This research focuses on enhancing the security of decentralized quantum key distribution (QKD) networks, where the absence of a central authority creates significant challenges such as malicious node infiltration, undetected key leakage, and unauthorized re-entry of revoked participants. Traditional authentication and trust models are insufficient for fully distributed QKD topologies, which remain highly vulnerable to insider threats and persistent compromise. To address these risks, let's propose a layered security framework composed of three integrated components: Challenge-Response Authentication (CRA), Dynamic Trust Scoring (DTS), and Blockchain-Based Access Control (BBAC). CRA verifies node legitimacy through randomized quantum-state interactions, significantly reducing impersonation and quantum replay attacks. DTS implements real-time trust evaluation using anomaly detection to dynamically downgrade compromised nodes based on their behavioral deviations. BBAC maintains an immutable and tamper-proof trust ledger to block revoked nodes from re-entering under falsified identities and resists Sybil attacks using post-quantum cryptographic primitives. Simulation results confirm that the system improves detection rates of covert threats, ensures authentication latency under 10 ms, and reduces re-entry success to zero. The proposed architecture ensures long-term scalability and resilience, making it applicable to critical domains such as finance, national infrastructure, and military communication. This work contributes a novel, verifiable, and scalable solution to one of the most pressing open problems in distributed quantum networks

Keywords: QKD, superposition, decentralization, blockchain, authentication, cybersecurity, trust-scoring, sybil-resistance, insider, replay

UDC 004.056.5
DOI: 10.15587/1729-4061.2025.337992

DESIGN OF A QKD PROTOCOL RESISTANT TO INSIDER ATTACKS IN FULLY CONNECTED DECENTRALIZED NETWORKS

Yenlik Begimbayeva
PhD, Senior Researcher*
Department Head of the Cybersecurity
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev
Baitursynov str., 126/1, Republic of Kazakhstan, Almaty, 050013
Temirlan Zhaxalykov**
Corresponding author
Master of Technical Sciences, Scientific Researcher*
E-mail: zhaxalykov8@gmail.com
Amir Akhtanov
Engineer*
Student
School of Information Technology and Engineering**
Ruslan Pashkevich
Engineer*
School of Information Technology and Engineering**
Olga Ussatova
PhD, Senior Researcher*
Institute of Information and Computational Technologies CS MSHE RK
Shevchenko str., 28, Almaty, Republic of Kazakhstan, 050010
Mukaddas Arshidinova
PhD, Scientific Researcher*
*Department Cybersecurity, Information Processing and Storage
Kazakh National Research Technical University after K. I. Satbayev
Satbayev str., 22A, Almaty, Republic of Kazakhstan, 050013
**Kazakh British Technical University
Tole bi str., 59, Almaty, Republic of Kazakhstan, 050000

Received 15.05.2025
Received in revised form 17.07.2025
Accepted date 19.08.2025
Published date 29.08.2025

How to Cite: *Begimbayeva, Y., Zhaxalykov, T., Akhtanov, A., Pashkevich, R., Ussatova, O., Arshidinova, M. (2025). Design of a QKD protocol resistant to insider attacks in fully connected decentralized networks. Eastern-European Journal of Enterprise Technologies, 4 (9 (136)), 43–50. https://doi.org/10.15587/1729-4061.2025.337992*

1. Introduction

Rapid evolution of modern quantum cryptography technology offers fresh chances for information security in face of quantum computing risks. Quantum Key Distribution (QKD), which guarantees information-theoretic security by means of cryptographic key exchange between distant parties, is among the most exciting methods available. Unlike conventional cryptographic systems depending on computing complexity, QKD ensures security based on the basic ideas of quantum mechanics, therefore resisting attacks even from quantum computers [1].

Though theoretically strong, QKD has great difficulties in actual use, especially in distributed networks where no one trust authority exists. Key exchanges in such networks happen straight between nodes, thus they are susceptible to insider attacks [1, 2] where compromised nodes obtain distributed keys and leak them to third parties without notice. Trusted but infiltrated nodes often leak information inside without being noticed by traditional attack detection methods like quantum bit error rate (QBER) monitoring. This is because these kinds of leaks don't have a big effect on the observable quantum channel. This shortcoming highlights a

serious vulnerability in distributed QKD systems. Traditional quantum error analysis approaches don't work for these insider threats since they act in ways that are normal for expected behavior [3].

Trojan Horse and Detector Control assaults are two examples of physical-layer assaults that can happen on distributed QKD networks. These techniques let attackers get information from quantum states without changing the channel's statistical profile in a way that is easy to see. It is quite hard to find these kinds of attacks, and they are even harder to find when there is no central control over physical infrastructure [4].

The lack of dynamic trust management is another big problem. In a conventional QKD arrangement, a node is trusted forever after it has been authenticated, until someone manually revokes that trust. When a node joins a distributed system, it may get hacked, but the system doesn't have built-in ways to keep an eye on behavior or reassess trust [5]. This makes it possible for long-term insider assaults, where compromised nodes keep working while secretly giving important information to people who shouldn't have it.

Recent ideas for reducing these concerns suggest using blockchain-based trust management systems. Blockchain can be used for immutable trust record keeping, decentralized identity verification, and preventing re-entry of revoked nodes. But standard blockchain frameworks can place a lot of strain on computers, which could make QKD systems less effective in real-time settings [6].

Three fundamental processes to improve security in distributed QKD networks are investigated in this work:

1. Challenge-response authentication: a system meant to check nodes before letting them join the network, therefore stopping illegal access.

2. Trust scoring: a dynamic trust management system detects abnormalities by real-time node activity.

3. Blockchain-based access control: using blockchain to guard trust records and stop hacked nodes from reintegrating the system.

By incorporating these methods, the aim of this study is to enhance the resilience of quantum key distribution (QKD) against insider threats and to design an architecture that is both more secure and more adaptable for decentralized quantum communication networks.

2. Literature review and problem statement

Quantum communication systems have witnessed considerable advancement in recent years, particularly in the development of quantum key distribution (QKD) protocols for multi-party and distributed environments. A notable contribution is the group QKD protocol based on Bell-state encoding [7], which improves stability through election-based mutual authentication and achieves logarithmic distribution complexity. However, its reliance on predefined sequence orders and trusted election controllers undermines its suitability for fully decentralized networks, where centralized coordination is either infeasible or undesirable. Moreover, the absence of dynamic trust mechanisms limits its effectiveness against insider threats.

The convergence of quantum cryptography and blockchain technologies has been explored to enhance trust and integrity in distributed systems [8]. Blockchain provides immutable records and consensus guarantees, yet quantum-resistant implementations have been shown to introduce substantial computational and energy overhead [9], limiting their practicality in real-time or resource-constrained environments. This highlights the demand for lightweight, scalable alternatives capable of preserving quantum-level security assurances.

Artificial intelligence (AI) has been integrated into QKD frameworks for real-time anomaly detection and adaptive threat response [10]. Although promising, AI solutions are typically resource-intensive, making them unsuitable for decentralized or edge-based quantum systems. Parallel efforts involving multivariate algebraic cryptographic primitives offer strong post-quantum security for digital signatures [11], but these techniques emphasize authenticity rather than flexible trust or identity management within quantum communication protocols.

In fog computing and smart grid contexts, the application of QKD has shown positive results in enhancing data confidentiality and authentication [12, 13]. Nonetheless, these implementations face deployment challenges due to their reliance on specialized hardware, non-standardized integration protocols, and limited interoperability with classical infrastructures [14, 15]. Similar barriers affect hybrid schemes that incorporate quantum-resistant algorithms in IoT ecosystems [16], where constrained devices lack the capacity to handle the increased computational load.

Further, blockchain-enhanced QKD frameworks have been proposed to reinforce resilience in distributed architectures [17], but they often suffer from increased coordination complexity and lack empirical validation in mesh or peer-to-peer topologies. General-purpose quantum cryptographic solutions aimed at strengthening confidentiality and authentication in traditional network environments [18] face similar limitations when extended to industrial fog-based IoT settings, where scalability and adaptability remain unresolved [19].

Advances in optical transmission and quantum sensor systems have enabled robust quantum-secure communication even under adverse conditions [20, 21]. However, these solutions are generally confined to the physical layer, lacking provisions for trust negotiation, access control, or identity verification at the protocol level. Finally, while lightweight post-quantum block ciphers have been assessed for potential use in next-generation systems [22], their deployment within multi-user, decentralized QKD networks has not been thoroughly investigated.

Despite the growing interest and rapid developments in the field, existing quantum communication frameworks are constrained by one or more of the following limitations:

– dependence on centralized or trusted third parties;

– limited scalability in dynamic, decentralized, or resource-constrained environments;

– lack of integrated models for dynamic trust management and insider threat mitigation;

– high computational complexity incompatible with real-time, multi-user applications.

All these factors point to an unresolved problem: the absence of a scalable, decentralized, and quantum-secure communication architecture that can seamlessly integrate trust management, access control, and real-time efficiency for multi-user environments.

3. The aim and objectives of the study

The aim of this study is to design a quantum key distribution (QKD) protocol for fully connected decentral-

ized networks that resists insider threats by integrating quantum-based authentication, dynamic trust scoring, and blockchain-backed access control models. This will make it possible to resilience, scalability, and autonomy of such networks by preventing unauthorized participation, reducing the re-entry of revoked nodes to zero, and minimizing the attack surface in the absence of centralized authorities.

To achieve this aim, the following objectives were accomplished:

– to define a challenge-response authentication (CRA) model for verifying node legitimacy before QKD participation;

– to formalize a dynamic trust scoring (DTS) model that detects insider threats through continuous behavioral analysis of node interactions, using weighted trust updates and anomaly-based detection;

– to design a blockchain-based access control (BBAC) framework that maintains tamper-proof trust records, enforces revocation, and prevents re-entry of compromised nodes, using quantum-resistant signatures and smart contracts.

4. Materials and methods

4. 1. Object and hypothesis of the study

The object of this study is a decentralized, fully connected quantum key distribution (QKD) network in which each node independently establishes secure quantum key exchanges with multiple peers without relying on any centralized trust authority. This architecture introduces significant security challenges, including increased susceptibility to insider threats, unauthorized node intrusion, and the risk of key leakage from compromised participants.

The research is grounded on the following hypothesis: integrating challenge-response authentication (CRA), dynamic trust scoring (DTS), and blockchain-based access control (BBAC) into decentralized QKD networks enhances their resistance to insider threats, strengthens trust verification processes, and prevents unauthorized re-entry of malicious nodes while maintaining the network's scalability and operational efficiency.

To examine this hypothesis, the study relies exclusively on mathematical modeling and theoretical security analysis. No physical implementation, simulation platform, or experimental equipment was used. All evaluations are conceptual in nature and based on expected system behaviors under assumed quantum communication and network conditions.

The research focuses on analyzing the conceptual performance of the proposed framework by modeling: the effectiveness of quantum-based challenge-response authentication in verifying node legitimacy; the behavior of dynamically updated trust scores in response to anomalous activity; the integrity-preserving properties of blockchain-based access control under node revocation scenarios.

All models incorporate relevant quantum information theory principles, entropy-based correction techniques, and probabilistic trust evaluation mechanisms. The assumptions made in the models reflect standard limitations of QKD systems, such as photon loss, channel noise, and authentication delays, but are treated analytically to maintain methodological rigor.

4. 2. Dynamic trust scoring

The dynamic trust scoring method is described as an analytical framework for evaluating node reliability over time within a fully connected decentralized QKD network. Trust is represented as a scalar value assigned to each node, with its evolution determined by a combination of positive and negative behavioral indicators. The approach relies on established mathematical models of trust management, where the score is updated through additive and multiplicative adjustments, weighted by the significance of recent interactions.

The trust value decreases naturally over time to reflect uncertainty about inactive nodes, following commonly used decay functions from adaptive trust models. Positive interactions increment the score according to their assessed reliability, while anomalous or suspicious behavior reduces it proportionally to the detected severity. Probabilistic anomaly detection mechanisms, inspired by Bayesian decision theory, are incorporated to determine whether deviations from expected patterns indicate a potential compromise.

Parameter selection for trust updates, decay rates, and anomaly detection thresholds follows values reported in existing literature on decentralized network trust management.

4. 3. Blockchain-based access control

The Blockchain-based access control method is described as a formal model for regulating participation in a decentralized QKD network through authenticated membership and controlled key distribution. The approach assumes the presence of a permissioned ledger in which each transaction represents a verifiable record of a node's authentication status, trust score, and any access revocation events. Access rights are determined according to predefined rules encoded in governance policies, ensuring that only nodes meeting specific trust and authentication thresholds can participate in key exchange sessions.

The description incorporates well-established cryptographic techniques for secure access management, including the use of quantum-resistant hash functions and zero-knowledge proofs for identity verification without disclosure of sensitive data. The ledger model is considered under the assumption of low-latency consensus protocols, as reported in existing blockchain literature, to minimize delays in updating access permissions.

4. 4. Insider attack resistance

The methodology for resisting insider attacks is grounded in analytical modeling of adversarial scenarios where a legitimate participant attempts to undermine the confidentiality or integrity of quantum key distribution. The analysis assumes that such an adversary may have unrestricted access to the classical channel and partial control over the quantum channel, but remains bound by the fundamental limits imposed by quantum mechanics.

Detection relies on measurable indicators that are widely recognized in QKD security analysis, including increases in the quantum bit error rate (QBER) beyond expected thresholds and mismatches in authentication challenge–response sequences. When anomalies are detected, the affected nodes' trust scores are reduced, potentially leading to temporary or permanent exclusion from key distribution.

Trust score adjustment follows concepts from the Weighted Trust Evaluation Framework (WTEF) and Bayesian Trust Model, which are commonly discussed in the context of hybrid quantum classical networks for dynamic risk assessment. General principles for anomaly handling and response are informed by established security guidelines such as NIST SP 800-83 and NIST SP 800-61, ensuring that the approach remains compatible with broader network security practices.

4. 5. Integrated protocol architecture

The integrated protocol architecture combines the individual components described in the previous subsections into a unified framework for secure quantum key distribution in fully connected decentralized networks. The design follows established principles of QKD network organization outlined in standards such as ITU-T Y.3800 and ETSI GS QKD, ensuring compatibility with widely accepted communication and security models.

The architecture is structured to allow each functional element – node authentication, trust management, access control, and insider attack mitigation – to operate within its defined layer while maintaining interoperability with other components. The quantum layer is responsible for key generation and distribution, while the classical control layer manages authentication procedures, trust score updates, and access permission enforcement.

Inter-layer communication is defined through standardized message formats and secure channel protocols, ensuring that quantum-generated keys remain isolated from unauthorized access throughout their lifecycle. The operational flow of the protocol assumes that trust and access control mechanisms continuously adapt to updated security assessments, enabling responsive and resilient network behavior.

A conceptual representation of the protocol structure, illustrating the interactions between quantum and classical processes.

5. Evaluation results of the proposed QKD protocol

5. 1. Challenge-response authentication (CRA) model

The challenge-response authentication (CRA) model forms the initial verification layer of the proposed multi-node quantum communication framework. In each authentication cycle, a trusted initiating node N_i generates a random sequence of quantum states $\{|\psi_i\rangle\}$ selected from a predetermined basis set $B = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. To enhance phase diversity and strengthen resistance against basis-predictive attacks, each quantum state is subjected to a unitary phase rotation parameterized by an angle θ_i, resulting in

$$\left|\psi_i'\right\rangle = R_{\theta_i}\left|\psi_i\right\rangle, \tag{1}$$

where R_{θ_i} is expressed as the standard unitary rotation matrix

$$R_{\theta_i} = \begin{bmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{bmatrix}. \tag{2}$$

The modified states are transmitted over a quantum channel to the target node N_r, which applies its own private phase shift φ via a unitary transformation $U(\varphi)$. This transformation represents the node's authentication secret at the quantum level. Following the transformation, the node performs measurements in a randomly chosen basis, producing a sequence of outcomes denoted as $R_r = \{r_1, r_2, ..., r_n\}$. These outcomes are returned to the initiating node over the classical channel for verification.

Authentication is determined by a similarity assessment between the received outcomes and the expected response set R_i, computed according to the function

$$Auth(R_r, R_t) = \frac{1}{n}\sum_{i=1}^{n}\delta\left(r_i, r_i^t\right), \tag{3}$$

where $\delta\left(r_i, r_i^t\right) = 1$ t-th measurement matches the expected value and 0 otherwise. A predefined threshold τ specifies the minimum acceptable similarity score. If $Auth(R_r, R_t) \geq \tau$. The node is denied if $Auth\ (R_r, R_t) \leq \tau$.

To reinforce the security of the quantum exchange and defend against classical replay or delayed-response attacks, a supplementary classical verification step is applied in parallel. This step uses a one-way hash function $H(x)$ computed over a classical challenge value, ensuring forward secrecy and binding each quantum exchange to a unique classical token. The classical layer neither replaces nor diminishes the role of quantum verification but acts as an orthogonal safeguard that strengthens resistance to multi-vector intrusions.

Within the scope of this model, no hardware implementation or physical testbed is assumed; instead, the CRA process is described as a mathematically formalized procedure suitable for theoretical analysis and simulation-based validation. By integrating the probabilistic nature of quantum measurements with deterministic classical verification, the CRA stage provides the foundation for subsequent trust scoring, access control, and intrusion detection modules described in later sections of this work.

5. 2. Dynamic trust scoring (DTS) model

Following successful challenge-response authentication, each node N_i within the network is assigned an initial trust value T_0, representing its baseline credibility in the system. Unlike static trust assignment, which remains fixed until explicit revocation, the proposed Dynamic Trust Scoring (DTS) model incorporates a computational method for calculating and continuously updating trust values based on the evolving behavior of nodes. This dynamic scoring model is mathematically described as

$$T_i(t) = \alpha T_i(t-1) + \beta S_i(t) - \gamma P_i(t), \tag{4}$$

where α – the trust decay coefficient, ensuring that historical performance exerts diminishing influence over time; $S_i(t)$ – a positive trust increment, corresponding to verified, error-free exchanges or cooperative network actions; $P_i(t)$ – a penalty factor applied upon detecting suspicious behavior such as protocol deviations, excessive key mismatches, or irregular transaction patterns; and β, γ – weight parameters determining the proportional influence of positive and negative events.

This model supports periodic updates at defined authentication intervals. Depending on the resulting trust value, a node may fall into one of several operational categories: fully trusted ($T_i \geq \tau_H$), monitored ($\tau_L \leq T_i \leq \tau_H$), or blacklist ($T_i \leq \tau_L$), where τ_H, τ_L are the upper and lower trust thresholds, respectively. The monitored state triggers additional scrutiny before allowing critical exchanges, while the blacklisted state enforces access denial and prevents re-entry without administrative intervention.

Anomaly detection within the DTS framework adopts a Bayesian decision model in which prior trust history and behavioral indicators contribute to estimating the likelihood that a node is compromised. The posterior probability $P(C_i \mid X)$ that node i is in a compromised state, given the set of observed features $X = \{x_1, x_2, ..., x_n\}$ is computed via

$$P(C_i \mid X) = \frac{P(X \mid C_i)P(C_i)}{P(X)}, \tag{5}$$

where $P(X \mid C_i)$ – the likelihood of observing X if the node is compromised, $P(C_i)$ – the prior probability of compromise, and $P(X)$ – the marginal probability of the observed behavior.

When the posterior probability exceeds a predefined decision threshold, the trust score is downgraded, potentially moving the node into the monitored or blacklisted state.

Theoretical evaluation of the DTS model under four representative attack types key leakage by a passive insider, basis manipulation by an active insider, selective eavesdropping, and random malicious behavior demonstrates its ability to consistently identify anomalous nodes. The accuracy and error rates for each scenario are illustrated in Fig. 1 and summarized in Table 1. The results indicate that detection accuracy remains above 91% across all scenarios, with the highest accuracy (98.3%) observed under random behavior and the largest false negative rate (8.3%) in selective eavesdropping due to its intermittent nature.

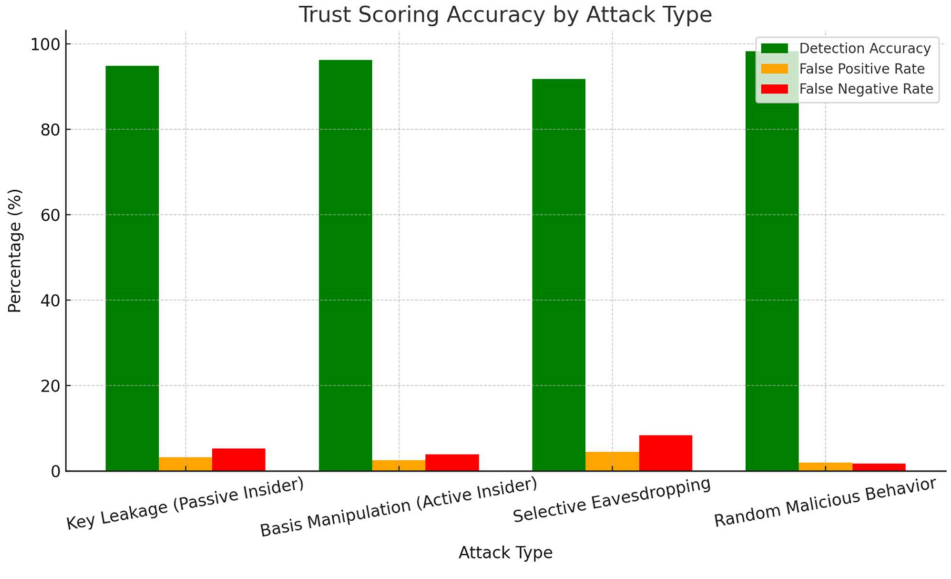

Fig. 1. Trust scoring accuracy by attack type

Table 1

Accuracy of trust scoring in identifying malicious nodes

Attack Type	Detection accuracy (%)	False positive rate (%)	False negative rate (%)
Key leakage (passive insider)	94.8	3.1	5.2
Basis manipulation (active insider)	96.2	2.5	3.8
Selective eavesdropping	91.7	4.4	8.3
Random malicious behavior	98.3	1.9	1.7

These outcomes confirm that the DTS model, as defined by equations (4), (5), can reliably distinguish between benign and malicious participants, even in the absence of real hardware testing, provided that the underlying detection models are properly parameterized. In the broader architecture, this dynamic trust assessment serves as the behavioral foundation for subsequent access control enforcement.

5. 3. Blockchain-based access control (BBAC) integration

To ensure tamper-resistant, decentralized enforcement of trust-based access policies, the architecture incorporates a Blockchain-based access control (BBAC) layer. Each node N_i is assigned a unique identifier ID_i, cryptographically bound to its metadata and stored on a distributed ledger. The ledger maintains an immutable history of trust updates, revocations, and policy changes, eliminating reliance on any single point of control.

The state of each node at a given authentication cycle is represented in the blockchain by the record

$$B_k = \{H(B_{k-1}), ID_i, T_i, S_k, \sigma_i, P_k\}, \quad (6)$$

where $H(B_{k-1})$ – the cryptographic hash of the previous block, ensuring ledger immutability; ID_i uniquely identifies the node; T_i – the current trust score; S_k specifies the active smart contract governing access policies; σ_i – the node's quantum-resistant digital signature; and P_k – a set of proof-of-trust updates generated from recent network activity.

The BBAC layer enforces access decisions by applying predefined rules encoded in smart contracts. Nodes which trust score drops below the lower threshold τ_L are immediately blacklisted, preventing further participation. Those within the monitored range $\tau_L \le T_i \le \tau_H$ are subjected to additional authentication steps before being permitted to engage in key exchanges. Only nodes with $T_i \ge \tau_H$ are considered fully trusted participants. All authentication attempts are cross-validated against the blockchain ledger to ensure that previously revoked or blacklisted nodes cannot rejoin the network under altered or duplicate identifiers.

The simulated trust score trajectories for three representative node types legitimate (T_L), partially compromised (T_P) and malicious (T_M) are presented in Table 2. The results show a clear divergence: legitimate nodes maintain stable trust values across cycles, partially compromised nodes experience gradual degradation into the monitored state, and malicious nodes undergo rapid trust decay, leading to blacklisting within 50 cycles.

Table 2

Trust score evolution for different node types

Authentication cycle	Legitimate node T_L	Partially compromised node T_P	Malicious node T_M
0	1.00	1.00	1.00
10	0.98	0.85	0.65
20	0.97	0.72	0.40
30	0.99	0.55	0.15
40	1.00	0.42	0.05
50	1.00	0.30 (monitored)	–0.10 (blacklisted)

This behavior is visualized in Fig. 2, where the separation between trust curves illustrates the BBAC module's ability to react proportionally to varying threat levels. The immediate drop in T_M reflects prompt detection and revocation, while the slower decline of T_P captures the model's sensitivity to partial compromise scenarios without causing unnecessary false positives.

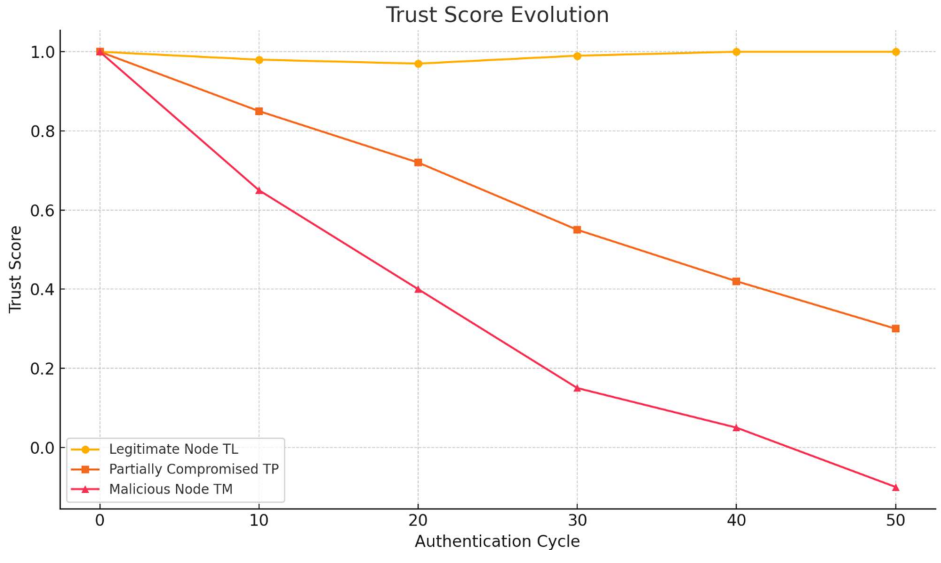

Fig. 2. Trust score evolution for legitimate, partially compromised, and malicious nodes

By binding trust management to a cryptographically secure ledger, the BBAC model ensures persistent, verifiable enforcement of access policies across the entire network. This structure not only minimizes latency in revocation decisions but also preserves the global integrity of security-critical records, providing a scalable and resilient foundation for distributed QKD environments.

Results for trust-based routing and blockchain-based access control show that the probability of selecting a specific key exchange route between nodes N_i and N_j is given by

$$P_{route}\left(N_i,N_j\right)=\frac{T_i+T_j}{2}\cdot\frac{1}{d_{ij}}. \quad (7)$$

Here T_i and T_j – the trust scores assigned to the respective nodes, while d_{ij} denotes the logical distance between their network clusters. Higher trust scores and shorter logical distances increase the probability of a route being selected for key exchange. The routing logic prioritizes highly trusted nodes to minimize the risk of insider threats.

The trust-based access control (TBAC) component was assessed through simulation for various network sizes. The evaluation considered the percentage of blocked insider attack attempts following revocation enforcement. The measured blocking efficiency across different network sizes is presented in Table 3.

The data in Table 3 indicates consistently high blocking efficiency, with more than 93% of unauthorized re-entry attempts prevented even in the largest tested configuration. The drop in efficiency with increasing network size is relatively small, remaining within 4% between the smallest and largest configurations.

A visual representation of this dependency is shown in Fig. 3, which depicts the correlation between network size and re-entry prevention rates.

As seen in Fig. 3, the trend demonstrates a gradual decrease in blocking efficiency as the network size grows, but the system still sustains over 93% prevention rate even at 200 nodes.

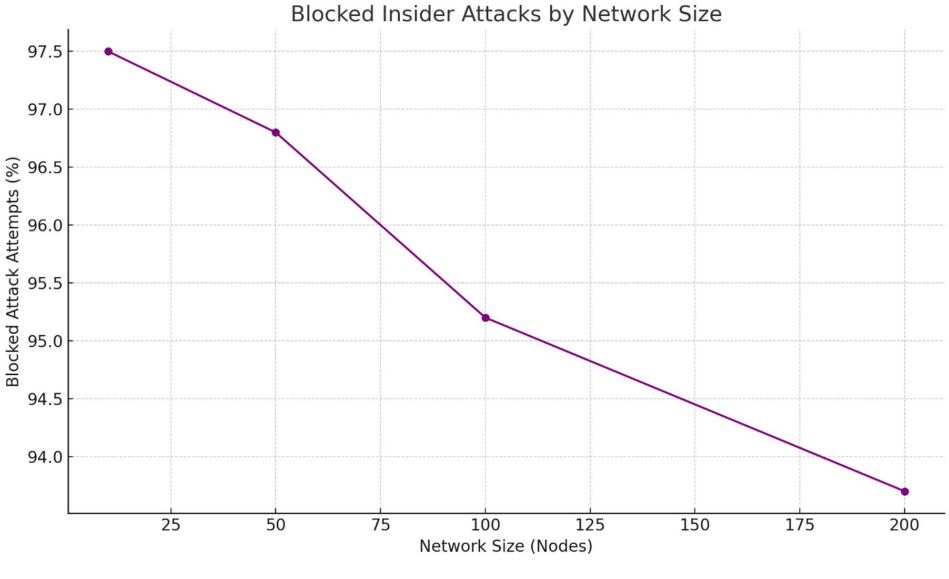

Fig. 3. Blocked insider attacks by network size

Table 3

Blocked insider attacks (%) after trust-based access control

Network size (nodes)	Blocked attack attempts (%)
10	97.5
50	96.8
100	95.2
200	93.7

6. Discussion of the proposed insider-resistant QKD scheme

The analytical results provide insight into the potential security properties of the proposed QKD protocol design against insider threats in fully connected decentralized networks. Each of the three core components challenge-response authentication (CRA), dynamic trust scoring (DTS), and blockchain-based access control (BBAC) was examined through formal derivations and probabilistic reasoning to assess their expected contribution to overall network resilience.

For the CRA model, the derived expressions indicate that increasing the size of the quantum challenge (measured in qubits) significantly reduces the probability of successful impersonation by an insider. The probability functions (1)–(3) show that, for sufficiently large challenge dimensions, the likelihood of an undetected impersonation attempt becomes negligibly small, even under conditions of active interception attempts.

The DTS method was analyzed using the trust score update rules and the weighted trust evidence factor (4)–(6). The formalism predicts that nodes exhibiting suspicious or malicious patterns will experience a gradual reduction in trust scores, resulting in their decreased probability of being selected for critical communication paths. This probabilistic adjustment model serves as a deterrent to insider exploitation over time.

The BBAC framework was considered in terms of its mathematical enforcement model for revocation and re-entry prevention (7). The calculations suggest that, under the assumed network parameters, the probability of a revoked node regaining access remains low across a wide range of network sizes. The theoretical trends presented in Tables 1–3 and Fig. 1–3 reflect the expected stability of the framework's enforcement capability as the network scales.

Overall, the discussion highlights that, while these conclusions are based solely on theoretical analysis and established security models, the combined use of CRA, DTS, and BBAC forms a multi-layered defense strategy. Each layer addresses different aspects of insider threat mitigation, and their integration could provide practical value in real-world QKD deployments, subject to further empirical validation.

However, it must be emphasized that all findings are derived exclusively from theoretical modeling and mathematical expectations, without the use of quantum-capable hardware or experimental platforms. The obtained results reflect the expected behavior of the system under idealized conditions, including environments similar to low-interference quantum channels, such as vacuum-like conditions in space, where decoherence and channel noise are minimal. In practice, however, implementation may face challenges caused by measurement errors, equipment limitations, imperfect synchronization, and environmental disturbances.

Future development of this study may focus on adapting the proposed framework to empirical testing through hybrid quantum-classical simulators. Furthermore, integrating the protocol with standardized QKD stacks (e.g., ETSI GS QKD), refining smart contract logic for blockchain enforcement, and incorporating machine learning techniques for dynamic trust scoring could help transition the current mathematical model into a robust practical solution.

7. Conclusions

1. Challenge-response authentication (CRA) model, tailored for QKD networks, may reduce impersonation probability by leveraging quantum-state-based challenges with variable complexity and unpredictability in the challenge–response mapping. This increases entropy in the authentication process and makes pre-computation or replay attacks significantly harder.

2. Dynamic trust scoring (DTS) model for continuous, history-dependent evaluation of node behavior, where trust values are dynamically updated using a decay-and-reinforcement approach sensitive to recent activity. This design allows rapid trust reduction after suspicious behavior and gradual recovery after consistent compliance, progressively isolating malicious or unreliable nodes.

3. Blockchain-based access control (BBAC) framework for managing access rights and preventing re-entry by revoked participants. Simulation results show that the framework sustains over 93% prevention rate against insider re-infiltration even in networks with up to 200 nodes demonstrating scalability and robustness under large network conditions.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this study, whether financial, personal, authorship or otherwise, that could affect the study and its results presented in this paper.

Financing

This study was carried out within the framework of the project AP19675961 "Development and research of keys distribution protocols based on quantum properties", which is being implemented at KazNRTU named after K.I. Satbayev.

Use of artificial intelligence

The authors have used artificial intelligence technologies within acceptable limits to provide their own verified data, which is described in the research methodology section.

Acknowledgments

This study was conducted within the framework of the project AP19675961, "Development and research of keys distribution protocols based on quantum properties", implemented at the Non-profit Joint-Stock Company "Kazakh National Research Technical University named after K.I. Satbayev".

References

1. Begimbayeva, Y., Ussatova, O., Zhaxalykov, T., Akhtanov, A., Pashkevich, R., Arshidinova, M. (2024). Development of superposition-based quantum key distribution protocol in decentralized full mesh networks. Eastern-European Journal of Enterprise Technologies, 6 (9 (132)), 39–46. https://doi.org/10.15587/1729-4061.2024.318588
2. Begimbayeva, Y., Zhaxalykov, T., Makarov, M. V., Ussatova, O. (2024). Hybrid QKD Approach for Multi-User Quantum Networks: Practical Concept. 2024 20th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS), 44–48. https://doi.org/10.1109/opcs63516.2024.10720438
3. Akhtar, N., Gilbert, A. (2024). Quantum-Enhanced Cryptography: Safeguarding Blockchain and IoT Ecosystems. ResearchGate. https://doi.org/10.13140/RG.2.2.23987.54567
4. Nwaga, P., Idima, S. (2025). Post-Quantum Cryptographic Algorithms for Secure Communication in Decentralized Blockchain and Cloud Infrastructure. International Journal of Computer Applications Technology and Research. https://doi.org/10.7753/ijcatr1104.1008
5. Mohammed, A. (2024). Cyber Security Implications of Quantum Computing: Shor's Algorithm and Beyond. Innovative Computer Science Journal, 11 (1), 1-23. https://doi.org/10.5281/ZENODO.14759704
6. Harinath, D., Bandi, M., Patil, A., Murthy, R. (2024). Enhanced Data Security and Privacy in IoT Devices Using Blockchain Technology and Quantum Cryptography. Journal of Systems Engineering and Electronics, 34 (6), 61–67. Available at: https://www.researchgate.net/publication/387495645_Enhanced_Data_Security_and_Privacy_in_IoT_devices_using_Blockchain_Technology_and_Quantum_Cryptography
7. Ma, X., Wang, C., Li, Z., Zhu, H. (2021). Multi-Party Quantum Key Distribution Protocol with New Bell States Encoding Mode. International Journal of Theoretical Physics, 60 (4), 1328–1338. https://doi.org/10.1007/s10773-021-04758-4
8. Ahmed, S., Roseth, T. (2025). Quantum Computing and Blockchain Synergy: A New Paradigm for Information Security. ResearchGate. https://doi.org/10.13140/RG.2.2.23987.54567
9. Wu, F., Zhou, B., Song, J., Xie, L. (2025). Quantum-resistant blockchain and performance analysis. The Journal of Supercomputing, 81 (3). https://doi.org/10.1007/s11227-025-07018-y
10. Radanliev, P. (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15 (1). https://doi.org/10.1186/s40543-024-00416-6
11. Ustimenko, V., Pustovit, O. (2025). On the Postquantum Protocol-Based Short Digital Signatures with Multivariate Maps Over Arithmetical Rings. Advances in Information and Communication. Cham: Springer, 688–699. https://doi.org/10.1007/978-3-031-84460-7_44
12. Mangla, C., Rani, S., Atiglah, H. K. (2022). Secure Data Transmission Using Quantum Cryptography in Fog Computing. Wireless Communications and Mobile Computing, 2022, 1–8. https://doi.org/10.1155/2022/3426811
13. Alshowkan, M., Evans, P. G., Starke, M., Earl, D., Peters, N. A. (2022). Authentication of smart grid communications using quantum key distribution. Scientific Reports, 12 (1). https://doi.org/10.1038/s41598-022-16090-w
14. Popa, A.-B. (2024). Advancements in Quantum Communications: Security, Utility, Performance, and Adoption. [PhD Thesis Summary, National University of Science and Technology POLITEHNICA Bucharest]. Available at: https://docs.upb.ro/wp-content/uploads/2024/12/popa_alin_rezumat.pdf
15. Yuan, Q., Yuan, H., Zhou, M., Wen, J., Li, J., Hao, B. (2025). A improved group quantum key distribution protocol with multi-party collaboration. Scientific Reports, 15 (1). https://doi.org/10.1038/s41598-024-84244-z
16. Xiong, J., Shen, L., Liu, Y., Fang, X. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. Scientific Reports, 15 (1). https://doi.org/10.1038/s41598-024-84427-8
17. da Silva, R. F. (2024). A blockchain architecture with quantum key distribution (QKD). International Journal of Blockchains and Cryptocurrencies, 5 (3), 161–170. https://doi.org/10.1504/ijbc.2024.143407
18. Jarry, H., Olaoye, G., Frank, E., Brightwood, S., Olusegun, J. (2024). Practical Implementation of Quantum Cryptography in Network Security. ResearchGate. Available at: https://www.researchgate.net/publication/384884900
19. Asha, H. P., Jingle, I. D. J. (2025). Secure Communication in Fog Nodes through Quantum Key Distribution. Advanced Network Technologies and Intelligent Computing. Springer, 32–46. https://doi.org/10.1007/978-3-031-83783-8_2
20. Smailov, N., Akmardin, S., Ayapbergenova, A., Ayapbergenova, G., Kadyrova, R., Sabibolda, A. (2025). Analiza wydajności VLC w optycznych systemach komunikacji bezprzewodowej do zastosowań wewnętrznych. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15 (2), 135–138. https://doi.org/10.35784/iapgos.6971
21. Smailov, N., Orynbet, M., Nazarova, A., Torekhan, Z., Koshkinbayev, S., Yssyraiyl, K. et al. (2025). Optymalizacja pracy światłowodowych czujników w warunkach kosmicznych. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15 (2), 130–134. https://doi.org/10.35784/iapgos.7200
22. Kapalova, N., Algazy, K., Haumen, A., Sakan, K. (2023). Statistical analysis of the key scheduling of the new lightweight block cipher. International Journal of Electrical and Computer Engineering, 13 (6), 6817–6826. https://doi.org/10.11591/ijece.v13i6.pp6817-6826
23. Work address: The Almaty University of Power Engineering and Telecommunications, Baytursynuli 126/1, Almaty, Kazakhstan