UDC 004.7: 004.056
IRSTI 50.47.29

https://doi.org/10.55452/1998-6688-2025-22-3-123-133

[1]*Sabeshuly I.
PhD student, ORCID ID: 0000-0002-9691-7993,
*e-mail: ilias.sabeshuly@gmail.com
[1]Akzhalova A.,
Professor, PhD, ORCID ID: 0000-0002-1141-7595,
e-mail: a.akzhalova@kbtu.kz
[2]Sadok Ben Yahia,
Professor, PhD, ORCID ID: 0000-0001-8939-8948,
e-mail: say@mmmi.sdu.dk

[1]Kazakh-British Technical University, Almaty, Kazakhstan
[2]University of Southern Denmark, Sonderborg, Denmark

QUANTUM-ENHANCED BLOCKCHAIN SECURITY: INTEGRATING QUANTUM COMPUTING WITH NETWORK ATTACK DETECTION

Abstract

This paper describes a security framework that uses both blockchain technology and quantum-enhanced anomaly detection. We propose use of blockchain to create an unchangeable record of security events and smart contracts to automatically respond to threats that have been confirmed. A variational quantum circuit (VQC) is the basis for our system's hybrid quantum-classical model. The VQC processes information by turning classical data into quantum states, using parameterized gates to model complicated dependencies, and then measuring the result to classify it. We use a One-vs-Rest (OvR) method to find network attacks like Botnet, Brute Force, and Port Scan. We tested how well it worked in both perfect (noiseless) and simulated noisy quantum environments.The model was 93% accurate without noise and only 92% accurate with noise, which shows that it is strong. We found a major trade-off: the OvR method works well, but it costs a lot of computing power. This indicates that subsequent efforts should concentrate on creating more efficient quantum multiclass classification frameworks.

Keywords: variational quantum circuit (vqc), network anomalies, hybrid quantum-classical architecture, multi-class classification

Introduction

In the financial technology (fintech) sector, smart contracts play a transformative role by automating and securing financial transactions and services. They provide more efficient, transparent, and cost-effective operation. Smart contracts are self-executing agreements whose terms are spelled directly in the code. By embedding contract terms into code on the blockchain, smart contracts automatically enforce agreements without intermediaries.

Blockchains are distributed ledgers that help parties securely send transactions without the need for a trusted third party. Cryptographic technologies and consensus models, such as PoW, PoS, DPoS, PBFT, and PoA, have made blockchains possible [7]. The blockchain guarantees data integrity, as changes in the data can be verified using digital signatures and hash values.

This blockchain functionality ensures the integrity of attack logs and security data, rendering them immutable and available for forensic investigation and compliance verification. Just recording attacks is insufficient; thus, an automatic response system must be implemented to react immediately upon the detection of a security breach.

This can be accomplished via smart contracts to guarantee that designated actions are executed in reaction to identified threats. Besides autonomously countering attacks, blockchain-based smart contracts can administer a decentralized reputation system. A trust rating can be allocated to each IP address or organization, subject to dynamic modification based on its conduct. When a certain source repeatedly engages in malicious activities, its reputation rating diminishes, enabling other servers and security systems to obstruct ongoing interactions with that source.

The integration of AI-driven attack classification with blockchain enhances the effectiveness of this method, utilizing AI to improve threat detection through traffic analysis and reduction of false positives, while the blockchain element guarantees that security decisions are founded on verifiable and safeguarded real-time data. AI-enhanced technologies display efficiency through the utilization of quantum computing. An alternative to this methodology is Quantum Machine Learning (QML).

Quantum computing, through superposition and entanglement for concurrent computation, improves public blockchain networks by enhancing data security, transaction speed, and analytical proficiency. These developments are especially applicable to the multi-stage lifetime of a transaction, involving its progression from user generation and signing to final confirmation on the blockchain by miners. The last block verification phase is crucial for network security, and we will analyze its foundational mechanisms, starting with the traditional Proof of Work (PoW), to evaluate their merits and drawbacks.

PoW is the most classic consensus mechanism on the blockchain, first used by Bitcoin. Its main idea is that the system's participants (the miners) use their computing power to compete in a hash operation (SHA-256). The algorithm for searching for a suitable hash is the most energy-consuming for miners. Each node consumes energy to solve this problem in a large blockchain network, making it energy intensive.

The winner, who is the first to find a hash value below the stated goal, has the right to insert a new block into the blockchain and receive a certain amount of reward. This process requires significant computational resources and energy, making it a secure but resource-intensive consensus method.

Addressing energy challenges related to Proof-of-Work is more efficiently accomplished through alternative consensus processes, technological enhancements, and energy-conserving behaviors within the current classical computing paradigm [1, 5, 16, 17, 29].

Proof-of-Stake (PoS) differs from PoW in using stakes instead of mathematical puzzles, alleviating PoW's energy consumption problem. The term "stake" refers to the number of tokens a user allocates to participate in the validation process. Nodes do not need to solve a mathematical puzzle; instead, their participation in the consensus mechanism correlates with their stakes, and larger stakes exert a more significant impact on the validation of the subsequent block, thus improving both efficiency and energy conservation in consensus. The concerns of Proof of Stake include the risk of centralization and the "nothing at stake" attack, wherein validators may endorse numerous competing chains due to the negligible cost involved, potentially resulting in forks and security vulnerabilities. The Future Outlook underscores the need to create and integrate quantum-resistant cryptographic methods to guarantee enduring security [4, 8, 12, 15, 18, 19, 26].

Delegated Proof of Stake (DPoS) is a type of PoS in which participants use their tokens to select validators who verify and add blocks for rewards. DPoS usually helps to provide much faster transaction processing than PoW as PoS. As such, DPoS usually has some drawbacks, including a less decentralization and various security issues. The challenges of DPoS are the risk of centralization and Manipulation of Voting; due to votes in DPoS systems being based on the amount of cryptocurrency owned, wealthy participants can potentially influence or monopolize decision-making. Quantum computing can potentially alleviate some of the issues with DPoS by improving security, decentralization, and efficiency [9, 10, 20, 23].

Specific consensus mechanisms, such as Practical Byzantine Fault Tolerance and Proof of Authority, are used for private and protected blockchains.

Practical Byzantine Fault Tolerance (PBFT) is a state machine replica copy algorithm that can be applied to synchronous network environments. PBFT has three essential components: view, primary,

and replica. The primary node initiates the voting process, and a replica node ensures its efficiency. When the primary node fails, the view rotation function is called to modify the current primary node. The challenges of PBFT are High Communication Overhead and Scalability Issues.

Quantum computation holds promise for alleviating PBFT's key problems by reducing communication overhead and improving scalability [6, 14, 21, 25, 27].

Proof of Authority (PoA) is an effective and swift consensus mechanism commonly utilized in private and regulated blockchains, like the POA Network, VeChain, and the Ethereum Kovan testnet. In a Proof of Authority (PoA) network, blocks and transactions are validated by authorized participants referred to as "validator nodes." The validator node can validate transactions, and valid transactions are passed on to the lead node for inclusion in new blocks. The proper functioning of PoA requires validator nodes to be uncompromising. Challenges of PoA are centralization, lack of anonymity, and risks related to trust in validators.

Quantum computing has the potential to mitigate many drawbacks of Proof of Authority by improving decentralization, security, privacy, and scalability. Significant contributions encompass quantum randomness for validator selection, quantum-resistant cryptography, and quantum machine learning for behavioral analysis [11, 24, 28].

Combining artificial intelligence, blockchain technologies, and quantum computing opens up new opportunities for creating more secure and effective systems for detecting and preventing attacks. This paper discusses methods for integrating quantum computing with network anomaly detection mechanisms to enhance the cybersecurity of blockchain systems.

This paper consists of the following sections: Introduction, Materials and methods (which details integration aspects and detection mechanisms), followed by sections on Results and Discussion and Conclusion.

Materials and methods

Modern network security uses advanced detection algorithms, including those based on machine learning and variational quantum circuits (VQC), to accurately identify and classify abnormal network traffic. Integrating these complex methods with blockchain technology forms a security ecosystem that ensures data integrity and consensus verification. Where detection results are verified and recorded on the blockchain, providing a reliable basis for analysis, these characteristics open up new opportunities to enhance network security by enabling the development of resilient and tamper-proof cybersecurity systems that seamlessly integrate advanced attack detection mechanisms with secure data management.

As noted above, smart contracts can automatically trigger actions, instant isolating affected nodes or blocking malicious IP addresses, when agents confirm the detection of network anomalies or attacks. To protect the network, smart contracts can distribute verified threat information between interconnected network segments or partner organizations, and can also initiate recovery protocols to restore normal operation after neutralizing the threat. This automation reduces reaction time and the number of human errors during critical security incidents.

Servers can log security events and network anomalies on the blockchain. This will increase transparency because incidents, such as distributed denial-of-service (DDoS) attacks, intrusion attempts, or suspicious activity, will be recorded as transactions in a block, which will create an immutable and reliable audit trail. This approach improves decentralization and distributes trust across the network reducing the number of points of failure and lowering the risk of manipulation by insiders.

Even though the combination of blockchain and network attack detection is promising, it is having trouble scaling up because networks need to be able to handle a lot of real-time security events without slowing down. There is also the problem of delay, since real-time verification is very important when threats are changing. Also, the need for good consensus mechanisms that can quickly check events so that a response can be made in a timely manner must be met. As a result, we

need to improve blockchain protocols for high-speed security applications, create quantum-resistant cryptographic methods, and look into adaptive smart contracts.

Security agents are very important in modern cybersecurity systems because they can adapt in real time, which makes networks more resilient and less likely to have performance problems. In this context, adding Quantum Machine Learning (QML) can speed up the processing of large amounts of data, which will help with accurate anomaly detection. Hybrid quantum-classical algorithms, which mix classical computations with quantum circuits, are the most promising solution, because physical quantum processors are affected by noise and decoherence, limiting their practical application.

Recent research shows a growing interest in QML. For example, provides detailed guidance on the practical application of QML, while explores the vulnerabilities of quantum neural networks and discusses the potential limitations of these methods [3, 22]. Also, demonstrates the effective application of QML in cybersecurity, specifically to detect network attacks [2].

This work utilizes a hybrid quantum-classical architecture based on a variational quantum circuit (VQC) for anomaly detection. The hybrid model combines the VQC with traditional preprocessing and a classification module, where we utilize a One-vs-Rest (OvR) methodology. Our VQC consists of three components, the first stage involves encoding input data and transforming classical information into a quantum state. The second stage consist of parameterized quantum gates, which form the crucial part of the circuit. Here, qubits undergo rotations and entanglement, enabling the modeling of complex nonlinear dependencies. The third stage involves measuring the output state, where quantum information is converted back to a classical representation, and the resulting data is used to update the circuit parameters.

The schematic of our hybrid quantum-classical architecture is outlined as follows:

The scaled input is then passed through a classical fully connected layer to reduce its dimensionality to match the number of qubits, $n_{\mathbf{qubits}}$.

$$\mathbf{z} = \mathrm{ReLU}(W_{\mathbf{fc}}\mathbf{x} + \mathbf{b}_{\mathbf{fc}}). \tag{1}$$

The weights $W_{\mathbf{fc}}$ are initialized using the Xavier (Glorot) method to promote stable convergence. Layer normalization and dropout are applied to obtain the following:

$$\mathbf{z}_{\mathbf{norm}} = \mathrm{LayerNorm}(\mathbf{z}), \quad \mathbf{z}_{\mathbf{drop}} = \mathrm{Dropout}(\mathbf{z}_{\mathbf{norm}}). \tag{2}$$

We apply [13] data reupload technique to improve the results. The quantum circuit encodes the classical features into a quantum state. For each qubit i, the initial encoding is performed by applying the following.

$$|\psi_0\rangle = \bigotimes_{i=1}^{n_q u b i t s} RY(x_{\mathbf{scaled},i})|0\rangle \tag{3}$$

The circuit then comprises $n_{\mathbf{layers}}$ variational blocks. In each block l and for each qubit i, we apply parameterized rotations:

$$|\psi_{l,i}\rangle = R_Y(\theta_{l,i} + 0.1)R_Z(\phi_{l,i} + 0.1)R_X(\gamma_{l,i} + 0.1)|\psi_i\rangle. \tag{4}$$

where $\theta_{l,i}$, $\phi_{l,i}$, and $\gamma_{l,i}$ are trainable parameters. The small offset of 0.1 improves stability during training. Following the rotations, a ring of CNOT gates is applied to entangle the qubits:

$$|\psi_{\mathbf{ent}}\rangle = \left(\prod_{i=1}^{n_{\mathbf{qubits}}-1} \mathrm{CNOT}(i, i+1)\right) \mathrm{CNOT}(n_{\mathbf{qubits}}, 1)|\psi\rangle, \tag{5}$$

After the entangling layer, the input data is reuploaded by reapplying formula four as suggested in [13], with the RZ operator. After that, we add noise to correlate with the real environment of quantum computing. Unlike classical systems, where errors can be corrected using traditional

correction methods, quantum systems are subject to irreversible changes due to the anticloning theorem.

$$|\psi_0\rangle = \bigotimes_{i=1}^{n_q qubits} RY(x_{\text{scaled},i})RZ((x_{\text{scaled},i})^2)|0\rangle \quad (6)$$

Depolarization means that a $1-p$ qubit remains unchanged with probability p and with probability p it becomes a random state. It is modeled as applying Pauli operators with equal probability, meaning that depolarization noise destroys the superposition and randomly changes the qubit's state. A depolarizing channel is applied to each qubit with probability $p = 0.01$:

$$E(\rho) = (1-p)\rho + p\frac{I}{2}. \quad (7)$$

In real quantum processors (such as IBM, Google, and Righetti), noise is unavoidable, and its impact increases with the number of qubits. Therefore, noise modeling in quantum simulators makes it possible to test the stability of quantum algorithms, develop error correction methods, and optimize quantum circuits before running them on real quantum devices. Thus, noise simulation plays a key role in the development of quantum computing, ensuring the transition from theoretical models to the practical use of quantum algorithms.

The circuit concludes with getting the results and converting them to classical values using the Pauli operation:

$$z_i = \langle\psi_{\text{var}}|Z_i|\psi_{\text{var}}\rangle, \quad i = 1, \dots, n_{\text{qubits}}. \quad (8)$$

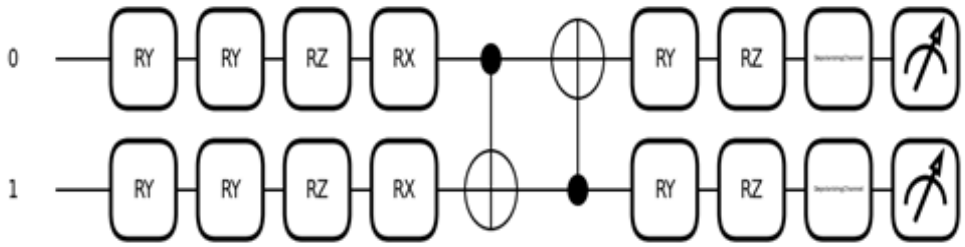

Figure 1 – Full quantum circuit diagram with two qubits, one layer, and noise simulation

The quantum circuit outputs a feature vector $\mathbf{q} \in \mathbb{R}^{n_{\text{qubits}}}$, which is processed by a classical classifier:

$$\mathbf{h} = \text{ReLU}(W_1\mathbf{q} + \mathbf{b}_1), \quad (9)$$

$$\text{logits} = W_2\mathbf{h} + \mathbf{b}_2. \quad (10)$$

The predicted class is determined by:

$$\hat{y} = \text{argmax}(\text{logits}). \quad (11)$$

In our OvR strategy, a separate binary classifier is trained for each class k. For each binary classifier, the labels are defined as:

$$y_{\text{bin}} = \begin{cases} 1, & \text{if } y = k, \\ 0, & \text{otherwise.} \end{cases} \quad (12)$$

Each binary classifier is trained using the binary cross-entropy loss:

$$\mathcal{L}_{\mathrm{BCE}} = -\frac{1}{N}\sum_{i=1}^{N}\left[y_{\mathrm{bin}}^{(i)}\log(p^{(i)}) + \left(1 - y_{\mathrm{bin}}^{(i)}\right)\log\left(1 - p^{(i)}\right)\right], \quad (13)$$

where $p^{(i)} = \sigma\left(\mathrm{logit}^{(i)}\right)$ and σ denotes the sigmoid function. During inference, the final class prediction is made by selecting the class with the highest probability:

$$\hat{y}_{\mathrm{OvR}} = \underset{k}{\mathrm{argmax}}\, p_k. \quad (14)$$

Results and discussion

This section presents the experimental results of the hybrid quantum-classical model for network anomaly detection. We evaluate multi-class classification of network threats, including Botnet, Brute Force, DoS/DDoS, Web Attack, Port Scan, and Normal traffic. Two scenarios are considered.: without noise and with noise introduced to simulate the realistic environment of quantum computing. The results are analyzed regarding precision, recall, and F1-score, followed by a comparative analysis and discussion of the findings.

For testing, we create a quantum model using the PennyLane framework to classify different types of attacks: Botnet, DoS/DDoS, Brute Force, Web Attack, and Port Scan. The testing environment utilizes a laptop with 32 GB of RAM, a 13th-gen Intel® CoreTM i9-13980HX CPU, and an NVIDIA GeForce RTX 4090 laptop GPU. The model determines whether the input is an attack or not. In the event of an attack, the model triggers a defense activation function, which then records the IP address as blocked.

This work utilizes network traffic data from several publicly available sources to evaluate our hybrid quantum-classical classifier. The dataset is formed by concatenating multiple CSV files from the CIC IDS 2017 dataset (https://www.unb.ca/cic/datasets/ids-2017.html) and the CIC-DDoS 2019 evaluation dataset available on Kaggle (www.kaggle.com/datasets/aymenabb/ddos-evaluation-dataset-cic-ddos2019/data/). These files contain traffic captures corresponding to various attack types (e.g., Port Scan, Web Attacks, DDoS, Infiltration) and normal traffic collected at different times and days.

Due to merging datasets with some different parameters, we needed these parameters for datasets that lack them, mainly synthetic IP addresses (Source IP and Destination IP) are generated. After merging the CSV files, the dataset undergoes preprocessing steps, including mean imputation for missing values, standard scaling, and class balancing via SMOTE. The final dataset comprises approximately 12000 samples, distributed evenly among six classes: Botnet, Brute Force, DoS/DDoS, Normal, Port Scan, and Web Attack. For testing, 20% of the dataset is used.

Table 1 – Classification Report Without Noise

Label	Precision	Recall	F1-score	Support
Botnet	0.92	0.97	0.94	439
Brute Force	0.90	0.99	0.94	439
DoS/DDoS	0.92	0.98	0.95	439
Normal	0.97	0.75	0.85	439
Port Scan	0.96	0.97	0.97	439
Web Attack	0.95	0.92	0.93	439
Accuracy			0.93	2634
Macro avg	0.93	0.93	0.93	2634
Weighted avg	0.93	0.93	0.93	2634

When evaluating the model's performance in a noise-free environment, it achieves an overall accuracy of 93% across all classes. The model demonstrates high reliability for the Botnet class with a precision of 0.92, a recall of 0.97, and an F1-score of 0.94, indicating minimal false positives. The model does a good job of finding Brute Force attacks, with a precision of 0.90 and a recall of 0.99, which means that it has a low false negative rate.

For DoS/DDoS attacks the model has a balanced precision of 0.92 and a recall of 0.98, which gives it a strong F1-score of 0.95. Port Scan detection is quite accurate, with a precision of 0.96 and a recall of 0.97. Web Attacks are classified effectively, with a precision of 0.95 and a recall of 0.92, which means that the system is both sensitive and specific. The accuracy for Normal traffic is good at 0.97, but the recall is much lower at 0.75, which means that there are some false negatives.

The model achieves 93% accuracy in a noise-free setting, which shows that it can generalize well across all classes. The macro-averaged precision, recall, and F1-score are 0.93, which shows that the classification performance is stable and trustworthy. These metrics show that the model can tell different forms of network traffic apart, with only small changes in performance between the classes. The results show that the hybrid quantum-classical model can accurately identify network threats in a perfect, noise-free environment. This proves that the variational quantum circuit architecture works well when used with classical preprocessing.

Table 2 – Classification Report with Noise

Label	Precision	Recall	F1-score	Support
Botnet	0.92	0.93	0.92	439
Brute Force	0.90	1.00	0.95	439
DoS/DDoS	0.86	0.97	0.92	439
Normal	0.97	0.75	0.84	439
Port Scan	0.93	0.98	0.95	439
Web Attack	0.94	0.88	0.91	439
Accuracy			0.92	2634
Macro avg	0.92	0.92	0.92	2634
Weighted avg	0.92	0.92	0.92	2634

The addition of noise changes how well different classes are classified. The model still has a high overall accuracy of 92%. For the Botnet class, precision stays the same at 0.92, but recall goes down a little to 0.93, which shows that noise has little effect. The Brute Force detection can still work even when there is noise, and it still has perfect recall at 1.00. When it comes to finding DoS/DDoS attacks, the accuracy drops to 0.86, which means there are more false positives, but the recall stays high at 0.97. Normal traffic classification has a high precision of 0.97 but a low recall of 0.75. This means that the noise did not have a big effect on how careful the model was. Port Scan detection is very reliable, with a precision of 0.93 and a recall of 0.98. Web Attack detection's recall goes down a little to 0.88, but its overall performance is still good, with an F1-score of 0.91. The macro-averaged precision, recall, and F1-score are all 0.92, which shows that the performance is stable across all classes. In general, the model is 92% accurate even when there is a lot of noise, which shows that it is very reliable even when the environment changes. The model still has high recall rates, which means that most attacks are still found, even though noise affects accuracy for some specific classes. The fact that the results stay the same even when there is noise shows that the model is strong and flexible, which shows that it could be useful in real-world quantum computing settings.

In terms of how well the model works, we can find numerous crucial indications by comparing the results we got with and without noise. Adding noise caused a little drop in overall accuracy, from 93% to 92%, which shows that the model's ability to classify things was only slightly affected.

The impact of noise differs by category. The recall rate for the Brute Attack class stays perfect at 1.00 in both cases, showing that the model is quite good at finding these kinds of attacks even when there is noise. For DoS/DDoS attacks, on the other hand, the accuracy drops from 0.92 to 0.86. This means that there are more false positives because of noise, but the recall number stays high at 0.97. For normal traffic, the same pattern can be seen, with a high precision of 0.97. The recall value, on the other hand, is lower at 0.75, which means that noise did not have a big effect on how the model classified normal requests.

The model has shown that it is stable in the Port Scan and Web Attack classes, keeping high levels of precision and recall even with noise. The results show that the model can handle interference well, especially when it comes to finding Brute Force, Port Scan, and Web Attacks. Even still, the higher number of false positives in DoS/DDoS attacks and the persistently poor recall for Normal traffic show that more optimization is needed to get a more even spread of indications across all classes. In general, the results demonstrate that noise might lower false alarms in certain areas but make others less sensitive. To increase performance in real-world situations, deliberate changes are needed.

Conclusion

This paper examines the integration of blockchain networks and smart contracts with quantum-enhanced anomaly detection systems to improve cybersecurity systems. We use a hybrid quantum-classical architecture with VQC. In silent and noisy environments, the model demonstrates an overall accuracy above 90% when classifying network anomalies such as Botnet, Brute Force, DoS/DDoS, Web Attacks, and Port Scans.

The model achieves an overall accuracy of 93% in a noiseless environment. However, due to the lower recall for normal traffic we can see an increase in false positives. In conditions of increased noise, the accuracy decreases slightly to 92%. Comparative analysis has shown that noise factors reduce false positives in some categories but reduce sensitivity in others. This indicates the need for further optimization to balance performance indicators in all classes.

A fundamental component of this research is the implementation of a binary classification strategy utilizing the OvR methodology. This technique trains different binary classifiers for each class, which lets the model handle difficult multiclass classification problems. But this method needs to train quantum circuits n times (where n is the number of classes), which costs a lot of computing power, and the accuracy improvement isn't much more than that of a single quantum multiclass model. This indicates that additional study is required to enhance the OvR technique for quantum circuits or to investigate more efficient designs for quantum multiclass classification. Consequently, subsequent research must enhance the OvR method, augment noise resilience, investigate more intricate quantum circuits, and create adaptive smart contracts for dynamic threat landscapes.

REFERENCES

1 Anita, N., Vijayalakshmi, M., and Shalinie, S. M. Proof-of-Improved-Participation: A New Consensus Protocol for Blockchain Technology. Computer Systems Science and Engineering, 44(3), 2007–2018 (2023).

2 Bellante, A., Fioravanti, T., Carminati, M., Zanero, S., and Luongo, A. Evaluating the potential of quantum machine learning in cybersecurity: A case-study on PCA-based intrusion detection systems. Computers & Security, 104341 (2025).

3 Du, Y., Wang, X., Guo, N., Yu, Z., Qian, Y., Zhang, K., Hsieh, M.-H., Rebentrost, P., and Tao, D. Quantum Machine Learning: A Hands-on Tutorial for Machine Learning Practitioners and Researchers. arXiv:2502.01146 [quant-ph] (2025).

4 Fitzi, M., Gazî, P., Kiayias, A., Russell, A., and Research, I. Proof-of-Stake Blockchain Protocols with Near-Optimal Throughput (2020).

5 Kim, H., and Kim, D. Adjusting the Block Interval in PoW Consensus by Block Interval Process Improvement. Electronics, 10(17), 2135 (2021).

6 Lao, L., Dai, X., Xiao, B., and Guo, S. G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications. In 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), 664–673 (2020).

7 Lin, Z. Comparative Analysis of Blockchain Consensus Algorithms. In Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024), 115, 264–276 (2024).

8 Li, A., Wei, X., and He, Z. Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems. Sustainability, 12(7), 2824 (2020).

9 Li, Y., Xia, C., Li, C., Zhao, Y., Chen, C., and Wang, T. HL-DPoS: An Enhanced Anti-Long-Range Attack DPoS Algorithm. arXiv:2310.15460 [cs] (2023).

10 Narayan, D. G., Arali, N., and Tejas, R. DPoSEB: Delegated Proof of Stake with Exponential Backoff Consensus Algorithm for Ethereum Blockchain. Computer Science Journal of Moldova, 32(2(95)), 262–288 (2024).

11 Naz, M. T., Elmedany, W., and Ali, M. Securing SCADA systems in smart grids with IoT integration: A Self-Defensive Post-Quantum Blockchain Architecture. Internet of Things, 28, 101381 (2024).

12 Neu, J., Sridhar, S., Yang, L., Tse, D., and Alizadeh, M. Longest Chain Consensus Under Bandwidth Constraint. arXiv:2111.12332 [cs] (2022).

13 Pérez-Salinas, A., Cervera-Lierta, A., Gil-Fuster, E., and Latorre, J. I. Data re-uploading for a universal quantum classifier. Quantum, 4, 226 (2020).

14 Qu, Z., Zhang, Z., Liu, B., Tiwari, P., Ning, X., and Muhammad, K. Quantum detectable Byzantine agreement for distributed data trust management in blockchain. Information Sciences, 637, 118909 (2023).

15 Sanda, O., Pavlidis, M., Seraj, S., and Polatidis, N. Long-Range attack detection on permissionless blockchains using Deep Learning. Expert Systems with Applications, 218, 119606 (2023).

16 Sayeed, S., and Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Applied Sciences, 9 (9), 1788 (2019).

17 Hazari, S. S., and Mahmoud, Q. H. Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work. Future Internet, 12 (8), 125 (2020).

18 Sharma, T., Krishna, C. R., and Bahga, A. A Cost-Efficient Proof-of-Stake-Voting Based Auditable Blockchain e-Voting System. IOP Conference Series: Materials Science and Engineering, 1099 (1), 012038 (2021).

19 Siddiqui, S., Srivastava, V., Maheshwari, R., and Gujar, S. QuickSync: A Quickly Synchronizing PoS-Based Blockchain Protocol. arXiv:2005.03564 [cs] (2023).

20 Sun, Y., Yan, B., Yao, Y., and Yu, J. DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. Procedia Computer Science, 187, 371–376 (2021).

21 Tang, S., Wang, Z., Jiang, J., Ge, S., and Tan, G. Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain. Scientific Reports, 12 (1), 4426 (2022).

22 Upadhyay, S., and Ghosh, S. Quantum Quandaries: Unraveling Encoding Vulnerabilities in Quantum Neural Networks. arXiv:2502.01486 [quant-ph] (2025).

23 Wang, B., Li, Z., and Li, H. Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS. Future Internet, 12(8), 122 (2020).

24 Wang, Z., Li, J., Liu, A., Ota, K., Dong, M., and Chen, X. RQPoA: A random quantum PoA Consensus Mechanism in Blockchain Based on Quantum Methods (2024).

25 Weng, C.-X., Gao, R.-Q., Bao, Y., Li, B.-H., Liu, W.-B., Xie, Y.-M., Lu, Y.-S., Yin, H.-L., and Chen, Z.-B. Beating the fault-tolerance bound and security loopholes for Byzantine agreement with a quantum solution. Research, 6, 0272 (2023).

26 Wu, Y., Song, P., and Wang, F. Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain. Mathematical Problems in Engineering, 2020, 1–13 (2020).

27 Xiao, J., Luo, T., Li, C., Zhou, J., and Li, Z. CE-PBFT: A high availability consensus algorithm for large-scale consortium blockchain. Journal of King Saud University - Computer and Information Sciences, 36 (2), 101957 (2024).

28 Zhang, Y., Wang, W., and Shi, F. Reputation-based Raft-Poa Layered Consensus Protocol Converging UAV Network (2024).

29 PoW-BC: A PoW Consensus Protocol Based on Block Compression. KSII Transactions on Internet and Information Systems, 15 (4) (2021).

[1]*Сабешулы И.,
докторант, ORCID ID: 0000-0002-9691-7993,
*e-mail: ilias.sabeshuly@gmail.com
[1]Ақжалова Ә.
профессор, PhD, ORCID ID: 0000-0002-1141-7595,
e-mail: a.akzhalova@kbtu.kz
[2]Sadok Ben Yahia,
профессор, PhD, ORCID ID: 0000-0001-8939-8948,
e-mail: say@mmmi.sdu.dk

[1]Қазақстан-Британ техникалық университеті, Алматы қ., Қазақстан
[2]Оңтүстік Дания университеті, Сённерборг қ., Дания

КВАНТТЫҚ-КҮШЕЙТІЛГЕН БЛОКЧЕЙН ҚАУІПСІЗДІГІ: ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУМЕН КВАНТТЫҚ ЕСЕПТЕУЛЕРДІ БІРІКТІРУ

Аңдатпа

Бұл мақалада блокчейн технологиясы мен кванттық-күшейтілген аномалияларды анықтауды біріктіретін қауіпсіздік жүйесі сипатталады. Біз қауіпсіздік оқиғаларының өзгермейтін жазбасын жасау үшін блокчейнді, ал расталған қауіп-қатерлерге автоматты түрде жауап беру үшін смарт-келісімшарттарды пайдалануды ұсынамыз. Вариациялық кванттық схема (VQC) біздің жүйеміздің гибридті кванттық-классикалық моделінің негізі. VQC ақпаратты классикалық деректерді кванттық күйлерге айналдыру, күрделі тәуелділіктерді модельдеу үшін параметрленген гейттерді қолдану және нәтижені жіктеу үшін өлшеу арқылы өңдейді. Біз Botnet, Brute Force және порттарды сканерлеу сияқты желілік шабуылдарды анықтау үшін «Біреуі бәріне қарсы» (OvR) әдісін қолданамыз. Біз оның өнімділігін идеалды (шусыз) және модельденген шулы кванттық орталарда тексердік. Модельдің дәлдігі шусыз ортада 93%-ды құрады және шулы ортада 92%-ға дейін ғана төмендеді, бұл оның тұрақтылығын көрсетеді. Біз маңызды ымыраны анықтадық: OvR әдісі тиімді, бірақ үлкен есептеуіш шығындарды қажет етеді. Бұл болашақтағы зерттеулерді кванттық көпкласты жіктеудің тиімдірек жүйелерін құруға бағыттау керектігін көрсетеді.

Тірек сөздер: вариациялық кванттық схема (VQC), желілік аномалиялар, гибридті кванттық-классикалық архитектура, көп класты жіктеу.

[1]*Сабешулы И.
докторант, ORCID ID: 0000-0002-9691-7993,
*e-mail: ilias.sabeshuly@gmail.com
[1]Акжалова А.,
профессор, PhD, ORCID ID: 0000-0002-1141-7595,
e-mail: a.akzhalova@kbtu.kz
[2]Sadok Ben Yahia,
профессор, PhD, ORCID ID: 0000-0001-8939-8948,
e-mail: say@mmmi.sdu.dk

[1]Казахстанско-Британский технический университет, г. Алматы, Казахстан
[2]Университет Южной Дании, г. Сённерборг, Дания

КВАНТОВО-УСИЛЕННАЯ БЕЗОПАСНОСТЬ БЛОКЧЕЙНА: ИНТЕГРАЦИЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ С ОБНАРУЖЕНИЕМ СЕТЕВЫХ АТАК

Аннотация

В данной статье описывается система безопасности, которая объединяет технологию блокчейн и квантово-усиленное обнаружение аномалий. Мы предлагаем использовать блокчейн для создания неизменяемой

записи событий безопасности, а смарт-контракты – для автоматического реагирования на подтвержденные угрозы. Вариационная квантовая схема (VQC) лежит в основе гибридной квантово-классической модели нашей системы. VQC обрабатывает информацию путем преобразования классических данных в квантовые состояния, использования параметризованных гейтов для моделирования сложных зависимостей и последующего измерения результата для его классификации. Мы используем метод «Один против всех» (OvR) для обнаружения сетевых атак, таких как Botnet, Brute Force и сканирование портов. Мы протестировали ее производительность как в идеальных (бесшумных), так и в симулированных шумных квантовых средах. Точность модели составила 93% в среде без шума и лишь незначительно снизилась до 92% в шумной среде, что демонстрирует ее устойчивость. Мы выявили существенный компромисс: метод OvR эффективен, но требует значительных вычислительных затрат. Это указывает на то, что последующие усилия должны быть сосредоточены на создании более эффективных систем квантовой многоклассовой классификации.

Ключевые слова: вариационная квантовая схема (VQC), сетевые аномалии, гибридная квантово-классическая архитектура, многоклассовая классификация.

Article submission date: 30.07.2025