapping + WLC)	**91.34**	**90.65**	**91.18**	**91.01**	**0.00045**

enhanced the blockchain resilience under evolving quantum threats and network conditions. The proposed framework responds dynamically to the real-time threat assessment and workload changes. The observed improvements in transaction throughput, stable block finality, and seamless cryptographic transitions confirm that adaptability is a key for future-proof blockchain systems. The zero-downtime switching between cryptographic schemes validated the feasibility of cryptographic agility without disrupting current network operations. The comparative analysis shows that the solution is more comprehensive as it addresses security and scalability issues together. Additionally, the suggested framework incorporates AI-based quantum threat classification and adaptive cryptographic switching and multi-consensus selection. This results in superior robustness across varying threat scenarios and transaction loads. This allows the blockchain to be able to operate optimally and reduce the emerging quantum risks. The advantages of the offered framework are real-time decision-making, cryptographic agility, and consensus flexibility in one system. The Bayesian-optimized consensus selection mechanism ensures efficient trade-offs between security and performance. This highlights that the proposed framework advances blockchain security models and demonstrates the practical benefits of intelligent adaptability. This also provides a promising direction for secure and scalable decentralized system in the post-quantum environments.

However, the study acknowledged some limitations. The quantum

Table 14
Ablation study 2- analysis of quantum-adaptive blockchain framework.

Configuration	TPS	Latency (s)	Consensus Optimality (%)	switch Downtime (s)	Threat Reaction Time (s)	Validator Recovery (s)	QRS (0–1)
With Decision Tree only	82.3	6.1	71.5	0.0	0.00050	1.8	0.74
No Crypto Switching (static ECDSA)	88.7	4.2	69.0	0.0	0.00040	1.6	0.61
No Crypto Switching (static ECDSA + Crystal-Dilithium)	83.2	6.8	72.8	0.0	0.00052	1.9	0.77
No Crypto Switching (static Crystal-Dilithium 3)	74.5	8.4	73.3	0.0	0.00059	2.1	0.83
No Bayesian Optimizer (static consensus PoS)	79.1	5.7	68.5	1.2	0.00045	2.0	0.70
No Bayesian Optimizer (static consensus dBFT)	85.6	6.2	71.0	1.4	0.00047	2.1	0.76
No Bayesian Optimizer (static consensus PBFT)	90.4	5.4	73.9	1.5	0.00050	2.3	0.79
Without Hot-Swappable	81.0	7.2	72.1	3.6	0.00055	3.4	0.72
Proposed (Quantum-adaptive blockchain framework)	**95.1**	**5.2**	**98.0**	**0.0**	**0.00045**	**1.2**	**0.94**

Table 15
Comparative analysis with existing state-of-the-art approaches.

Reference	Model	TPS	Latency (s)
Revathi and Suganthi, 2025, [16]	Falcon and Crystal-Dilithium	94.2	6.4
Reddy et al., 2025, [17]	Crystal-Dilithium	93.45	7.3
Frikha et al., 2021, [18]	Blockchain consensus algorithm	92.31	6.8
Liu et al., 2024, [19]	QBIoT	92.6	6.3
Proposed		**95.1**	**5.2**

threat assessment model depended on predefined datasets and simulated threat scenarios, which did not accurately reflect the future quantum attacks. Also, using adaptive cryptographic and consensus algorithms introduces additional computational costs. This impacts performance in resource constrained environments. Future research will focus on large-scale real-world deployment and benchmarking of the proposed framework on heterogeneous blockchain networks. Future research will also focus on integrating similarity-based sequential prediction models that can learn from historical operating regimes to predict network conditions, validate behavior, and evolve quantum threats [42,43]. Such predictive intelligence would enable the blockchain to anticipate environmental changes and perform proactive cryptographic scheme selection and consensus adaptation. These enhancements improve the practical applicability of the proposed approach in quantum-adaptive blockchain environments.

5. Conclusion

The study successfully developed a quantum-adaptive cryptography and adaptive multi-consensus blockchain framework. The proposed framework addressed the emerging quantum computing threats and maintained scalability and efficiency. The proposed framework integrated AI-driven quantum threat classification with dynamic cryptographic switching between ECDSA, hybrid ECDSA with Crystals-Dilithium, and Crystals-Dilithium 3. This enabled seamless security adaptation without network downtime. The Bayesian optimization-based multi-consensus layer dynamically selects the most suitable consensus protocol (PoS, PBFT, or dBFT) based on real-time network conditions and validator behavior. Experimental results demonstrated improved transaction throughput, stable block finality, reduced validator recovery time, and enhanced quantum resilience across varying threat scenarios. These confirm the effectiveness of the proposed framework in achieving a secure, scalable, and future-proof blockchain framework.

The managerial and economic contributions of this study provide practical guidance for blockchain frameworks. The ability to dynamically switch cryptographic schemes and consensus mechanisms without service disruption reduces upgrade costs, minimizes operational downtime, and lowers long-term maintenance risks. This adaptability enables organizations to extend the lifecycle of blockchain infrastructures. This improves return on investment while maintaining evolving security standards in quantum-aware environments. The proposed framework introduces a quantum-adaptive framework, which integrates real-time quantum threat detection, dynamic cryptographic switching, and adaptive consensus selection. The proposed approach extends theoretical understanding of blockchain adaptability by demonstrating how AI-driven decision mechanisms can be embedded into consensus layers. The findings contribute to the future-proof distributed ledger systems by formalizing adaptability as a fundamental design principle for quantum-resilient blockchains. The proposed framework supports scalable and resilient blockchain deployment across heterogeneous operational environments. The proposed framework demonstrates an effective approach for achieving quantum-resilient blockchain security by integrating AI-driven quantum threat assessment, adaptive cryptographic migration, and dynamic consensus selection. The experimental results validate its capability to improve security adaptability and scalability under varying blockchain conditions. The effectiveness of the framework is demonstrated within the evaluated blockchain security scenarios; however, further validation on larger-scale blockchain networks and real-world deployment environments remains an important direction for future research.

CRediT authorship contribution statement

Jermin Jeaunita T. C: Writing – original draft, Conceptualization. **Panimozhi K:** Conceptualization. **Sangeetha Francelin Vinnarasi F:** Methodology. **Upendra Kumar:** Project administration. **Haiter Lenin Allasi:** Writing – review & editing. **Sasikumar P:** Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] A. Wicaksana, A survey on quantum-safe blockchain security infrastructure, Comput. Sci. Rev. 57 (2025) 100752, https://doi.org/10.1016/j.cosrev.2025.100752.
[2] M. Campbell-Verduyn, F. Giumelli, Enrolling into exclusion: african blockchain and decolonial ambitions in an evolving finance/security infrastructure, J. Cult. Econ. 15 (4) (2022) 524–543.

[3] H. Gharavi, J. Granjal, E. Monteiro, Post-quantum blockchain security for the internet of things: survey and research directions, IEEE Commun. Surv. Tutor. 26 (3) (2024) 1748–1774, https://doi.org/10.1109/COMST.2024.3355222.

[4] A.U. Kulkarni, S. Jain, A. Kumar, Quantum computing and quantum blockchain: Recent advancements, analysis and future directions. Quantum and Blockchain for Modern Computing Systems: Vision and Advancements: Quantum and Blockchain Technologies: Current Trends and Challenges, Springer International Publishing, Cham, 2022, pp. 311–339.

[5] Z. Yang, M. Zolanvari, R. Jain, A survey of important issues in quantum computing and communications, IEEE Commun. Surv. Tutor. 25 (2) (2023) 1059–1094, https://doi.org/10.1109/COMST.2023.3254481.

[6] K. Csenkey, N. Bindel, Post-quantum cryptographic assemblages and the governance of the quantum threat, J. Cybersecur. 9 (1) (2023) tyad001.

[7] T.C. Jermin Jeaunita, T. Ramesh, C.V.S.R. Manjushree, P.T. Shantala, A decentralized and efficient crowdfunding framework for secure transactions and user engagement, Radioengineering 34 (3) (2025) 381–392, https://doi.org/10.13164/re.2025.0381.

[8] R. Vadisetty, A. Polamarasetti, Quantum computing for cryptographic security with artificial intelligence, in: 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA), IEEE, 2024, pp. 252–260, https://doi.org/10.1109/ICCMA63715.2024.10843897.

[9] B. Fauseweh, Quantum many-body simulations on digital quantum computers: state-of-the-art and future challenges, Nat. Commun. 15 (1) (2024) 2123.

[10] K. Cherkaoui Dekkaki, I. Tasic, M.D. Cano, Exploring post-quantum cryptography: review and directions for the transition process, Technol. (Basel) 12 (12) (2024) 241.

[11] M.S. Ferdous, M.J.M. Chowdhury, M.A. Hoque, A survey of consensus algorithms in public blockchain systems for crypto-currencies, J. Netw. Comput. Appl. 182 (2021) 103035.

[12] 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 (2023) 74088–74100.

[13] K. Revathi, K. Suganthi, Enhancing blockchain security against quantum threats through integration of post-quantum cryptographic algorithms, Comput. Electr. Eng. 127 (2025) 110610.

[14] H. Kim, W. Kim, Y. Kang, H. Kim, H. Seo, Post-quantum delegated proof of luck for Blockchain consensus algorithm, Appl. Sci. 14 (18) (2024) 8394.

[15] O.O. Aramide, Post-quantum cryptography (PQC) for identity management, Adhyayan: J. Manag. Sci. 12 (02) (2022) 59–67.

[16] H. Yi, Y. Li, M. Wang, Z. Yan, Z. Nie, An efficient blockchain consensus algorithm based on post-quantum threshold signature, Big Data Res. 26 (2021) 100268.

[17] S. Li, Y. Chen, L. Chen, J. Liao, C. Kuang, K. Li, W. Liang, N. Xiong, Post-quantum security: opportunities and challenges, Sensors 23 (21) (2023) 8744.

[18] J. Chen, W. Gan, M. Hu, C.M. Chen, On the construction of a post-quantum blockchain, in: 2021 IEEE conference on dependable and secure computing (DSC), IEEE, 2021, pp. 1–8, https://doi.org/10.1109/DSC49826.2021.9346253.

[19] X. Sun, P. Kulicki, M. Sopek, Logic programming with post-quantum cryptographic primitives for smart contract on quantum-secured blockchain, Entropy 23 (9) (2021) 1120.

[20] K. Revathi, K. Suganthi, Enhancing blockchain security against quantum threats through integration of post-quantum cryptographic algorithms, Comput. Electr. Eng. 127 (2025) 110610.

[21] N.R. Reddy, S. Suryadevara, K.G.R. Reddy, R. Umamaheswari, R. Guttula, R. Kotoju, Quantum secured blockchain framework for enhancing post quantum data security, Sci. Rep. 15 (1) (2025) 31048.

[22] O.O. Aramide, Post-Quantum Cryptography (PQC) for Identity Management, Adhyayan: J. Manag. Sci. 12 (02) (2022) 59–67.

[23] P. Nwaga, S. Idima, Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure, Int. J. Comput. Appl. Technol. Res. 11 (04) (2022) 155–170.

[24] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, A. Kerrouche, Implementation of blockchain consensus algorithm on embedded architecture, Secur. Commun. Netw. 2021 (1) (2021) 9918697.

[25] A. 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) (2024) 1727–1751.

[26] J. Ktari, T. frikha, M. Hamdi, N. Affes, H. Hamam, Enhancing blockchain security and efficiency through fpga-based consensus mechanisms and post-quantum cryptography, Recent Adv. Electr. Electron. Eng. 18 (7) (2025) 946–958.

[27] H. Qin, Y. Cheng, X. Ma, F. Li, J. Abawajy, Weighted byzantine fault tolerance consensus algorithm for enhancing consortium blockchain efficiency and security, J. King Saud Univ.-Comput. Inf. Sci. 34 (10) (2022) 8370–8379.

[28] S. Tian, F. Bai, T. Shen, C. Zhang, B. Gong, Vssb-raft: a secure and efficient zero trust consensus algorithm for blockchain, ACM. Trans. Sens. Netw. 20 (2) (2024) 1–22.

[29] R. Ramakrishnan, P.O. Dral, M. Rupp, O.A. Von Lilienfeld, Quantum chemistry structures and properties of 134 kilo molecules, Sci. data 1 (1) (2014) 140022, https://doi.org/10.1038/sdata.2014.22.

[30] A.A. Hassan, R.K. Muhammed, T.Y. Mawlood, A.M. Aladdin, B.A. Hassan, T. A. Rashid, Addressing missing data in machine learning: a comparative insights on imputation techniques and classification accuracy, in: 2025 International Conference on Next Generation Information System Engineering (NGISE) 1, IEEE, 2025, pp. 1–10.

[31] A. Mumuni, F. Mumuni, Automated data processing and feature engineering for deep learning and big data applications: a survey, J. Inf. Intell. 3 (2) (2025) 113–153.

[32] S. Kappal, Data normalization using median median absolute deviation MMAD based Z-score for robust predictions vs. min–max normalization, Lond. J. Res. Sci.: Nat. Form. 19 (4) (2019) 39–44.

[33] J. Duan, P. Wang, W. Ma, S. Fang, Z. Hou, A novel hybrid model based on nonlinear weighted combination for short-term wind power forecasting, Int. J. Electr. Power Energy Syst. 134 (2022) 107452.

[34] J. Shanthi, D.G.N. Rani, S. Rajaram, A C4. 5 decision tree classifier based floorplanning algorithm for System-on-Chip design, Microelectron. J. 121 (2022) 105361.

[35] J.M. Chung, Smart Contracts and Ethereum. Emerging Secure Networks, Blockchains and Smart Contract Technologies, Springer Nature Switzerland, Cham, 2024, pp. 229–248.

[36] J.J. Puthiyidam, S. Joseph, B. Bhushan, Temporal ECDSA: a timestamp and signature mask enabled ECDSA algorithm for IoT client node authentication, Comput. Commun. 216 (2024) 307–323.

[37] K.A. Jackson, C.A. Miller, D. Wang, Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Nature Switzerland, Cham, 2024, pp. 418–446.

[38] K. Wang, A.W. Dowling, Bayesian optimization for chemical products and functional materials, Curr. Opin. Chem. Eng. 36 (2022) 100728.

[39] S.M. Hashemi, R.M. Botez, G. Ghazi, Blockchain PoS and PoW consensus algorithms for airspace management application to the UAS-S4 Ehécatl, Algorithms 16 (10) (2023) 472.

[40] X. Wu, Z. Wang, X. Li, L. Chen, DBPBFT: a hierarchical PBFT consensus algorithm with dual blockchain for IoT, Future Gener. Comput. Syst. 162 (2025) 107429.

[41] Y. Kareem, H. Jahankhani, Development of a Decentralized Personal Indefinable Information (PII) Management Systems Using Blockchain dBFT Consensus Algorithm. AI, Blockchain and Self-Sovereign Identity in Higher Education, Springer Nature Switzerland, Cham, 2023, pp. 167–191.

[42] Han, R., Lin, L.H. Similarity-Based Prediction for Digital Twins: Panel Data, Theory, and Applications. arXiv preprint arXiv:2607.00128, 2026. doi: 10.48550/arXiv.2607.00128.

[43] S. Daliri, S.J. Jassbi, Distributed reinforcement learning for heterogeneous blockchain networks: a customized multi-agent architecture for cross-chain optimization, J. Supercomput. 82 (1) (2026) 4.