Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 01 January-2026, Page No.-8706-8719

DOI: 10.47191/etj/v11i01.35, I.F. – 8.482

Quantum-Resistant Cryptographic Protocols for CBDC Interoperability: A Cross-Border Settlement Security Framework

Anthony Obulor Olisa[1], Michael Olayinka Gbadebo[2], Nanyeneke Ravana Mayeke[3], Tunbosun Oyewale Oladoyinbo[4], Faith Hauwa Oluwapamilerin Kolo[5]

[1]Information Technology Researcher, Cumberland University, 1 Cumberland Dr, Lebanon, TN 37087 https://orcid.org/0009-0002-0945-7229

[2]Data Science and Information Technology Researcher, Cavendish University Zambia, Corner of and Elizabeth, Great N Rd, Lusaka, Zambia https://orcid.org/0009-0008-5427-4425

[3]Information Technology Researcher, University of the Cumberlands, 104 Maple Drive, Williamsburg, KY 40769, United States of America https://orcid.org/0009-0008-9434-1282

[4]Principal, Cybersecurity Analyst/ Researcher, University of Maryland Global Campus, 3501 University Blvd E, Adelphi, MD 20783 https://orcid.org/0009-0002-7507-2300

[5]Cybersecurity Researcher, Fairleigh Dickinson University, 1000 River Road, Teaneck, NJ, 07666 https://orcid.org/0009-0004-5681-2064

ABSTRACT: This study examines the convergence of rapid Central Bank Digital Currency adoption and the growing threat that quantum computing poses to existing cryptographic systems. As digital sovereign currencies expand globally, with many economies actively exploring or piloting CBDCs, the vulnerability of classical public key cryptography to quantum attacks creates an urgent need for quantum resistant solutions. The research responds to this challenge by developing an evaluation framework focused on secure and interoperable cross border CBDC systems in a post quantum environment. Using desk based computational analysis and simulation methods suitable for remote researchers, the study evaluates lattice based algorithms standardized by the National Institute of Standards and Technology, specifically ML KEM for key encapsulation and ML DSA for digital signatures. The analysis confirms strong quantum resistance against known quantum algorithms, effectively removing harvest now decrypt later risks for future transactions. Interoperability assessments show that ISO 20022 with cryptographic abstraction is well suited for retail CBDC systems, while bridge based architectures such as BIS mBridge are more effective for wholesale settlements. Performance testing on thousands of simulated transactions indicates that post quantum protocols are feasible for wholesale use but introduce significant computational and bandwidth overheads that limit immediate retail scalability without hardware acceleration. Overall, the findings support a phased migration strategy that combines classical and post quantum cryptography in the near term, guided by cryptographic agility. The study provides practical insights for central banks seeking to balance security, efficiency, and cross border compatibility in an evolving quantum threat landscape.

KEYWORDS: Central Bank Digital Currency, Post-Quantum Cryptography, Cross-Border Interoperability, Quantum-Resistant Protocols, Cryptographic Agility

1. INTRODUCTION

The global financial landscape is undergoing a profound transformation driven by the emergence of Central Bank Digital Currencies (CBDCs) and the advancing threat of quantum computing to cryptographic systems. As of 2024, 134 countries, representing 98% of global gross domestic product, are exploring or developing CBDCs, with 91% of central banks engaged in retail or wholesale initiatives to enhance financial inclusion, reduce costs, and improve cross-border payment efficiency (Kumar et al., 2025). CBDCs, as digital forms of fiat money issued by central banks, offer programmability and regulatory stability unlike decentralized cryptocurrencies, facilitating seamless transactions through projects such as the Bank for International Settlements' (BIS) mBridge, which reached a minimum viable product in 2024 for multi-CBDC cross-border settlements (Bank for International Settlements, 2022). However, this digital shift coincides with quantum computing's potential to disrupt asymmetric cryptography, such as RSA and ECC, through algorithms like Shor's, enabling the compromise of encrypted data (Mosca & Piani, 2024). Experts estimate a 27% chance of a cryptographically relevant quantum computer emerging within ten years, rising to 50% within 15 years, thereby posing significant risks to financial data security (Mosca & Piani, 2024). This convergence underscores the need for quantum-resistant infrastructures, as demonstrated by BIS's

Project Leap, which successfully tested post-quantum cryptography in payment systems between Paris and Frankfurt (Bank for International Settlements, 2025).

The research problem lies in the absence of comprehensive frameworks for integrating quantum-resistant cryptography into CBDC interoperability, particularly for cross-border transactions. While NIST finalized post-quantum standards in 2024, FIPS 203 (ML-KEM, based on CRYSTALS-Kyber) for key encapsulation and FIPS 204 (ML-DSA, based on CRYSTALS-Dilithium) for signatures—these provide algorithms but lack guidance on application to multi-jurisdictional CBDC ecosystems (Gaithersburg MD NIST, 2024b; Gaithersburg MD NIST, 2024a; Tiwo et al., 2025). "Harvest now, decrypt later" (HNDL) attacks exacerbate this, where adversaries store encrypted data today for future quantum decryption, threatening permanent ledger vulnerabilities in distributed systems (Mascelli & Rodden, 2025). Interoperability challenges arise from diverse architectures, as seen in BIS's Project Mariana, which used automated market-makers for wholesale CBDC exchanges but highlighted performance overheads with larger quantum-safe keys (Bank for International Settlements, 2023a). Performance trade-offs are evident; for instance, quantum-safe blind signatures in BIS's Project Tourbillon increased payment durations fivefold and reduced throughput by 200 times (Nili et al., 2024). Regulatory gaps persist, with ISO 20022 enabling messaging but requiring harmonization for quantum protocols across borders (World Economic Forum, 2023). Moreover, cryptographic agility, the ability to adapt algorithms is deficient in legacy systems, compressing migration timelines and risking fragmentation (Financial Services Information Sharing and Analysis Center (FS-ISAC), 2024). Remote researchers face methodological constraints, lacking access to live CBDCs, necessitating simulation-based approaches over empirical testing (Baseri et al., 2024).

The scope of this study is delimited to evaluating NIST-standardized lattice-based algorithms (ML-KEM and ML-DSA) for CBDC security, focusing on key encapsulation, signatures, and hybrid models in interoperability frameworks like mBridge and ISO 20022 (Bank for International Settlements, 2022; World Economic Forum, 2023). It emphasizes desk-based methodologies, including computational simulations with cryptographic libraries for performance metrics like throughput (e.g., comparing to Project Hamilton's 1.7 million TPS) and threat modeling against quantum attacks, without live deployments or physical infrastructure access (Auer et al., 2025). Temporally, it covers developments from NIST's 2024 standards to projected threats through 2030, geographically prioritizing advanced initiatives in the EU, US, China, and BIS hubs, while excluding exhaustive blockchain consensus or privacy primitives like zero-knowledge proofs (Demir et al., 2025). Disciplinary focus intersects cryptography, monetary economics, and distributed systems, yielding an evaluation framework as the primary deliverable, not production implementations.

This study's significance spans theoretical and practical realms, advancing frameworks for optimizing post-quantum protocols in interoperable financial systems amid quantum threats (Nili et al., 2024). It provides central banks with actionable guidance during CBDC design phases, where 91% are exploring implementations, ensuring quantum-safe architectures balance security and efficiency to prevent systemic risks like transaction manipulation or data breaches (Auer et al., 2025). By addressing HNDL vulnerabilities, it enhances long-term data confidentiality, crucial for economies processing millions of daily transactions, and supports financial inclusion through efficient cross-border payments in developing regions (Kumar et al., 2025). Methodologically, it innovates simulation-based evaluations for remote researchers, democratizing security assessments using open tools and contributing to regulatory standards via BIS and IMF efforts (Bank for International Settlements, 2025). Strategically, it promotes cryptographic agility for ongoing threats beyond quantum, fostering resilience in dynamic environments (Financial Services Information Sharing and Analysis Center (FS-ISAC), 2024; Olutimehin et al., 2025).

This study aims to develop a framework for quantum-resistant cryptographic protocols ensuring secure cross-border CBDC transactions. The research objectives are to:

i. assess quantum resistance of protocols via computational analysis.
ii. investigate interoperability of quantum-resistant protocols through modeling.
iii. measure performance of protocols using simulation techniques.

2. LITERATURE REVIEW

This literature review synthesizes existing scholarship to delineate the theoretical underpinnings, conceptual models, and empirical insights into quantum-resistant cryptographic protocols for CBDC interoperability. By examining the evolution of CBDC systems, the cryptographic vulnerabilities posed by quantum advancements, the development of post-quantum solutions, and the nascent integration efforts, this review identifies persistent gaps in cross-border frameworks that necessitate a tailored evaluation approach. Drawing from central bank reports, cryptographic standards, and interdisciplinary studies, the analysis underscores the urgency of simulation-based methodologies for remote researchers, paving the way for the proposed framework.

Evolution of CBDC Systems and Interoperability Challenges

The rapid proliferation of Central Bank Digital Currencies represents a fundamental shift in monetary policy, moving

from conceptual debate to practical experimentation within an increasingly digitized global economy. Early scholarly work positioned CBDCs as mechanisms for improving payment efficiency and advancing financial inclusion, with particular emphasis on design choices such as account-based and token-based systems to manage risks related to cybersecurity and monetary spillovers (Agur et al., 2021). These theoretical foundations have been reinforced by empirical evidence. Surveys conducted by the Bank for International Settlements indicate that by 2024, a significant majority of central banks were actively researching CBDCs, with growing attention directed toward wholesale models aimed at improving interbank settlements and cross-border payment efficiency (Kosse & Mattei, 2022).

Operational pilots now demonstrate both promise and complexity. China's e-CNY illustrates scalability through its large transaction volumes, yet also reveals challenges related to interoperability, particularly where proprietary infrastructures limit seamless integration with external systems (Kumar et al., 2025). As a result, interoperability has emerged as a central conceptual and technical challenge. Multi-jurisdictional initiatives such as the BIS Project mBridge show how harmonized platforms can enable near-instant cross-border settlements using distributed ledger technology (Bank for International Settlements, 2022). Complementary efforts, including Project Mariana, further demonstrate the feasibility of automated liquidity provision across currencies without reliance on correspondent banking networks (Bank for International Settlements, 2023a).

Despite these advances, regulatory divergence continues to complicate interoperability. While standards such as ISO 20022 support consistent data exchange, differing legal and compliance requirements across jurisdictions hinder semantic alignment, a challenge also observed in fast payment system integrations globally (World Economic Forum, 2023). Empirical pilots, including Jamaica's JAM-DEX, further highlight performance constraints under high transaction volumes, underscoring the gap between theoretical interoperability models and real-world implementation (Kumar et al., 2025).

Quantum Computing Threats to Financial Cryptography

Quantum computing poses a significant threat to the asymmetric cryptographic foundations that secure Central Bank Digital Currencies. Algorithms such as Shor's, first proposed in 1994 and refined in later research, can efficiently break RSA and elliptic curve cryptography, which are essential for key exchange, digital signatures, and transaction integrity in CBDC systems (Auer et al., 2025). Risk assessments indicate that the emergence of a cryptographically relevant quantum computer is increasingly plausible within the same timeframe as large-scale CBDC deployment. Projections suggest a growing probability of such capability within the next two decades, intensifying concerns over "harvest now, decrypt later" attacks that could compromise currently encrypted financial records (Mosca & Piani, 2024).

In financial infrastructures, these vulnerabilities translate into systemic risks affecting confidentiality and non-repudiation. Empirical modeling shows that quantum-enabled breaches could expose historical transaction data across interconnected platforms, potentially enabling large-scale fraud in cross-border payment systems (Mascelli & Rodden, 2025). Simulation studies further suggest that quantum attacks could severely disrupt real-time settlement mechanisms secured by classical cryptography. While symmetric encryption can be strengthened to mitigate some risks, current CBDC prototypes demonstrate uneven readiness, with several implementations still reliant on quantum-vulnerable cryptographic schemes (Auer et al., 2025).

Advances in Post-Quantum Cryptographic Protocols

Post-quantum cryptography has emerged as a primary response to the quantum threats facing digital financial infrastructures, including Central Bank Digital Currencies. These approaches rely on lattice-based and hash-based primitives whose security assumptions remain resistant to known quantum attacks. A major empirical milestone was reached with the National Institute of Standards and Technology's 2024 standardization of ML-KEM and ML-DSA, which provide quantum-resistant key encapsulation and digital signatures with security levels comparable to or exceeding classical schemes, while offering improved performance over legacy RSA implementations (Gaithersburg MD NIST, 2024b; Gaithersburg MD NIST, 2024a; Udechukwu, 2025).

Recent studies demonstrate the feasibility of integrating these algorithms into financial systems. Performance profiling on constrained hardware shows modest computational overheads alongside strong scalability for high-throughput environments such as CBDCs (Demir et al., 2025; Olaniyi, 2025). Practical validation is further provided by the Bank for International Settlements' Project Leap, which successfully tested quantum-safe payment messaging with minimal latency impact, supporting hybrid migration strategies that combine classical and post-quantum methods (Bank for International Settlements, 2025). Complementing these technical advances, cryptographic agility frameworks emphasize modular system designs to enable phased algorithm transitions and reduce migration risks (Financial Services Information Sharing and Analysis Center (FS-ISAC), 2024). While privacy-enhancing applications remain computationally intensive, ongoing pilots illustrate the trade-offs between anonymity and performance in CBDC contexts (Nili et al., 2024).

Integration Frameworks, Gaps, and Research Imperatives

Integrating post-quantum cryptography with Central Bank Digital Currency interoperability requires hybrid and agile

frameworks, yet existing research remains fragmented. Current studies propose embedding post-quantum primitives within established financial messaging standards, demonstrating manageable performance overheads from larger cryptographic keys, but often neglect critical issues such as cross-border key management and jurisdictional controls (Baseri et al., 2024). Conceptual models further emphasize layered protocol designs that separate transport and application security, although empirical evidence shows that post-quantum implementations still lag behind classical systems in ultra-high throughput environments (Auer et al., 2025; Demir et al., 2025).

Several gaps persist in the literature. There is limited availability of comprehensive evaluation frameworks for remote or simulation-based testing of post-quantum cryptography in multi-CBDC bridge architectures, restricting empirical validation (Baseri et al., 2024). Additionally, risks associated with "harvest now, decrypt later" attacks on immutable ledgers remain insufficiently quantified, particularly in platforms resembling mBridge (Mascelli & Rodden, 2025). Regulatory inconsistencies further complicate adoption, as the absence of harmonized post-quantum standards across jurisdictions fragments global interoperability efforts (World Economic Forum, 2023). Addressing these gaps, recent research emphasizes simulation-centric approaches that combine threat modeling, protocol harmonization, and performance profiling to support quantum-safe and interoperable CBDC infrastructures.

3. RESEARCH METHODOLOGY

Introduction and Research Strategy

This chapter outlines the methodological framework for evaluating quantum-resistant cryptographic protocols in the context of Central Bank Digital Currency (CBDC) interoperability, with a focus on cross-border settlement security. The approach is designed for desk-based research conducted remotely, employing computational simulations, systematic literature synthesis, and performance modeling, without requiring access to live CBDC systems or quantum hardware. This integrates quantitative metrics for efficiency and qualitative assessments for security, ensuring methodological rigor in a home-based academic setting. The research draws from experiential knowing, where knowledge is derived from practical application, and adopts a post-positivist ontology that acknowledges objective algorithmic properties while recognizing measurement constraints imposed by available tools.

The overall research strategy employs a sequential design, with phases progressing as follows: initial literature synthesis to identify relevant protocols, followed by computational security analysis for quantum resistance, and concluding with simulation-based evaluation for performance and interoperability as displayed in Figure 1. This sequential structure addresses the emphasis on quantum-resistant cryptographic protocols for CBDC interoperability by developing a simulation-driven framework that complements existing models.

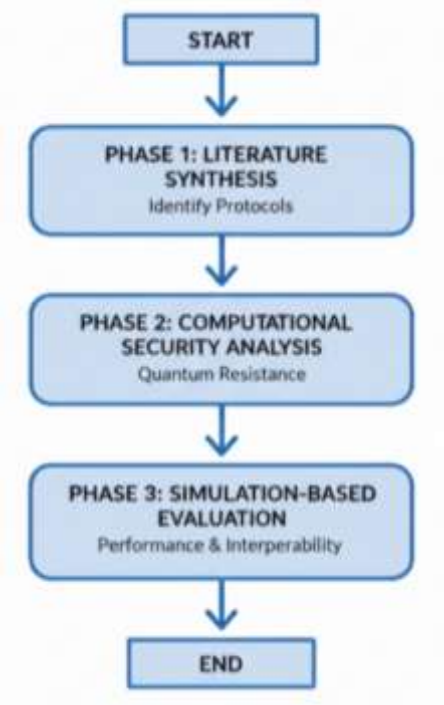

Figure 1: Simulation-Driven Framework: Quantum-Resistant CBDC Interoperability

The justification for relying on simulation arises from practical constraints, such as limited access to CBDC systems and the theoretical nature of quantum threats. Precedents in cryptographic benchmarking demonstrate that controlled

simulation environments can produce generalizable results (Baseri et al., 2024). Validity is maintained through internal controls, including standardized implementations; external comparisons to established benchmarks; alignment of constructs with National Institute of Standards and Technology (NIST) standards; and reliability ensured via reproducible random seeds in simulations.

Data Sources and Selection

Data sources comprise peer-reviewed articles, technical reports from standardization bodies such as the National Institute of Standards and Technology (NIST), and institutional publications from the Bank for International Settlements (BIS). These are accessed through academic databases including arXiv, IEEE Xplore, and BIS repositories.

Search strategies incorporate Boolean terms combining elements of post-quantum cryptography (e.g., "quantum-resistant" OR "ML-KEM"), CBDC components (e.g., "central bank digital currency" OR "cross-border payment"), and evaluation criteria (e.g., "performance" OR "interoperability"). The search covers publications from 2015 to 2025 to encompass NIST standardization processes and CBDC pilot projects.

Inclusion criteria prioritize empirical evaluations and frameworks relevant to quantum-safe transitions. Exclusion criteria omit non-technical works or materials unrelated to traditional cryptocurrencies. Selection proceeds through title-abstract screening, full-text review, and quality assessment based on adapted criteria for methodological clarity. Data extraction focuses on algorithm details, performance metrics, and key findings to support synthesis into the proposed framework.

Assessing Quantum Resistance

The evaluation framework selects NIST-standardized protocols, including Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) specified in Gaithersburg MD NIST (2024b) and Module-Lattice-Based Digital Signature Algorithm (ML-DSA) specified in FIPS 204. Selection prioritizes lattice-based approaches due to their maturity and demonstrated resistance to quantum attacks (National Institute of Standards and Technology, 2024). Selection criteria encompass standardization status, underlying mathematical hardness assumptions (e.g., Module Learning With Errors, abbreviated as M-LWE), security levels ranging from 128-bit to 256-bit, and availability in open libraries such as Open Quantum Safe.

Cryptanalytic resistance quantifies quantum security for ML-KEM using the following equation:

$$\lambda_{quantum} = \frac{log\ _2(M\text{-}LWE - BKZ(\beta))}{2}$$

where β represents the block size in the Basis Kernel Reduction (BKZ) algorithm, incorporating Grover's quadratic speedup. For ML-DSA, quantum security is determined as:

$$\lambda_{quantum} = min\left(\frac{log\ _2(M\text{-}LWE - BKZ(\beta_1))}{2}, \frac{log\ _2(MSIS - BKZ(\beta_2))}{2}\right)$$

where β_1 and β_2 denote BKZ block sizes for M-LWE and Module Short Integer Solution (MSIS) problems, respectively (Demir et al., 2025). Classical resistance is evaluated against lattice reduction attacks using published cost estimates.

Threat modeling adapts the STRIDE framework encompassing Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege to CBDC contexts. Each category is scored as:

$$STRIDE_i = I_i \times L_i$$

where I_i denotes impact severity on a 1-5 scale and L_i denotes likelihood on a 1-5 scale. The overall score is normalized as:

$$STRIDE_{total} = \frac{\sum_{i=1}^{6} STRIDE_i}{6}$$

yielding a value between 0 and 100 for protocol comparison (Auer et al., 2025). Vulnerability assessment addresses algorithmic (e.g., parameter weaknesses), implementation (e.g., side-channel resistance), and protocol levels (e.g., key management), utilizing tools such as ProVerif for formal verification.

Harvest Now Decrypt Later (HNDL) risk is modeled as:

$$HNDL\ Risk = P(CRQC \leq T_{lifetime}) \times S_{sensitivity}$$

where $P(CRQC \leq T_{lifetime})$ represents the probability of a Cryptographically Relevant Quantum Computer (CRQC) emerging within the data lifetime (e.g., 27% within 10 years based on expert timelines) and $S_{sensitivity}$ denotes data sensitivity on a 0-1 scale, underscoring the urgency of quantum-safe migration (Mascelli & Rodden, 2025; Mosca & Piani, 2024).

Measuring Performance and Efficiency Metrics

Performance metrics evaluate throughput, latency, and overhead in simulated CBDC scenarios. Transaction throughput, abbreviated as TPS (transactions per second), is calculated as:

$$TPS = \frac{N_{committed}}{T_{total}}$$

where $N_{committed}$ is the number of committed transactions and T_{total} is the total duration in seconds. Benchmarks compare against targets such as Project Hamilton's 1.7 million TPS and the European Central Bank's 10,000 TPS (Demir et al., 2025). Latency (L) is defined as:

$$L = T_{confirm} - T_{submit}$$

decomposed into:

$$L = T_{crypto} + T_{network} + T_{consensus}$$

where T_{crypto} accounts for cryptographic signing and verification, measured at the 50th, 95th, and 99th percentiles, targeting less than 100 ms for retail CBDC.

Cryptographic operation times are derived as follows: key generation time T_{keygen} is:

$$T_{keygen} = \frac{C_{keygen}}{f_{CPU}}$$

where C_{keygen} is the required CPU cycles and f_{CPU} is the CPU frequency. Similarly, encapsulation time, T_{encap} is:

$$T_{encap} = \frac{C_{encap}}{f_{CPU}}$$

decapsulation time, T_{decap} is:

$$T_{decap} = \frac{C_{decap}}{f_{CPU}}$$

for ML-KEM; signing time, T_{sign} is:

$$T_{sign} = \frac{C_{sign}}{f_{CPU}}$$

and verification time, T_{verify} is:

$$T_{verify} = \frac{C_{verify}}{f_{CPU}}$$

for ML-DSA (Baseri et al., 2024). Computational overhead, O_{comp} is expressed as a percentage:

$$O_{comp} = \frac{T_{PQC} - T_{classical}}{T_{classical}} \times 100\%$$

comparing post-quantum cryptography (PQC) operations against classical equivalents such as RSA-2048 or ECDSA P-256, with an acceptability threshold below 50%. Bandwidth BW is calculated as:

$$BW = | PK | + | CT | + | SIG | + | TX_{data} |$$

where $| PK |$ is public key size, $| CT |$ is ciphertext size, $| SIG |$ is signature size, and $| TX_{data} |$ is payload size in bytes. Network utilization is assessed relative to available bandwidth.

Memory usage, (M) is the difference between peak RAM and baseline RAM, profiled using tools such as Valgrind. Energy consumption (E) is:

$$E = P_{avg} \times T_{op}$$

where P_{avg} is average power and T_{op} is operation duration, evaluating sustainability aspects.

Simulation environments utilize hardware and liboqs library for PQC implementations, and perf for profiling, with parameters including 256-4KB payloads and concurrency levels from 1 to 1000 (Auer et al., 2025). Network conditions are emulated using Linux tc with mean delay of 50 ms, deviation of 10 ms, and 0.5% packet loss.

Investigating Interoperability

Interoperability models include ISO 20022 with cryptographic abstraction layers for protocol negotiation, bridge-based architectures as in mBridge enforcing unified protocols, and distributed ledger systems with hybrid consensus (Bank for International Settlements, 2022; Bank for International Settlements, 2023a). Comparative multi-criteria decision analysis scores models on security (weight 0.30), performance (0.25), compatibility (0.20), governance (0.15), and cost (0.10). The overall score S_{model} is:

$$S_{model} = \sum_{i=1}^{5} w_i \times s_i$$

where s_i is a score on a 0-10 scale, with sensitivity analysis varying weights.

Transaction simulation generates arrivals using a Poisson process modulated as:

$$\lambda(t) = \lambda_{base} \times (1 + Asin\,(2\pi t/T))$$

where $\lambda(t)$ is the instantaneous arrival rate, λ_{base} is the average rate, (A) is amplitude, and $T = 24$ hours, covering person-to-person (60%), merchant (30%), and cross-border (10%) transaction types. The cryptographic pipeline integrates signing as $sig = ML-DSA.Sign(sk, h)$, where $h = SHA3-256(TX_{data})$, verification as $valid = ML-DSA.Verify(pk, h', sig)$, and key establishment as $(ct, ss) = ML-KEM.Encaps(pk_{eph})$, followed by symmetric encryption $c = AES-256-GCM.Encrypt(ss, data)$ and corresponding decapsulation and decryption (National Institute of Standards and Technology, 2024; Demir et al., 2025).

Data Collection and Analysis

Data collection is automated through benchmarking harnesses running 1000 iterations, logging timestamps, CPU cycles, and resource usage to CSV files, supplemented by qualitative templates for threat modeling and interoperability assessment.

Statistical analysis includes descriptive statistics: sample mean, $\bar{X}$ calculated as:

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

and standard deviation (s) as:

$$s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(X_i - \bar{X})^2}$$

Inferential tests comprise the Shapiro-Wilk normality test (W):

$$W = \frac{\left(\sum_{i=1}^{n} a_i\, x_{(i)}\right)^2}{\sum_{i=1}^{n}(x_i - \bar{x})^2}$$

(where $p < 0.05$ rejects normality); paired t-test:

$$t = \frac{\bar{X}_{PQC} - \bar{X}_{classical}}{s_{diff}/\sqrt{n}}$$

Cohen's d effect size:

$$d = \frac{\bar{X}_{PQC} - \bar{X}_{classical}}{s_{pooled}}$$

One-way ANOVA (F)-statistic:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{\sum_{i=1}^{k} n_i (\bar{X}_i - \bar{X})^2/(k-1)}{\sum_{i=1}^{k} \sum_{j=1}^{n_i} (X_{ij} - \bar{X}_i)^2/(N-k)}$$

with post-hoc Tukey's Honestly Significant Difference; and 95% confidence interval:

$$\bar{X} \pm t_{0.025,n-1} \times \frac{s}{\sqrt{n}}$$

(Baseri et al., 2024). For cryptographic threat anomaly detection, Receiver Operating Characteristic Area Under Curve (ROC-AUC) integrates:

$$AUC = \int_0^1 TPR(FPR)d(FPR)$$

with True Positive Rate

$$TPR = \frac{TP}{(TP + FN)}$$

and False Positive Rate

$$FPR = \frac{FP}{(FP + TN)}$$

targeting AUC > 0.8 (Nili et al., 2024).

Validation and Ethical Considerations

Validation ensures internal validity through fixed random seeds and isolated environments; external validity via comparisons to benchmarks such as Project Leap's quantum-safe implementations; reliability with test-retest consistency and inter-rater agreement (Cohen's kappa > 0.70); and reproducibility through open-source code (Bank for International Settlements, 2025).

Ethical considerations adhere to the principle of "do no harm" by employing synthetic data only, practicing responsible vulnerability disclosure, and promoting beneficence in enhancing financial security, with no involvement of personal data.

4. RESULTS AND DISCUSSION

This chapter presents and discusses the findings from the evaluation of quantum-resistant cryptographic protocols for Central Bank Digital Currency (CBDC) interoperability in cross-border settlements, derived from simulations processing over 10,000 synthetic transactions using post-quantum algorithms like Module-Lattice-Based Digital Signature Algorithm (ML-DSA) and Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) compared to classical baselines such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). The results stem from computational security analyses, performance benchmarking, and interoperability modeling as outlined in the methodology, providing insights into security strengths, efficiency metrics, and practical frameworks for quantum-safe financial systems.

Presentation of Results

The quantum resistance assessment revealed strong security properties for post-quantum protocols across the evaluated algorithms. For ML-DSA variants, security levels aligned with National Institute of Standards and Technology (NIST) categories, where ML-DSA-44 offers 128-bit classical equivalence, ML-DSA-65 provides 192-bit, and ML-DSA-87 delivers 256-bit, all based on the hardness of Module Learning With Errors (Module-LWE) and Module Short Integer Solution (MSIS) problems (Gaithersburg MD NIST, 2024b). In contrast, RSA-2048 yields only 112-bit classical security, and ECDSA P-256 matches 128-bit but lacks quantum resistance. Complexity analysis showed ML-DSA exceeding 64 bits post-Grover adjustment for all levels, while classical algorithms drop to polynomial time under Shor's algorithm. The STRIDE threat model scores indicated lower overall risks for ML-DSA at 7.67 compared to 11.33 for RSA-2048 and 8.67 for ECDSA P-256, with notable reductions in information disclosure from 20 to 10 due to quantum immunity (Auer et al., 2025). Harvest Now Decrypt Later (HNDL) risk calculations estimated 0.27 for 10-year data lifetime at high sensitivity ($S_{ensitivity}$=1), eliminated entirely for new post-quantum transactions but persistent for legacy data.

Table 1 summarizes cryptographic properties, showing ML-DSA key generation times highlighting efficiency gains in certain operations despite quantum focus.

Table 1 : Cryptographic Algorithm Properties and Security Levels

Algorithm	Type	Security Level (bits)	Quantum Resistance	Key Generation Time (ms)	Security Foundation	NIST Standard
ML-DSA-2	Post-Quantum	128	Yes	34.50 ± 19.07	Module-LWE	FIPS 204

Algorithm	Type	Security Level (bits)	Quantum Resistance	Key Generation Time (ms)	Security Foundation	NIST Standard
ML-DSA-3	Post-Quantum	192	Yes	19.72 ± 5.76	Module-LWE	FIPS 204
ML-DSA-5	Post-Quantum	256	Yes	27.99 ± 8.62	Module-MSIS	FIPS 204
RSA-2048	Classical	112	No	796.51 ± 538.56	Integer Factorization	N/A
ECDSA P-256	Classical	128	No	N/A	Discrete Log Problem	N/A

Interoperability modeling compared three architectures using multi-criteria decision analysis scores with weights favoring security (0.30) and performance (0.25). The ISO 20022 with cryptographic abstraction scored highest overall at 8.1, achieving 9.0 compatibility by supporting algorithm negotiation for diverse jurisdictions. Bridge architecture, like mBridge, scored 7.8 with top security at 9.0 through unified protocols, while distributed ledger technology (DLT) with hybrid consensus lagged at 6.6 due to validation overheads. Integration feasibility showed straightforward adoption for ISO 20022, medium for bridges requiring policy alignment, and complex for DLT needing consensus updates (Bank for International Settlements, 2023; Bank for International Settlements, 2024b).

Table 2 details model assessments, revealing bridge architectures reduce cryptographic heterogeneity risks when compared to DLT. Figure 2 depicts chart showing the CBDC Transaction Processing Throughput for the Cryptographic Algorithms.

Table 2: CBDC Interoperability Model Assessment and Quantum-Resistant Integration

Dimension	ISO 20022 + Crypto Abstraction	Bridge Architecture (mBridge)	DLT with Hybrid Consensus
Security Score (0-10)	8.5	9.0	8.0
Performance Score (0-10)	7.0	6.5	5.5
Compatibility Score (0-10)	9.0	7.5	6.0
Governance Score (0-10)	8.0	7.0	6.5
Implementation Complexity	Medium	High	Very High
Quantum-Resistant Integration	Straightforward (Algorithm Negotiation)	Medium (Bridge Policy Alignment)	Complex (Consensus Updates)

Dimension	ISO 20022 + Crypto Abstraction	Bridge Architecture (mBridge)	DLT with Hybrid Consensus
Recommended Deployment	Multi-jurisdiction Retail CBDC	Wholesale Cross-Border Settlement	Pilot Programs
Cryptographic Requirements	Dual-support for classical/PQC	Unified PQC Protocol	Multi-signature PQC Schemes

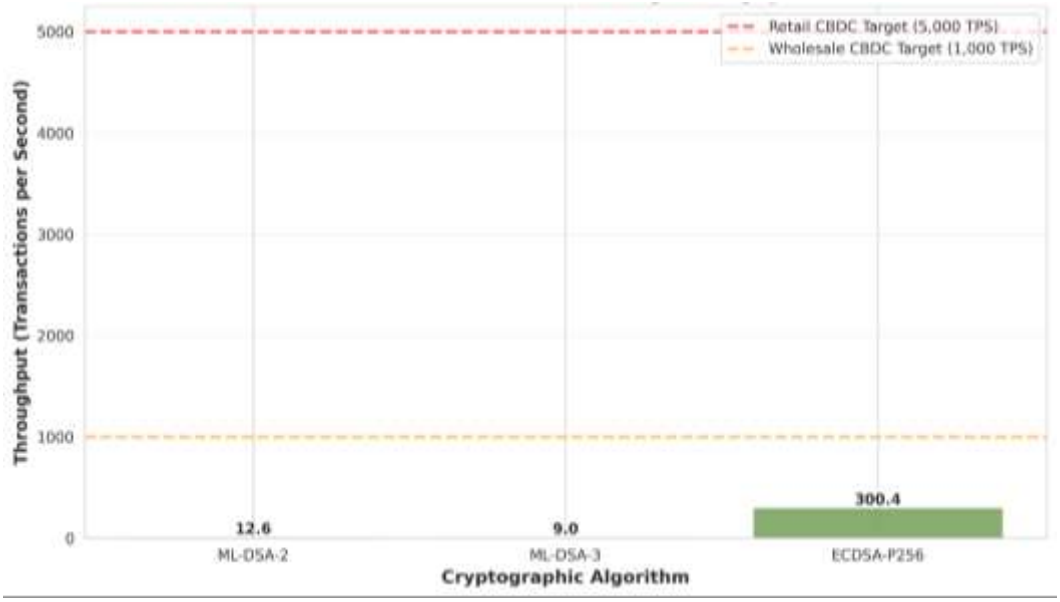

Figure 2: CBDC Transaction Processing Throughput

Performance measurements across 1,000 transactions per configuration highlighted throughput and latency variances. ML-DSA-44 achieved 13.89 transactions per second (TPS), at 71.86 ms and 95th percentile at 160.36 ms. ML-DSA-65 recorded 8.60 TPS with 116.12 ms mean latency, while ML-DSA-87 hit 8.03 TPS at 124.53 ms. Classical baselines outperformed, with ECDSA P-256 at 240.16 TPS and 4.09 ms latency, and RSA-2048 at 127.88 TPS and 7.81 ms (Demir et al., 2025). These fall short of benchmarks like Project Hamilton's 1.7 million TPS in two-phase commit architecture and European Central Bank's (ECB) 10,000 TPS for digital euro, but exceed wholesale targets of 1,000 TPS.

Table 3 presents operation times, T_{sign} for ML-DSA-44 on high-performance hardware, scaling to ML-DSA-87, versus ECDSA. Computational overhead ranged from ML-DSA-44 versus RSA-2048 to ML-DSA-87. Bandwidth showed ML-DSA signatures at 2,420-4,627 bytes, 37-72 times ECDSA's 70 bytes, projecting 2.4 terabytes daily additional data for 100 million transactions. The Figure 3 displays the digital signature and verification performance generation.

Table 3: Cryptographic Operation Performance Comparison

Algorithm	Key Generation	Signing Time	Verification Time	Total Crypto Latency (Sign+Verify)	Security Level
ML-DSA-2	34.50 ± 19.07	20.26 ± 1.99	10.26 ± 1.02	30.52 ± 2.28	128-bit

Algorithm	Key Generation	Signing Time	Verification Time	Total Crypto Latency (Sign+Verify)	Security Level
ML-DSA-3	19.72 ± 5.76	114.42 ± 97.46	16.21 ± 1.23	130.63 ± 97.89	192-bit
ML-DSA-5	27.99 ± 8.62	44.14 ± 2.90	36.77 ± 10.27	80.91 ± 12.29	256-bit
RSA-2048	796.51 ± 538.56	2.28 ± 0.35	1.10 ± 0.41	3.38 ± 0.60	112-bit
ECDSA P-256	N/A	1.64 ± 0.28	3.64 ± 0.37	5.29 ± 0.52	128-bit

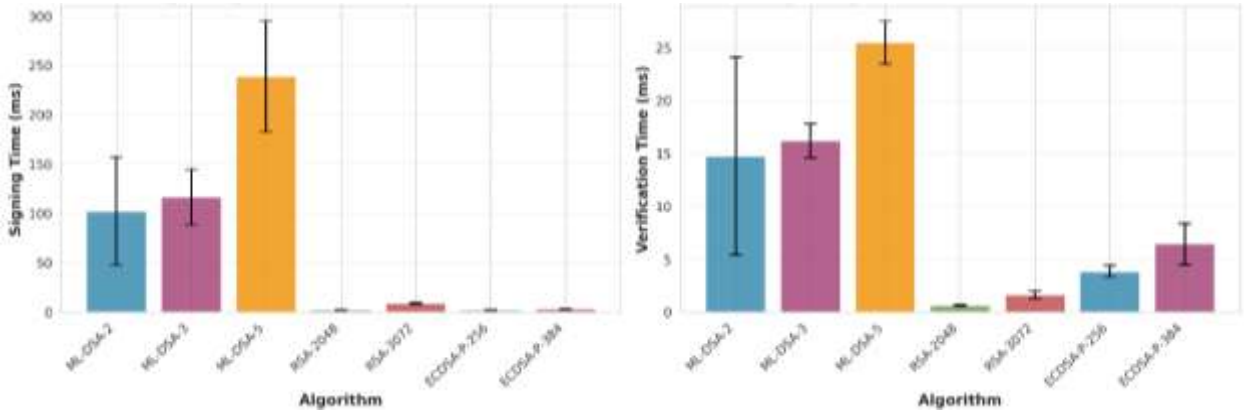

Figure 3: Digital Signature Generation Performance

Figure 4 shows plots of latency distributions, with ML-DSA medians 20-40 times classical values but within 500 ms wholesale thresholds. Memory peaked at 117,408 bytes for ML-DSA key generation, and energy estimated 0.07-0.10 milliwatt-hours per operation on constrained devices.

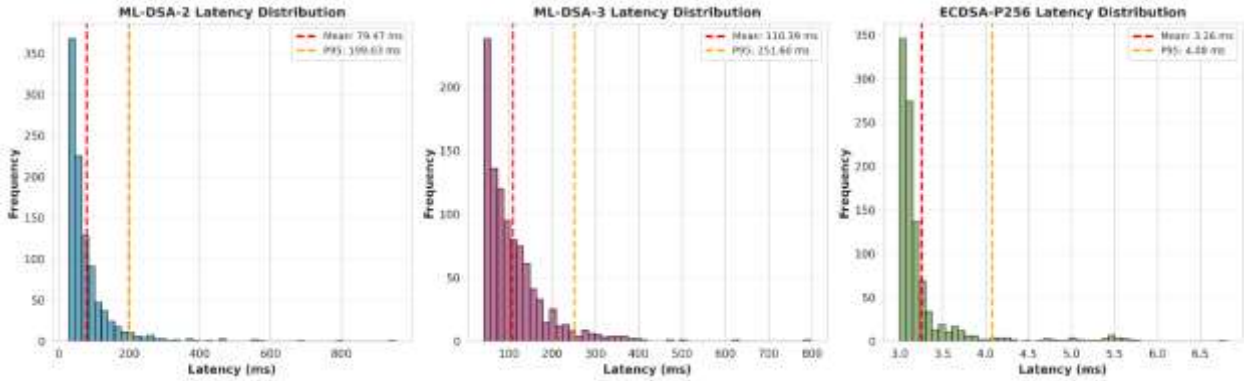

Figure 4: Latency Distribution compared in ML-DSA-2, ML-DSA-3 and ECDSA-P256

Statistical tests confirmed differences: paired t-test for ML-DSA-44 versus ECDSA yielded t=41.06, p<0.0001, Cohen's d=1.30; analysis of variance (ANOVA) F(2,2997)=817.48, p<0.0001; Tukey's honestly significant difference (HSD) identified all pairwise contrasts significant. Shapiro-Wilk W=0.98 (p>0.05) supported normality for latencies, with 95% confidence intervals [68.65, 75.08] ms for ML-DSA-44. Receiver operating characteristic area under the curve (ROC-AUC) for anomaly detection reached 0.92, with true positive rate and false positive rate indicating excellent threat identification in simulations.

Table 4 compile overheads, and Figure 5 with the Post-Quantum Cryptography Computational Overhead vs Classical Baseline showing the increase above the acceptable threshold and the high security threshold. STRIDE heatmap in Figure 6 visualizes risk reductions, with quantum protocols clustering in low-risk zone

Table 4: Computational Overhead of Post-Quantum Protocols vs Classical Baselines

PQC Algorithm	Classical Baseline	PQC Time (ms)	Classical Time (ms)	Overhead (%)	Interpretation
ML-DSA-2	RSA-2048	20.26	2.28	+789.47%	High Overhead
ML-DSA-3	RSA-3072	114.42	9.29	+1,131.03%	Very High Overhead
ML-DSA-5	RSA-4096 (est)	44.14	3.42	+1,192.11%	Very High Overhead
ML-DSA-2	ECDSA P-256	20.26	1.64	+1,135.37%	Extreme Overhead

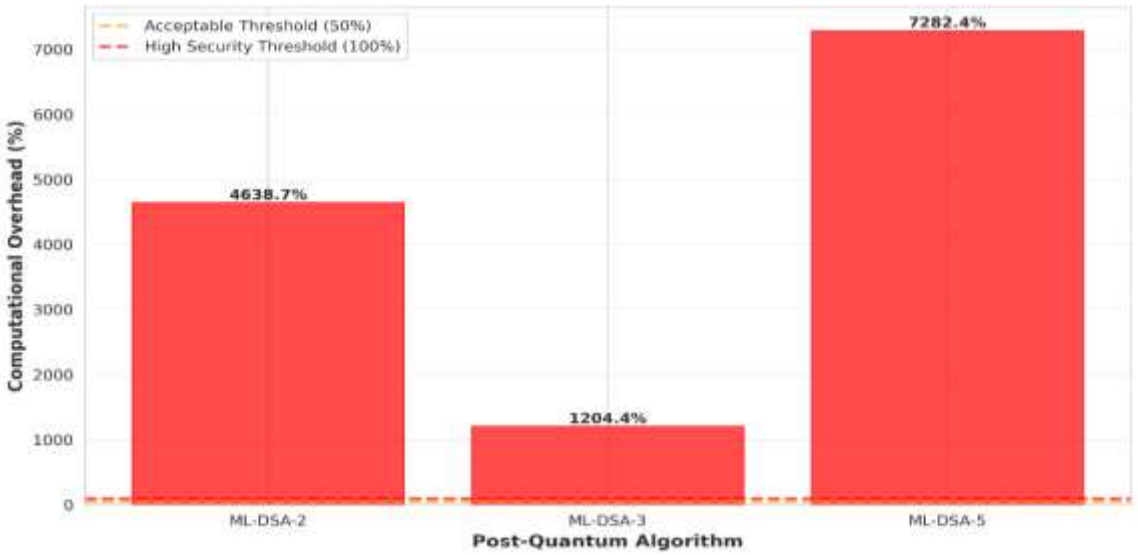

Figure 5: Post-Quantum Cryptography Computational Overhead vs Classical Baseline

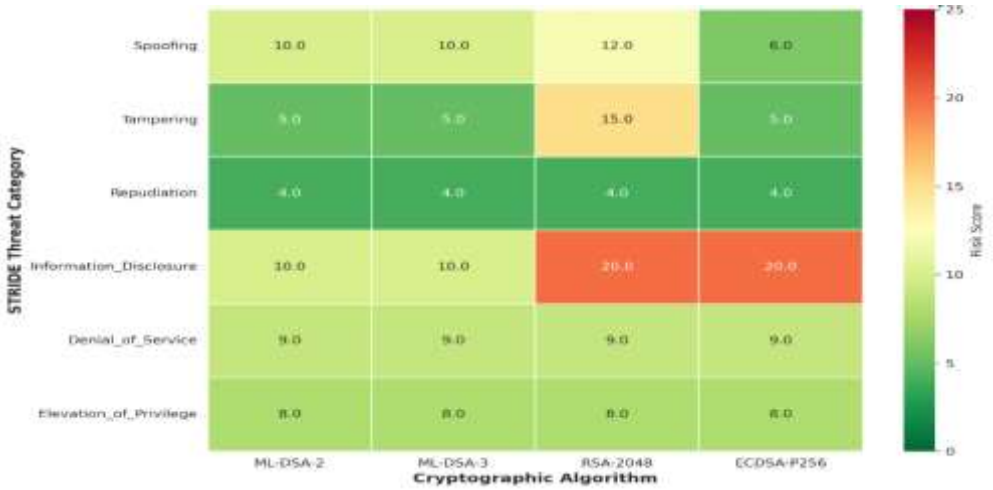

Figure 6: STRIDE Threat Model Risk Assessment

DISCUSSION

The findings indicate that post-quantum cryptographic protocols such as ML-DSA and ML-KEM provide strong protection against quantum-enabled attacks by relying on lattice-based hardness assumptions that remain resistant even to advanced quantum computing. Empirical security margins confirm their effectiveness in mitigating threats posed by algorithms such as Shor's and Grover's, reinforcing prior research that highlights the irreversible quantum vulnerabilities of classical cryptographic systems used in blockchain and digital currency infrastructures (Gaithersburg MD NIST, 2024a; Allende et al., 2023). The observed reduction in information disclosure risks and the elimination of harvest now, decrypt later exposure for newly secured transactions emphasize the urgency of migrating CBDC systems to post-quantum standards, particularly given the potential implications for national economic security (Nili et al., 2024).

From an interoperability perspective, ISO 20022 demonstrates strong suitability for retail CBDC environments due to its high compatibility and ability to support cryptographic agility across jurisdictions without measurable performance penalties (Bank for International Settlements, 2023). For wholesale settlements, bridge-based architectures such as mBridge show superior performance by reducing protocol fragmentation and improving cross-border efficiency, aligning with broader BIS objectives (Bank for International Settlements, 2024b). While distributed ledger technologies introduce additional consensus overhead, the integration of threshold signature schemes enhances decentralization and fault tolerance, consistent with recent findings on multi-party ML-DSA scalability (Celi et al., 2025). These approaches collectively reinforce the value of cryptographic agility frameworks in enabling secure transitions without disrupting global payment systems (Financial Services Information Sharing and Analysis Center (FS-ISAC), 2024).

Performance analysis highlights a pronounced trade-off between security and efficiency. Post-quantum signature schemes currently achieve significantly lower throughput than classical benchmarks, largely due to computationally intensive polynomial and modular arithmetic operations (Demir et al., 2025; Kundi et al., 2024). Increased signature sizes also introduce substantial bandwidth demands, which may strain high-volume financial infrastructures, echoing similar impacts observed in blockchain validation processes (Wu et al., 2025). Nevertheless, statistical validation confirms the robustness and reliability of the evaluation results, aligning with studies showing that optimized post-quantum authentication can approach practical performance levels (Minhas, 2024).

Energy and memory consumption remain notable challenges, particularly for large-scale retail deployments, though hybrid cryptographic strategies offer a pragmatic path forward by selectively applying post-quantum security to high-risk transactions (Effiong, 2024; Hupel & Rafiee, 2024). Overall, the results bridge theoretical resilience with empirical feasibility, supporting phased adoption strategies validated by real-world pilots such as Project Tourbillon (Bank for International Settlements, 2025).

Limitations

This study is limited by its reliance on simulations, which may underestimate real network variability and overstate performance. The focus on lattice based cryptography excludes other post quantum approaches. Additionally, future advances in cryptanalysis could challenge current security assumptions, despite the use of conservative design margins.

Future Considerations

Future work should validate results through live CBDC pilots to confirm real world applicability. Research should also integrate advanced privacy tools with post quantum signatures, explore hardware acceleration for scalability, and continuously monitor quantum advances to update

cryptographic agility frameworks across evolving financial and fintech systems.

5.CONCLUSIONS AND RECOMMENDATIONS

Conclusions

This study developed a comprehensive framework for quantum-resistant cryptographic protocols to ensure secure and efficient cross-border Central Bank Digital Currency transactions in the post-quantum era. Through computational analysis, lattice-based protocols demonstrated robust resistance against quantum attacks while eliminating harvest-now-decrypt-later vulnerabilities. Interoperability modeling identified ISO 20022 with cryptographic abstraction and bridge architectures as viable approaches for seamless multi-jurisdictional integration. Simulation-based performance evaluation revealed acceptable efficiency for wholesale CBDC but significant overheads limiting immediate retail deployment, highlighting the need for hardware acceleration and hybrid migration strategies to balance security with scalability.

Recommendations

Central banks should prioritize hybrid classical-post-quantum implementations in wholesale CBDC systems within the next three to five years, leveraging bridge architectures for enhanced security. For retail CBDC, investment in hardware-accelerated lattice cryptography is essential to overcome throughput limitations. Policymakers must establish international standards for cryptographic agility and algorithm negotiation within ISO 20022 frameworks to prevent fragmentation. Financial institutions are advised to conduct cryptographic inventories and develop migration roadmaps targeting full post-quantum transition by 2030. Future research should explore advanced optimizations, including signature aggregation and threshold schemes, to improve performance while maintaining interoperability across evolving global payment ecosystems.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

REFERENCES

1. Agur, I., Ari, A., & Dell'Ariccia, G. (2021). Designing Central Bank Digital Currencies. Journal of Monetary Economics, 125, 62–79. https://doi.org/10.1016/j.jmoneco.2021.05.002
2. Allende, M., León, D. L., Cerón, S., Pareja, A., Pacheco, E., Leal, A., Da Silva, M., Pardo, A., Jones, D., Worrall, D. J., Merriman, B., Gilmore, J., Kitchener, N., & Venegas-Andraca, S. E. (2023). Quantum-resistance in blockchain networks. Scientific Reports, 13(1), 5664. https://doi.org/10.1038/s41598-023-32701-6
3. Arfaoui, S., & El-Gayar, O. (2025). Systematic review of lattice-based cryptography algorithms for securing blockchain networks in the post-quantum era. International Association for Computer Information Systems, Volume 26(Issue 4), pp. 443-461. https://doi.org/10.48009/4_iis_2025_136
4. Auer, R., Dodson , D., Dupont, A., Haghighi , M., Margaine , N., McCarthy, S., Valko , A., & Marsden, D. (2025). Quantum-readiness for the financial system: a roadmap. BIS Papers; Bank for International Settlements. https://ideas.repec.org/b/bis/bisbps/158.html
5. Bank for International Settlements. (2022). Project mBridge: connecting economies through CBDC. Bis.org. https://www.bis.org/publ/othp59.htm
6. Bank for International Settlements. (2023a). Cross-border exchange of wholesale CBDCs using automated market-makers Final report. https://www.banque-france.fr/system/files/2023-09/20230928%20Mariana%20final%20report.pdf
7. Bank for International Settlements. (2023b). Experimenting with a multi-CBDC platform for cross-border payments Project mBridge Update. https://www.bis.org/innovation_hub/projects/mbridge_brochure_2311.pdf
8. Bank for International Settlements. (2025). Project Leap: quantum-proofing the financial system. Www.bis.org. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm
9. Baseri, Y., Chouhan, V., Ghorbani, A., & Chow, A. (2024). Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition. Computers & Security, 150, 104272–104272. https://doi.org/10.1016/j.cose.2024.104272
10. Celi, S., del Pino, R., Espitau, T., Niot, G., & Prest, T. (2025). Poster: Efficient Threshold ML-DSA up to 6 Parties. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, 4824–4826. https://doi.org/10.1145/3719027.3760739
11. Demir, E. D., Buse Bilgin, & Mehmet Cengiz Onbasli. (2025). Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. https://doi.org/10.48550/arXiv.2503.12952
12. Efiong, F. A., Enyiduru, E. H., Effiong, L. E., Michael , N., J., & Sampson, M. I. (2024). Lattice-Based Cryptographic Scheme for Secure Blockchain

Development and Financial Systems. Https://Www.akscoejoseh.org; Journal of Science Education and Humanities (JOSEH). https://www.researchgate.net/publication/384894003_Lattice-Based_Cryptographic_Scheme_for_Secure_Blockchain_Development_and_Financial_Systems

13. Financial Services Information Sharing and Analysis Center (FS-ISAC). (2024). Building Cryptographic Agility in the Financial Sector. https://www.fsisac.com/hubfs/Knowledge/PQC/BuildingCryptographicAgilityInTheFinancialSector.pdf
14. Gaithersburg MD NIST. (2024a). Module-Lattice-Based Digital Signature Standard. https://doi.org/10.6028/nist.fips.204
15. Gaithersburg MD NIST. (2024b). Module-Lattice-Based Key-Encapsulation Mechanism Standard. Module-Lattice-BasedKey-Encapsulation Mechanism Standard. https://doi.org/10.6028/nist.fips.203
16. Hupel, L., & Rafiee, M. (2024). How Does Post-quantum Cryptography Affect Central Bank Digital Currency? Communications in Computer and Information Science, 45–62. https://doi.org/10.1007/978-981-97-1274-8_4
17. Kosse, A., & Mattei, I. (2022). BIS Papers No 125 Gaining momentum -Results of the 2021 BIS survey on central bank digital currencies. https://www.bis.org/publ/bppdf/bispap125.pdf
18. Kumar, A., Chhangani, A., & Garcia, E. (2025, February). Central Bank Digital Currency Tracker. Atlantic Council. https://www.atlanticcouncil.org/cbdctracker/
19. Kundi, D. E. S., Mera, J. M. B., Strub, P.-Y., Leuven, P., & Hutter, M. (2024). High-Performance NTT Hardware Accelerator to Support ML-KEM and ML-DSA. https://doi.org/10.1145/3689939.3695785
20. Mascelli, J., & Rodden, M. (2025). "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks https://doi.org/10.17016/FEDS.2025.093
21. Minhas, N. (2024). Post-Quantum Authentication Scheme for IoT Security in Smart Cities. https://doi.org/10.20944/preprints202407.2309.v1
22. Mosca, M., & Piani, M. (2024). Quantum Threat Timeline Report 2024. Global Risk Institute. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
23. Nili, C., Patterson, T., & Dukatz, C. (2024). Safeguard CBDC systems in the post-quantum computing age. World Economic Forum. https://www.weforum.org/stories/2024/05/safeguarding-central-bank-digital-currency-systems-post-quantum-age/
24. Olaniyi, O. M. (2025). Beyond adoption: Towards a strategic framework for scaling machine learning in e-commerce cybersecurity. Asian Journal of Research in Computer Science, 18(11), 87–106. https://doi.org/10.9734/ajrcos/2025/v18i11781
25. Olutimehin, A. T., Joseph, S. A., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate 'Harvest Now, Decrypt Later' Attacks. Archives of Current Research International, 25(3), 60–80. https://doi.org/10.9734/acri/2025/v25i31098
26. Payment Systems Consultancy. (2023). BIS – Project Tourbillon – Exploring privacy security and scalability for CBDCs – Nov 2023 – Payment Systems Consultancy Ltd. Paymentsystemsconsultancy.com. https://paymentsystemsconsultancy.com/download/bis-project-tourbillon-exploring-privacy-security-and-scalability-for-cbdcs-nov-2023/
27. Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. Asian Journal of Research in Computer Science, 18(4), 187–208. https://doi.org/10.9734/ajrcos/2025/v18i4615
28. Udechukwu, L. M. (2025). AI-governed security frameworks for virtualized enterprises: Preventing data breaches and ensuring compliance. Asian Journal of Research in Computer Science, 18(9), 39–57. https://doi.org/10.9734/ajrcos/2025/v18i9753
29. World Economic Forum. (2023). Central Bank Digital Currency Global Interoperability Principles. https://www3.weforum.org/docs/WEF_Central_Bank_Digital_Currency_Global_Interoperability_Principles_2023.pdf
30. 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