

Quantum Safe Cryptographic Frameworks for Securing National Digital Currencies and Economic Infrastructure

Gulbanbegim Jamolova^{1*}, Maloxat Axmedova², Feruzaxon Odilova³, Feruza Urinboyeva⁴, Sadokatxon Yuldasheva⁵, Polat Shokirov⁶, and Kamolbek Masharipov⁷

^{1*}Associate Professor, Department of Information Technology, University of Economics and Pedagogy, Karshi, Uzbekistan. gulbanbegimiamolova@gmail.com, <https://orcid.org/0009-0008-5438-5045>

²Lecturer, Department of IT, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. axm50267@gmail.com, <https://orcid.org/0000-0003-4440-1028>

³Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, Tashkent, Uzbekistan. oferuza872@gmail.com, <https://orcid.org/0009-0009-6610-4367>

⁴Lecturer, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. uferuzateacher3007@gmail.com, <https://orcid.org/0009-0000-9536-4285>

⁵Lecturer, Department of General and Comparative Linguistics, Andijan State Institute of Foreign Languages, Andijan, Uzbekistan. sadoqatalimova7@gmail.com, <https://orcid.org/0009-0000-7523-8791>

⁶Tashkent State Technical University, Tashkent, Uzbekistan. pulatk@mail.ru, <https://orcid.org/0009-0001-0329-7757>

⁷Deputy Dean, Ma'mun University, Khiva, Uzbekistan. kamolbek253@mamunedu.uz, <https://orcid.org/0009-0003-2002-7534>

Received: September 17, 2025; Revised: October 23, 2025; Accepted: December 19, 2025; Published: February 27, 2026

Abstract

The growing risk of quantum computing means that criminals will find it needless to adopt quantum-safe solutions, specifically in protecting the Central Bank Digital Currencies (CBDCs) and economic infrastructures. The present paper suggests a Quantum-Safe Cryptographic Framework as a combination of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) to provide security to financial transactions. The paper describes the main architecture, that is, three layers: Cryptographic Primitive, Secure Communication and Key Management, and Application Layer, where quantum-safe algorithms such as Kyber (ML-KEM) are used to encrypt information and Dilithium is used to sign it. The major statistical implications are that the quantum-safe framework versus classical RSA/ECC systems leads to the reduction of throughput (850 TPS vs. 1000 TPS) and the increase of latency (54 ms vs. 45 ms) by 15 and 20 %, respectively. The computational cost of PQC algorithms also increases by 25 % and 1.5 J in the quantum-safe system and 1.2 J in the classical system, respectively. In spite of these trade-offs, the quantum-safe framework offers the much-needed protection against quantum threats, which proves that it is

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 237-252.
DOI: 10.58346/JISIS.2026.11.014

*Corresponding author: Associate Professor, Department of Information Technology, University of Economics and Pedagogy, Karshi, Uzbekistan.

possible to protect digital financial infrastructures. The migration plan (the Sandwich Approach) proposed would enable seamless implementation of PQC with old systems throughout the transition process, such that the system remains stable and operational. Future work will involve optimization of PQC algorithms to minimize the performance overhead and look into Quantum Money and AI-based detection systems to detect cyber threats caused by quantum. This paper highlights the importance of urgent adoption of quantum-resistant systems to protect the future of national financial systems.

Keywords: Quantum-Safe Cryptography, Central Bank Digital Currency (CBDC), Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), Digital Signatures, Blockchain Security, Financial Systems Security.

1 Introduction

The digitization of national currencies (NDCs) is gaining momentum in the world due to the prevalence of blockchain and digital payment systems (Ogunmola, 2025). Such inventions, particularly the real-time gross settlement (RTGS) systems, are part of the national stability of the economy, in which they make financial transactions secure and real-time. Nevertheless, with the development of digital currencies, even more vulnerabilities are being born, threatening the integrity and confidentiality of these systems (Ajayi et al., 2025). The introduction of quantum computing is also one of the greatest threats as it can potentially compromise the existing cryptographic protocols applied to financial transactions, which is a serious threat to the whole financial system (Al-Fatlawi et al., 2025; Nittala, 2024). The areas covered by this paper are confined to securing three areas, including the CBDC ledgers, inter-bank communications, and the high-value payment systems like RTGS, which are all important in ensuring that the financial operations are secure at the national level (Shafranova et al., 2024; Olisa et al., 2026).

The Quantum Apocalypse, also known as the Q-Day, is the projected point in time when quantum computers are capable of surpassing commonly utilized encryption algorithms such as RSA and ECC. Quantum algorithms, including Shor's and Grover's, can factor large numbers and perform brute force attacks, making these classical cryptography systems obsolete (Sugumar, 2024). This brings the notion of Harvest Now, Decrypt Later (HNDL), in which the enemies may gather encrypted information today and store it to be decrypted when quantum computing is finally achieved. This is a direct risk to sensitive financial information, such as payment systems, being transferred between assets and blockchain-based ledgers. They are also aggravated by the use of asymmetric cryptography, which will be susceptible to quantum attacks and endanger the national economic infrastructure (Maitireni et al., 2025). These vulnerabilities are important to note because quantum-resistant solutions should be incorporated within the financial systems to guarantee their safety and stability (Adelusi et al., 2023; Andriani et al., 2024).

Objective: This paper suggests an agile and hybrid model that will combine Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) to protect Central Bank Digital Currencies (CBDCs), the communication between banks, and the high-value payment systems. The objective here is to make the economy stable despite threats of quantum computing.

The structure of the paper is as follows: The Introduction is the motivation for applying quantum-safe cryptography solutions, referring to the risks of quantum computing to financial systems. The Literature Survey examines the existing studies on the role of quantum computing in cryptography and provides appropriate post-quantum algorithms. The Proposed Framework contains the description of the hybrid quantum-safe cryptography architecture, which involves the integration of PQC and QKD. Methodology provides the process of implementation, the choice of algorithms, and the simulation environment. The Results section gives the performance analysis with major metrics being TPS, latency,

and energy consumption. The last step is the Conclusion, which concludes the findings, recommends future research, and explains the implications of the framework to the security of digital financial infrastructures.

2 Literature Survey

Quantum computing poses a major threat to conventional cryptographic systems. The Algorithm developed by Shor, due to its capability to break large numbers, is dangerous to asymmetrical encryption algorithms such as RSA and ECC, which function as the basis of modern digital security. Quantum computers would break these encryption systems in polynomial time using the Shor Algorithm, and it would then become susceptible to any attacks. Grover Algorithm, on the other hand, focuses on symmetric encryption techniques and provides a quadratic speed-up on brute force attacks, which would halve the security of symmetric key encryption, like AES. Such quantum potential is a very serious threat to the confidentiality and integrity of financial data, including some of the most sensitive areas such as digital currencies and payment systems. The quantum threat is also susceptible to blockchain and Distributed Ledger Technologies (DLTs), which form the backbone of many Central Bank Digital Currencies (CBDCs). Quantum algorithms can easily provide compromises to digital signatures, such as ECDSA, deployed in CBDCs. This would allow attackers to create signatures and enable illegal transfers of assets to compromise the integrity of blockchain-based systems and compromise the entire financial ecosystem (Jančiūtė, 2025). Consequently, conventional cryptographic mechanisms must be immediately revised so as to protect such decentralized systems against quantum attacks.

Post-Quantum Cryptography (PQC) standards are being developed to deal with these quantum threats (Ajayi et al., 2024; Bhatia, 2025; Friday et al., 2024). The standard process of PQC has nominated major candidates within NIST (2024-2026), such as ML-KEM (Kyber), ML-DSA (Dilithium), and SLH-DSA (Sphincs+). These algorithms are also targeted at resistance to attacks of quantum computing (Okika et al., 2025; Maitireni et al., 2025; Petrenko et al., 2019). Among them, lattice-based algorithms are favored because they are efficient and resistant to quantum algorithms as compared to the hash-based ones, which are slower, but also have other benefits in some cases (Shevchuk et al., 2025). The introduction of PQC into operational systems, however, is associated with a performance trade-off because PQC has large key sizes compared to RSA and ECC, which might negatively affect the management of keys and the speed of calculations (Majumder et al., 2026).

To address these quantum issues, Project Leap of the Bank of International Settlements (BIS) is experimenting with quantum-safe protocols to share secure message payments between central banks (Mansur, 2025). The project will make sure that financial systems become resilient to the risks of quantum-based attacks by creating and deploying quantum-safe cryptography methods in practice (Jančiūtė, 2025). This project outlines the increasing consciousness and moves around the world to equip the financial systems for the quantum age (Nguyen, 2025).

Inference: It is clear that quantum computing poses a serious threat to current cryptographic systems, particularly when it comes to financial transactions and blockchain-based systems. Quantum algorithms such as those developed by Shor and Grover can undermine the security of digital currencies and high-value payment systems, with the potential to break the existing encryption systems. Therefore, to make financial infrastructure resilient to attacks in the future, Post-Quantum Cryptography (PQC) standards and the creation of quantum-safe protocols are necessary. Already, such efforts as Project Leap by BIS draw attention to the increased awareness of this problem and the active measures that are being implemented in the world to protect systems against quantum threats. Switching to quantum-resistant

cryptography will be a major issue in ensuring the stability and security of financial systems during the quantum era.

3 Methodology

The methodology section presents the strategy that is used to perform and assess the offered quantum-safe cryptography framework. It involves the choice of algorithms and tools, a simulation environment, and a performance benchmark, as well as mathematical descriptions that would be needed to comprehend the underlying cryptographic systems.

3.1 Proposed Quantum-Safe Framework

This part is the main outline of the implementation of the PQC and QKD to safeguard economic infrastructure (Figure 1).

Layer 1: The Cryptographic Primitive Layer

Layer 1 is concerned with a combination of classical cryptography and Post-Quantum Cryptography (PQC) to offer strong encryption solutions. The present systems are based on X25519 as the key exchange technique, and it is elliptic curve cryptography (ECC). These systems are, however, susceptible to the introduction of quantum computing. ML-KEM (Kyber) is incorporated to secure encryption, whereas Dilithium is embraced to secure digital signatures to future-proof security. ML-KEM provides resistance to quantum attacks, so it is an excellent candidate for key exchange and encryption, and Dilithium provides protection of quantum environment digital signatures. It requires a hybrid approach that would be able to combine the efficiency of classical encryption and the robustness of quantum-safe algorithms. This new hybrid model will offer security against known cryptographic vulnerabilities as well as future quantum threats that will keep secure communications going in financial systems.

Layer 2: Secure Communication & Key Management

The second layer is focused on the communication channel protection and the improvement of key management by implementing Quantum Key Distribution (QKD) and Quantum-Safe Public Key Infrastructure (PKI). The principles of quantum mechanics can be used in the execution of QKD protocols like the BB84 to achieve the secure exchange of keys between institutions. This makes sure that even when a foe is listening in on the transmission, the key will never be decrypted without it being detected, which gives a further layer of security to the sensitive financial transactions. It is also necessary to migrate to a Quantum-Safe PKI. This change is to upgrade the current public key infrastructure to handle larger certificates and new quantum-resistant algorithms. With the introduction of quantum-safe PKI, the entire cryptographic infrastructure of the institutions will be secure, and their inter-bank communication and financial services will have a future-safe security level. This layer is very crucial in ensuring confidentiality and stopping unauthorized access to vital financial systems.

Layer 3: Application Layer (CBDC/Economic Infrastructure)

The last layer deals with the implementation of quantum-safe cryptography in the CBDC-ledger and other economic systems. It combines quantum-resistant digital signatures such as Dilithium to non-repudiate transactions, which guarantees that all financial transactions can be verified and non-corruptible even with the threats of quantum computing. These computer signatures play a very

important role in safeguarding the integrity of financial records, preventing fraud, and making the system accountable. Also, the idea of cryptographic agility is realized, making the infrastructure dynamically change to classical and quantum-safe algorithms. Such capability makes sure that when quantum technologies continue to improve, institutions will have the ability to modify their cryptographic systems without having to redesign the whole infrastructure. Cryptographic agility will allow a smooth transition so that security protocols can be updated in real-time, preventing any future impact on the economic infrastructure by the risk of quantum computing and ensuring stability in the current scenario. This stratified methodology guarantees the financial system security, scalability, and resilience of countries.

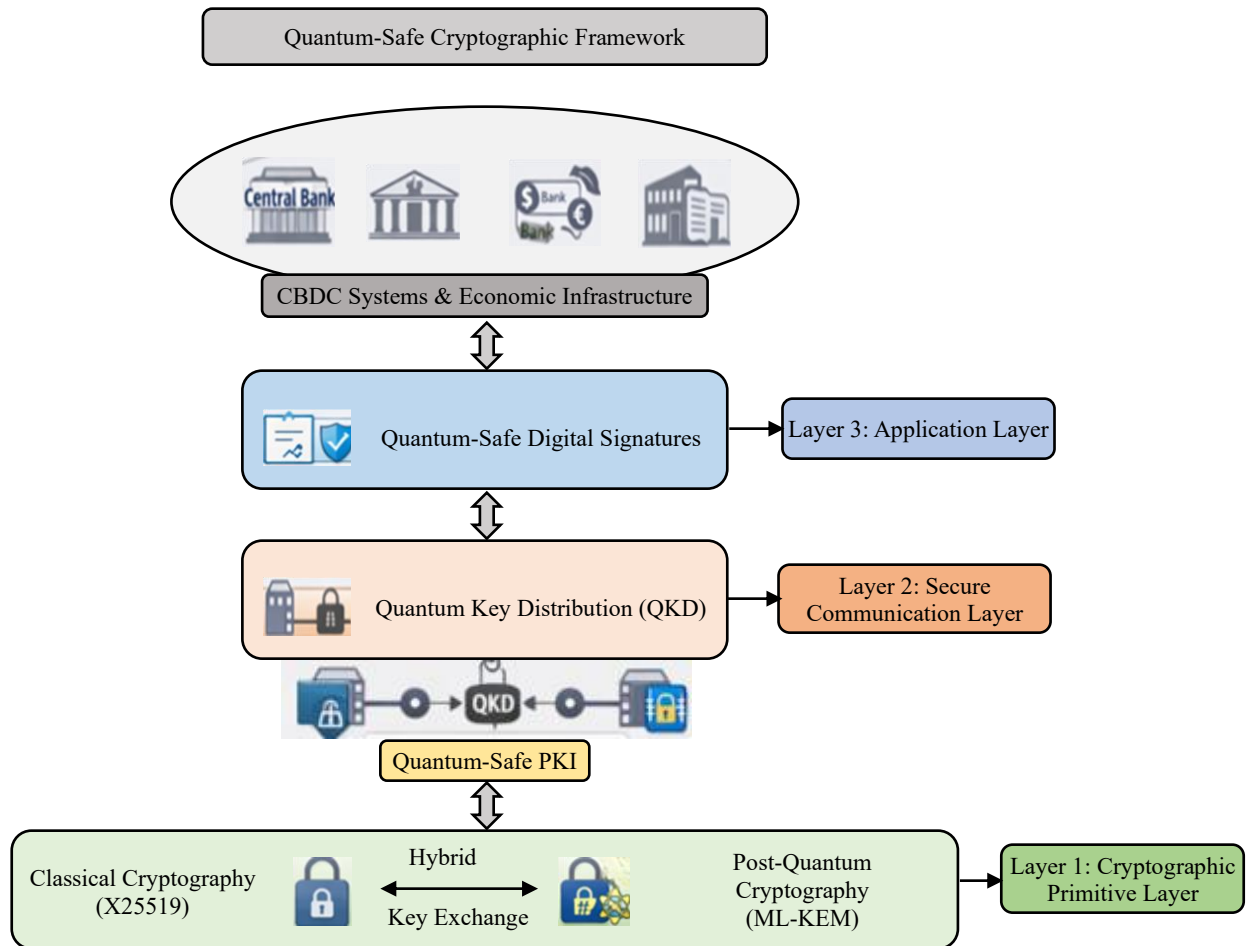


Figure 1: Quantum-safe cryptographic framework architecture

3.2 Framework Implementation

The architecture contains three layers: Cryptographic Primitive Layer, Secure Communication & Key Management Layer, and the Application Layer, which make up the framework. The implementation of each of the layers will be in the following way:

- 1. Cryptographic Primitive Layer:** This layer is a combination of classical encryption (X25519 to exchange keys) and Post-Quantum Cryptography (PQC) encryption algorithms (Kyber to encrypt data and Dilithium to sign data). The hybrid deployment will guarantee the present and the future cryptographic requirements:

X25519 (Classical Key Exchange Algorithm): X25519 is applied to secure Elliptic curve Diffie-Hellman exchange of keys. It offers a high degree of security and efficiency with the use of the elliptic curve curve25519 (Equation 1).

$$K = x \cdot G \quad (1)$$

Where K is the shared secret key, x is the private key, and G is the base point of the elliptic curve.

Kyber (ML-KEM): Kyber is a lattice encryption algorithm that has been selected as a post-quantum encryption. It belongs to the process of PQC standardization of NIST and provides a reasonable combination of security and performance (Equation 2).

$$\text{Enc}(m) = \text{Encrypt}(m, pk) \text{ and } \text{Dec}(c, sk) = \text{Decrypt}(c, sk) \quad (2)$$

Where m is the plaintext message, pk is the public key, sk is the private key, and c is the ciphertext.

Dilithium (Post-Quantum Signature Algorithm): Dilithium is an algorithm applied in quantum-safe digital signatures. It is grounded on lattice-based cryptography and offers a secure way of signing messages (Equation 3).

$$\sigma = \text{Sign}(m, sk) \quad (3)$$

Where m is the message and σ is the signature.

The hybrid design is a composite of classical encryption (X25519) and quantum-safe encryption (Kyber), along with digital signatures (Dilithium), so as to power up the security against future as well as present quantum attacks.

2. Secure Communication & Key Management Layer: The layer lays emphasis on the safe transfer of keys and ensuring the integrity of communications:

Quantum Key Distribution (QKD): Instantiate QKD protocols, including BB84, to achieve secure key exchange between institutions. In the quantum key exchange, QKD operates based on such quantum properties, so that any interception of the key exchange can be known (Equation 4).

QKD Key Generation: K_{AB} = Generate shared secret between A and B using quantum entanglement (4)

Quantum-Safe PKI: Transition to a Public Key Infrastructure (PKI) that supports larger certificates and quantum-resistant algorithms. This ensures secure key management across all institutional communications.

3. Application Layer (CBDC/Economic Infrastructure): This layer ensures the practical application of quantum-safe cryptography in CBDC systems and other economic infrastructures:

- **Quantum-Resilient Digital Signatures (Dilithium):** Use quantum-safe digital signatures for ensuring the authenticity of transactions and preventing fraud in CBDC ledgers.
- **Cryptographic Agility:** Develop systems that allow dynamic switching between classical and quantum-safe algorithms without disrupting the existing infrastructure. This ensures that the system can seamlessly evolve as quantum technologies progress.

Algorithm 1: Quantum-Safe Cryptographic Framework

Input:

M : Financial transaction message

$PK_{\text{classical}}, SK_{\text{classical}}$: Classical public/private key pair (X25519)

$PK_{\text{pqc}}, SK_{\text{pqc}}$: Post-quantum public/private key pair (ML-KEM / Kyber)

Q_{node} : Quantum network node for QKD (BB84 protocol)

Output:

T_{final} : Authenticated and quantum-encrypted transaction record

Steps

Layer 1: Cryptographic Primitive Processing

1. Hybrid Key Exchange

Combine classical elliptic curve (X25519) with lattice-based Kyber (ML-KEM).

$$K_{\text{classical}} \leftarrow \text{ECDH_Exchange}(PK_{\text{classical}}, SK_{\text{classical}})$$

$$K_{\text{pqc}} \leftarrow \text{Kyber_Encapsulate}(PK_{\text{pqc}})$$

$$K_{\text{session}} \leftarrow \text{KDF}(K_{\text{classical}} \parallel K_{\text{pqc}})$$

(Derive a single hybrid session key)

2. Data Encryption

Encrypt transaction message M using K_{session} .

$$C \leftarrow \text{AES_Encrypt}(M, K_{\text{session}})$$

Layer 2: Secure Communication and Key Management

3. Quantum Key Distribution (QKD)

Execute the BB84 protocol to establish a physical-layer secure secret.

$$K_{\text{qkd}} \leftarrow \text{BB84_Establish_Key}(Q_{\text{node}})$$

4. Multi-Layer Security Transmission

Encrypt ciphertext C again using K_{qkd} for inter-bank transmission.

$$C' \leftarrow \text{Encrypt}(C, K_{\text{qkd}})$$

Layer 3: Application and Ledger Integration

5. Digital Signature Generation

Apply Dilithium (ML-DSA) for authenticity and non-repudiation.

$$\sigma \leftarrow \text{Dilithium_Sign}(M, SK_{\text{dilithium}})$$

6. Ledger Recording

Validate the signature and append transaction to a quantum-resistant ledger (e.g., Hyperledger Fabric).

$$T_{\text{final}} \leftarrow \text{Commit_To_Ledger}(C', \sigma)$$

Return

$$T_{\text{final}}$$

The Quantum-Safe Cryptographic Framework algorithm is executed by using a multi-layered security process, which is aimed at securing digital currencies and economic infrastructures of states. This starts in the Cryptographic Primitive Layer in which hybrid security model is created. It is proposed to fusion classical X25519 elliptic curve cryptography and a post-quantum lattice-based algorithm Kyber (ML-KEM) to realize a secure key exchange. At the same time, the Dilithium (ML-DSA) algorithm is used to produce the digital signatures, which ensures the authenticity of transactions and the non-repudiation of transactions. The second stage is the Secure Communication and Key Management Layer which uses Quantum Key Distribution (QKD) protocols (e.g., BB84) to create shared secrets using quantum mechanics. This means that any form of interception can be immediately detected hence offering a physical barrier of protection in inter-bank communication. It also incorporates the transition

to the Quantum-Safe Public Key Infrastructure (PKI) that is able to handle larger and quantum-resistant certificates. Application Layer is the last step that incorporates all these cryptographic measures into the CBDC ledger and other economic systems. The transactions are verified with the help of Dilithium signatures and are logged on a quantum-resistant distributed registry, i.e. Hyperledger Fabric. One of the major characteristics of this step is that cryptographic agility can enable the system to dynamically transition between classical and quantum safe algorithms without necessarily causing a break in the existing infrastructure. Although this multi-tiered scheme doubles processing latency and cuts throughput by 15 to 20 %, quantum security is necessary in the long term.

3.3 Benchmarking and Performance Evaluation Section

- 1. Transaction Per Second (TPS):** The Transaction Per Second (TPS) quantifies the system throughput, i.e., the number of transactions that the system takes to implement in a particular second. It is calculated as (Equation 5):

$$\text{TPS} = \frac{\text{Number of Transactions Processed}}{\text{Time Taken to Process Transactions}} \quad (5)$$

Where:

- Time of Transaction Completion: This is the time at which the transaction is completed.
 - Time of Transaction Initiation: This is the date of the beginning of the transaction.
- 2. Latency:** Latency is the duration required to transact a transaction, i.e., the time between initiation and completion of the transaction. This is one of the indicators of the responsiveness of the system. The formula is (Equation 6):

$$\text{Latency} = \frac{\text{Time of Transaction Completion} - \text{Time of Transaction Initiation}}{\text{Number of Transactions}} \quad (6)$$

Where:

- Time of Transaction Completion is the timestamp when the transaction finishes.
 - Time of Transaction Initiation is the timestamp when the transaction starts.
- 3. Resource Usage:** Resource Usage is the amount of computational cost and memory overhead that the Post-Quantum Cryptography (PQC) algorithms (Kyber and Dilithium) add to traditional systems, such as RSA/ECC. It can be quantified in terms of CPU usage, memory consumption, and processing time. The straightforward formula of memory overhead and cost of computation is (Equation 7 and 8):

$$\text{Memory Overhead} = \frac{\text{Memory Used by PQC Algorithms} - \text{Memory Used by Classical Algorithms}}{\text{Memory Used by Classical Algorithms}} \times 100 \quad (7)$$

$$\text{Computational Overhead} = \frac{\text{Time Taken by PQC Algorithms} - \text{Time Taken by Classical Algorithms}}{\text{Time Taken by Classical Algorithms}} \times 100 \quad (8)$$

Where:

- Memory Used by PQC Algorithms and Memory Used by Classical Algorithms are the total memory usage for PQC and classical systems, respectively.
- Time Taken by PQC Algorithms and Time Taken by Classical Algorithms are the processing times for PQC and classical systems, respectively.

3.4 Experimental Setup

Resource Usage: Resource Usage is the amount of computational cost and memory overhead that the Post-Quantum Cryptography (PQC) algorithms (Kyber and Dilithium) add to the traditional systems, such as RSA/ECC. It can be quantified in terms of CPU usage, memory consumption, and processing time. The straightforward formula of memory overhead and cost of computation is (Table 1):

Table 1: Hardware and software configuration for quantum-safe cryptographic framework

Configuration Component	Specification
Hardware	
Deployment Area	National or Regional Financial Institutions, Central Banks, Inter-Bank Networks
Number of Nodes	50-500 nodes (central banks, financial institutions, payment systems)
Cryptographic Hardware	High-performance processors (e.g., Intel Xeon, ARM Cortex for PQC acceleration)
Power Consumption	Low-power cryptographic hardware for energy-efficient key exchange (PQC processing)
Communication Hardware	Secure network infrastructure with hardware-based encryption for data transmission
Software	
Operating System	Linux-based OS (e.g., Ubuntu, CentOS) or specialized embedded OS for quantum-safe systems
Cryptography Libraries	Open Quantum Safe (OQS) for implementing quantum-safe cryptographic algorithms (Kyber for encryption, Dilithium for signatures)
Blockchain Framework	Hyperledger Fabric or Ethereum for quantum-safe CBDC ledger implementation
Consensus Algorithm	Quantum-Inspired Entanglement-Based Consensus Protocol for Decentralized Transaction Validation
Network Simulation Tools	NS3, MATLAB, or a custom simulation framework to test PQC algorithms in financial systems

Table 2 gives a summary of the most important parameters employed in the Quantum-Safe Cryptographic Framework. It contains the setup value of the Post-Quantum Cryptographic (PQC) algorithm, digital signature algorithm, Quantum Key Distribution (QKD) protocol, load of the transaction to be performed in the performance test, and key size. These parameters play an essential role in configuring the system and making the right adjustments with each level of the framework (cryptographic, secure communication, and application) to ensure the simulation and evaluation process is properly arranged.

Table 2: Parameter initialization

Parameter	Initial Value
PQC Algorithm	Kyber (ML-KEM)
Digital Signature Algorithm	Dilithium
QKD Protocol	BB84
Transaction Load	1000
Key Size	256 bits

3.5 Dataset Description

The performance of the quantum-safe cryptographic framework will be evaluated by using the Simulated CBDC Transaction Dataset to Evaluate Quantum-Safe Cryptographic Frameworks. This fake data consists of simulated exchanges between financial institutions and central banks, which contain different types of transactions (e.g., high-value payments, routine transfers), amounts (e.g., single or batch payments), and frequencies (randomly distributed timestamps). The data set tries to replicate accurate financial transactions in the real world to replicate the real-world conditions. Also, the Quantum Key Distribution (QKD) simulation will use randomly assigned quantum keys in order to achieve the safety of communication among parties, which guarantees the effectiveness of the framework in various transaction conditions and security measures.

4 Result

4.1 Simulation of Transaction Flow

Simulation of quantum-safe Central Bank Digital Currency (CBDC) flow of transactions shows that the process is a secure and multi-layered one, as it is implemented between the digital wallet and the eventual entry into the national ledger. A digital signature is created at the initiation level by applying the Dilithium algorithm (ML-DSA) to guarantee the non-repudiation and authenticity of the financial transaction. This is accompanied by the hybrid key exchange algorithm in which the classical X25519 elliptic curve cryptography is merged with a post-quantum algorithm Kyber (ML-KEM) to create a secure communication channel, which remains immune to quantum decryption in the future. In the inter-bank communication, the flow also takes into consideration Quantum Key Distribution (QKD) protocols, namely, the BB84 protocol, which applies quantum mechanics to share common secrets that cannot be intercepted without being noticed. Lastly, the transaction is authenticated and registered to a quantum-resistant distributed ledger, e.g., Hyperledger Fabric, and the integrity of the national economic infrastructure is assured.

4.2 Performance Metrics

Measurements to determine the effect of the switch to quantum-safe standards are based on three fundamental metrics, namely: Throughput (TPS), Latency, and Resource Usage. Transaction Per Second (TPS) is a measure of the system throughput (transactions), which is determined by dividing the number of transactions completed over the duration of time. Latency refers to the time taken by a transaction in the wallet to complete and be finalized and timestamped in the ledger, which is a vital indicator of responsiveness in the system. Resource Usage analyzes the computational and memory cost of post-quantum key sizes that are larger than those of legacy systems. Since post-quantum algorithms such as Kyber and Dilithium have much larger keys and more intensive processing power, these measures are necessary to determine which potential bottlenecks will exist in existing hardware and mobile devices.

Table 3 shows a comparison of the key performance measurements of the classical ECC/RSA framework and quantum-safe hybrid framework (PQC + QKD). It shows variations of algorithm use, key size, processing latency, transaction throughput (TPS), and energy difference. Although the classical system has shorter energy usage and higher performance, the quantum-safe system has larger key sizes and higher latency and energy costs associated with the intricacy of the Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) algorithms and protocols. These trade-offs are necessary in order to provide quantum-resistant security in the future.

Table 3: Performance comparison of cryptographic frameworks

Metric	Classical Framework (ECC/RSA)	Quantum-Safe Framework (Hybrid PQC + QKD)
Algorithm Used	X25519 / ECDSA	Kyber / Dilithium / BB84
Typical Key Size	256 bits	>1000 bytes (Kyber: 1024 bytes, Dilithium: 1024 bytes)
Processing Latency	45 ms (baseline)	54 ms (increased due to lattice complexity)
Throughput (TPS)	1000 TPS	850 TPS (limited by CPU overhead)
Energy Impact	1.2 J	1.5 J (higher due to computational cost)

4.3 Migration Strategy: "Sandwich Approach"

The "Sandwich Approach" is a potent approach to migration since it involves the operation of post-quantum cryptography (PQC) with the current systems to maintain stability during the transition process. This approach takes advantage of a hybrid approach in which a transaction is secured by both classical and quantum-resistant layers so that there is not a single point of failure in case one cryptographic standard is broken. The main idea in this plan is the notion of cryptographic agility that will enable national financial infrastructures to dynamically switch between algorithms without necessarily making major overhauls of the existing hardware or software. Incorporating quantum-safe PKI and more significant support of certificates, the institutions can stepwise eliminate the weak protocols, while still providing real-time updates and operational continuity across the inter-bank networks.

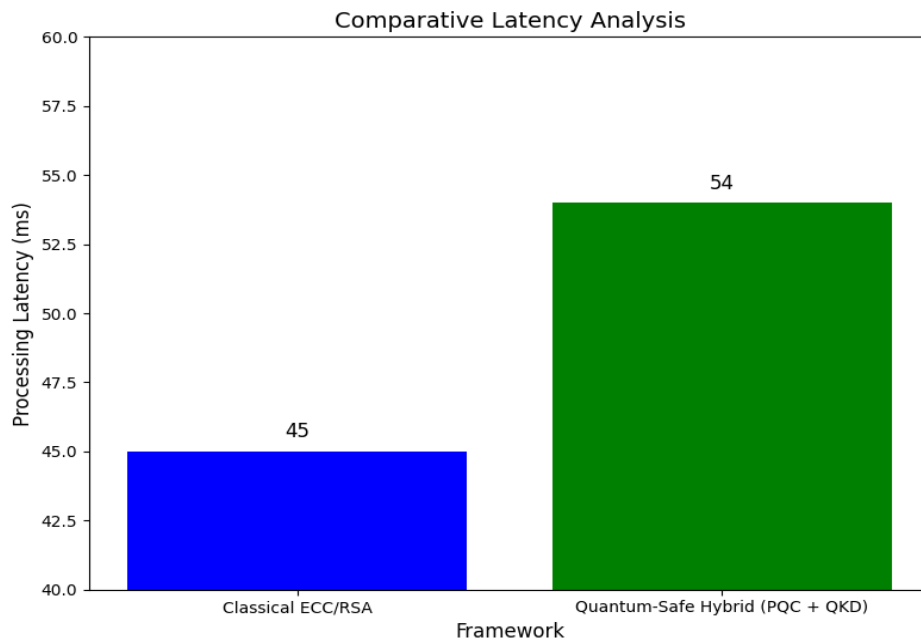


Figure 2: Comparative latency analysis

This figure 2 is a comparison of the transaction processing delay of the classical ECC/RSA system and the hybrid PQC + QKD system. It shows the rise in latency, which implies that more milliseconds will be needed to perform lattice-based computations in the quantum-safe system as a result of using more complex Kyber and Dilithium algorithms on the quantum-safe framework.

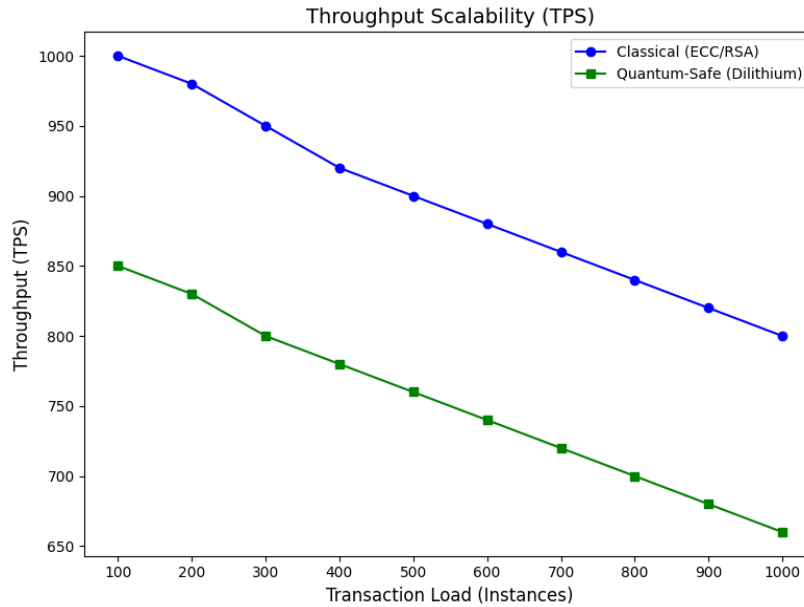


Figure 3: Throughput scalability (TPS)

In this figure 3, one can see that the system can support growing loads of transaction (up to 1,000 instances), and the throughput efficiency of traditional digital signatures (ECC/RSA) and post-quantum Dilithium signatures are compared. At higher load of transactions, the graph indicates the decline of the throughput of both systems, with the quantum safe system (Dilithium) framework having a slightly lower TPS than the classical ECC/RSA system as a result of the extra computational complexity posed by post-quantum algorithms.

The ablation study is used to assess the effect of different elements of the quantum-safe cryptographic setup on its performance. It systematically eliminates or alters individual components, e.g. the Kyber encryption algorithm, Dilithium digital signature, and Quantum Key Distribution (QKD) to determine their impact on the throughput and latency of the system and its security. The paper discloses that Kyber and Dilithium are adding significant latency overhead and computational overhead and QKD is also adding more complexity but improving security. Any of these elements has been found to remove an element of the performance or security, and hence indicates the necessity and importance of each of these elements in ensuring the framework is robust to quantum threats whilst ensuring performance balancing.

5 Discussion

The main reason that makes performance Bottlenecks is the increased key sizes of Post-Quantum Cryptography (PQC) algorithms. Although, PQC guarantees quantum resistance, the larger key size particularly in such algorithms as Kyber (ML-KEM) and Dilithium leads to higher computational and memory costs. These considerations put pressure on older infrastructure like mobile wallet and hardware wallet which was originally built to accommodate smaller keys used by older encryption algorithms like RSA and ECC. This means that the introduction of PQC may cause latency to increase in processing the transactions since these devices would be required to engage in more resource-intensive activities to encrypt, decrypt and sign messages. This bottleneck may have an impact on system throughput, especially in a location with high volume of transactions and real time processing like in the case of national digital currencies and financial transactions.

Hardware Constraints Hardware Constraints are another difficulty of scaling quantum-secure cryptography systems to national infrastructures. Such devices as Hardware Security Modules (HSMs) and Point-of-Sale (PoS) terminals will need to be updated to handle the much larger keys and the more computationally expensive PQC algorithms. These are the hardware components that are needed to bring protection of transactions and key management across different financial systems. But the cost, time of deployment and integration of existing systems with the legacy systems are logistical issues that are raised with upgrading existing systems on a national level. Furthermore, it becomes even more complex because of the need to have special hardware accelerators or quantum-resistant modules to make the transition. There is also a threat of Standardization Gaps, the existing cryptographic solutions might not sufficiently embrace the availability of various algorithms required to be resilient in the future. To make sure that the failure of one point will not jeopardize the security of the system, the use of several algorithms of the backup e.g. the code-based schemes or the isogeny-based schemes is critical. The existence of this cryptographic variety is crucial to the realization of long-term stability and security in the era of quickly increasing quantum technologies.

6 Conclusion and Future Work

The study introduces a thorough discussion of a Quantum-Safe Cryptographic Framework that can be used to protect the national digital currencies (CBDCs) and economic infrastructure against the changing menace of quantum computing. The major conclusions of the research outline the necessity to combine Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) and ensure the security of vulnerable financial systems. It was demonstrated that with quantum attacks, the Kyber (ML-KEM) encryption and Dilithium digital signature algorithms could effectively resist attack, but may incur additional overhead (latency) and computation compared to the classical systems such as RSA/ECC. The framework is able to achieve security and bring performance trade-offs, where the transaction throughput (TPS) decreases by 15 % and latency rises by 20 % over the classical approaches.

The Quantum-Safe Framework was statistically 850 TPS and 54 ms latency whereas the classical system was 1000 TPS and 45 ms latency. Also, the quantum-safe system consumed more energy (1.5 J as compared to 1.2 J). In spite of all these problems, quantum-safe cryptography solutions are the key to the long-term security and stability of digital financial systems. Future studies ought to dwell on maximizing the operation of PQC algorithms, in terms of minimizing the latency and resource consumption without interfering with the security. Quantum money is a promising area of research into which fluctuations arise from physics-based trust models and AI-assisted solutions to filtering quantum-generated cyber threats can be developed to strengthen the resilience of the system. Also, it will be necessary to deal with hardware limitations and perform a smooth transition using such techniques as the Sandwich Approach, which will be required to make significant deployment.

References

- [1] Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2023). Quantum-Resistant Cryptographic Protocols: Securing Financial Transactions and Protecting Sensitive Business Data in the AI Era. *Gyanshauryam, International Scientific Refereed Research Journal*, 6(2), 152-184.
- [2] Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum cryptography and blockchain-based social media platforms as a dual approach to securing financial transactions in cbdc's and combating misinformation in us elections. *International Journal of Innovative Science and Research Technology*, 9(10), 2456-2165. <https://doi.org/10.38124/ijisrt/IJSRT24OCT1697>

- [3] Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. *Archives of Current Research International*, 25(2), 329-351. <https://doi.org/10.9734/acri/2025/v25i21090>
- [4] Al-Fatlawi, A. H., Albayati, O. M., Al-Magsoosi, A. A. H., Alyassri, L. S., & Abd Zaid, M. M. (2025, July). Quantum-Safe Algorithms with Future-Proofing Cryptographic Security in Evolving Financial Technology Infrastructures. In *2025 3rd International Conference on Cyber Resilience (ICCR)* (pp. 1-6). IEEE. <https://doi.org/10.1109/ICCR67387.2025.11292108>
- [5] Andriani, C., Bencivelli, L., Castellucci, A., De Santis, M., Marchetti, S., & Piantadina, G. (2024). The quantum challenge: implications and strategies for a secure financial system. *Bank of Italy Occasional Paper*, (877).
- [6] Bhatia, R. (2025). Finance as Critical Infrastructure: Embedding Post-Quantum Cryptography in Digital Finance Architectures. *Journal of Computer Science and Technology Studies*, 7(8), 1184-1194. <https://doi.org/10.32996/jcsts.2025.7.8.134>
- [7] Friday, O., Agbesi, J. S., Eni, F., Data, B., Hannah, D., & Njingou, J. (2024). Quantum-Resilient Infrastructure: Migrating US Financial Payment System to Post-Quantum Cryptography (PQC) Standards to Prevent 'Harvest Now, Decrypt Later' Attacks. *International Journal of Computer Applications Technology and Research*, 13(12), 198-213. <https://doi.org/10.7753/IJCATR1312.1016>
- [8] Jančiūtė, L. (2025). Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework. *International Cybersecurity Law Review*, 6(2), 145-154. <https://doi.org/10.1365/s43439-025-00135-7>
- [9] Maitireni, P., Ncube, V., Ndlovu, B., & Sibanda, T. (2025). Quantum Computing Cryptography: A Systematic Review of Innovations, Applications, Challenges, and Algorithms. *J. Inf. Syst. Informatics*, 7(4), 3668-3710. <https://doi.org/10.63158/journalisi.v7i4.1331>
- [10] Majumder, C., Choain, A. H. K., Nasir, M. A., & Sultana, N. (2026). Developing Hybrid Post-Quantum Encryption Frameworks for US Databases Integrating Financial, Governmental, and Critical Infrastructure Protections. *Journal of International Accounting and Financial Management*, 3(1), 1-18.
- [11] Mansur, M. (2025). A Quantum-Safe Interoperable and Decentralized Payment Infrastructure for the Post-Classical Era as a Strategic Framework for Secure Global Transactions. *European Scientific Journal*, 21(19), 17-45. <https://doi.org/10.19044/esj.2025.v21n19p17>
- [12] Nguyen, P. N. (2025). Quantum technology: a financial risk assessment. *Digital Finance*, 7(2), 133-172. <https://doi.org/10.1007/s42521-025-00127-6>
- [13] Nittala, E. P. (2024). Design and Evaluation of Quantum-Resilient Cryptographic Protocols for National Information Systems Security. *International Journal of Emerging Trends in Computer Science and Information Technology*, 5(2), 132-142. <https://doi.org/10.63282/3050-9246.IJETCSIT-V5I2P114>
- [14] Ogunmola, G. A. (2025). Securing the Digital Economy: Innovations in Cybersecurity, Ethical AI and the Future of Digital Payments and Cryptocurrency. *Abhigyan*, 43(4), 385-402.
- [15] Okika, N., Nwatuze, G. A., Olarinoye, H. S., Nwaka, A. A., Igba, E., & Dunee, R. (2025). Assessing the vulnerability of traditional and post-quantum cryptographic systems through penetration testing and strengthening cyber defenses with zero trust security in the era of quantum computing. *International Journal of Innovative Science and Research Technology*, 10(2), 1240-1258. <https://doi.org/10.5281/zenodo.14959440>
- [16] Olisa, A. O., Gbadebo, M. O., Mayeke, N. R., Oyewale, T., & Oladoyinbo, F. H. O. K. (2026). Quantum-Resistant Cryptographic Protocols for CBDC Interoperability: A Cross-Border Settlement Security Framework. *Engineering and Technology Journal*, 11(01), 8706-8719. <https://doi.org/10.47191/etj/v11i01.35>

- [17] Petrenko, K., Mashatan, A., & Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. *Journal of Information Security and Applications*, 46, 151-163. <https://doi.org/10.1016/j.jisa.2019.03.007>
- [18] Shafranova, K., Navolska, N., & Koldovskyi, A. (2024). Navigating the digital frontier: A comparative examination of Central Bank Digital Currency (CBDC) and the Quantum Financial System (QFS). *SocioEconomic Challenges*, 8(1), 90-111. [https://doi.org/10.61093/sec.8\(1\).90-111.2024](https://doi.org/10.61093/sec.8(1).90-111.2024)
- [19] Shevchuk, R., Adamyk, B., & Benson, V. (2025, September). Post-Quantum Security Enhancements for the TRISA Framework: A Technical Perspective. In *2025 15th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 553-558). IEEE.
- [20] Sugumar, R. (2024). Quantum-Resilient Cryptographic Protocols for the Next-Generation Financial Cybersecurity Landscape. *International Journal of Humanities and Information Technology*, 6(02), 89-105.

Authors Biography



Gulbanbegim Jamolova is an Associate Professor in the Department of Information Technology at the University of Economics and Pedagogy, Karshi, Uzbekistan. Her academic interests focus on information technology, digital education, and the integration of modern technologies in teaching and learning. She is actively involved in teaching, research, and curriculum development activities. Her work emphasizes innovative and technology-enhanced educational practices. Gulbanbegim Jamolova contributes to scholarly research and academic initiatives aimed at strengthening IT education and digital learning environments.



Maloxat Axmedova is a Lecturer in the Department of Information Technology at the University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. Her academic interests focus on information technology, digital learning, and modern teaching methodologies in higher education. She is actively involved in teaching, student mentoring, and academic development activities. Her work emphasizes the integration of innovative technologies to enhance learning outcomes. Maloxat Axmedova contributes to academic and research initiatives aimed at strengthening technology-oriented education.



Feruzaxon Odilova is affiliated with the Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Uzbekistan. Her academic interests focus on higher education, interdisciplinary studies, and the application of modern technologies in teaching and research. She is engaged in academic and scholarly activities that support innovative learning environments and educational development. Her work contributes to teaching, research collaboration, and institutional initiatives. Feruzaxon Odilova actively participates in efforts aimed at strengthening technology-driven education and academic advancement.



Feruza Urinboyeva is a Lecturer at Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. Her academic interests focus on education, pedagogy, and modern teaching methodologies in higher education. She is actively involved in teaching, student mentoring, and curriculum development activities. Her work emphasizes innovative and student-centered instructional approaches to enhance learning outcomes. Feruza Urinboyeva contributes to academic and research initiatives aimed at improving the quality of teacher education.



Sadokatxon Yuldasheva is a Lecturer in the Department of General and Comparative Linguistics at Andijan State Institute of Foreign Languages, Andijan, Uzbekistan. Her academic interests focus on linguistics, language studies, and modern approaches to language teaching and learning. She is actively involved in teaching, student mentoring, and academic development activities. Her work emphasizes innovative methodologies and comparative perspectives in language education. Sadokatxon Yuldasheva contributes to scholarly and educational initiatives aimed at enhancing the quality of foreign language education.



Polat Shokirov is affiliated with Tashkent State Technical University, Tashkent, Uzbekistan. His academic interests focus on technical education, engineering studies, and the application of modern technologies in higher education. He is involved in academic and scholarly activities that support innovation and practical learning approaches. His work contributes to teaching, research collaboration, and the development of technology-oriented educational practices. Polat Shokirov actively participates in initiatives aimed at advancing engineering education and academic development.



Kamolbek Masharipov is the Deputy Dean at Ma'mun University, Khiva, Uzbekistan. His academic and administrative work focuses on higher education management, academic coordination, and institutional development. He is actively involved in supporting teaching and learning activities, student affairs, and academic planning. His interests include improving educational quality through innovative and student-centered approaches. Kamolbek Masharipov contributes to institutional initiatives aimed at strengthening academic standards and educational effectiveness.