Resilience Analysis of Clearing and Settlement Systems Under Quantum-Enabled Cybersecurity Threats

Deni Teminyan
ENKA Schools

***Abstract*—Clearing and settlement systems are the hidden core of global finance. They make sure trades are finalized, payments are delivered, and counter-party risk is controlled between large institutions. As quantum computing develops, these systems face new cybersecurity risks, especially against the cryptography that protects messages, keys, and digital signatures. In this project, I develop a resilience analysis framework for clearing and settlement systems under quantum-enabled attack scenarios. The framework maps technical components, operational dependencies, and cryptographic touchpoints, and then studies how quantum attacks—such as harvest-now-decrypt-later strategies, breaking public-key schemes, or tampering with validation messages—could spread through the system. Using ideas from financial market infrastructure regulation and quantum security research, I identify pressure points where cryptographic failure could trigger liquidity shocks or settlement delays. Based on these findings, I outline a layered defence model that combines post-quantum cryptography, cryptographic agility, real-time monitoring, and strong governance and incident-response planning. The main goal is to keep transaction finality, data integrity, and market stability even when quantum-capable attackers appear. The project offers practical guidance for central banks, clearing houses, and payment processors preparing for a quantum-resilient financial ecosystem.**

Clearing and settlement systems are critical parts of financial market infrastructure. They handle trade matching, the transfer of cash and securities, and the control of liquidity and counterparty risk (Saguato, 2025). Because many institutions and markets depend on them, any disruption can quickly affect confidence and stability across the whole financial system (Xu, 2025).

At the same time, the threat landscape is changing. Quantum computing can solve certain mathematical problems much faster than classical computers, creating serious risks for widely used cryptographic algorithms (Columbus Chinnappan et al., 2025). Shor's algorithm threatens public-key schemes such as RSA and ECC, while Grover's algorithm can weaken symmetric encryption. For clearing and settlement systems, this means a higher chance of data interception, mes-

Digital Object Identifier 10.62802/fzgkpv73

Date of publication 10 10 2025; date of current version 16 11 2025

sage forgery, and unauthorized transaction execution (Uzoma, Enyejo, & Motilola Olola, 2025).

Because clearing and settlement processes are time-critical and highly interconnected, a quantum-enabled attack could block payment messages, break digital signatures, or delay settlement cycles, leading to liquidity problems and contagion across markets (Elmisery, Sertovic, Zayin, & Watson, 2025). Regulators and policymakers now talk more about cryptographic agility and post-quantum readiness in financial infrastructures (Zafar, 2025). This project responds to that need by proposing a resilience analysis framework and a layered defence model for clearing and settlement systems in the quantum era.

Methods

System Mapping and Dependency Analysis

First, the study builds a conceptual map of a generic clearing and settlement system:

- Core functions (clearing, netting, settlement, messaging),
- Supporting services (identity, key management, time-stamping),
- External dependencies (payment systems, CSDs, central banks, communication networks).

Each component is linked to its main cryptographic mechanisms (e.g., TLS channels, digital signatures, hardware security modules). This mapping helps identify where cryptographic failure would have the greatest operational impact.

Quantum Threat Scenario Definition

Next, a set of quantum-enabled threat scenarios is defined using current cybersecurity and quantum research (Bishnoi & Pomeroy, 2025; Elmisery et al., 2025):

- Harvest-now-decrypt-later: attackers store encrypted traffic today and decrypt it later with a large quantum computer.
- Break of public-key infrastructure (PKI): compromise of certificates, signatures, and authentication flows.
- Manipulation of validation messages: forging or blocking messages that confirm trades, margin calls, or settlement status.

For each scenario, the analysis asks: which parts of the system are affected, what kind of failures could occur, and how these failures might propagate.

Resilience and Defence Model Design

Finally, the study designs a layered defence architecture based on:

- Post-quantum cryptographic schemes and cryptographic agility,
- Real-time anomaly detection and AI-driven monitoring (Saeed, 2025),
- Governance measures such as clear incident-response plans and regulatory reporting.

This model is aligned with existing guidance on critical financial infrastructures and quantum-safe transition planning (Zafar, 2025).

Results

Identified Vulnerabilities and Pressure Points

The resilience analysis highlights several key pressure points:

- Communication channels between CCPs, CSDs, and payment systems that rely on vulnerable public-key encryption.
- Digital signatures used for transaction validation and settlement instructions, which could be forged if current algorithms are broken.
- Time-critical processes, such as end-of-day settlement cycles, where delays caused by attacks could create liquidity shortfalls.

In quantum-enabled scenarios, harvest-now-decrypt-later attacks are especially dangerous because they allow silent data collection today and visible damage later, even after systems “upgrade” to post-quantum schemes.

Resilience Requirements

The analysis shows that resilience in the quantum era must:

- Treat quantum risks and traditional cyber risks together, not in isolation.
- Include cryptographic agility, so algorithms and keys can be replaced quickly without redesigning the whole system (Bishnoi & Pomeroy, 2025).
- Use real-time monitoring to detect unusual delays, message patterns, or signature failures that could signal an ongoing attack.

Without these features, clearing and settlement systems may struggle to maintain transaction finality and market confidence during a quantum-driven crisis.

Discussion

Implications for Financial Market Infrastructures

The findings suggest that central banks, clearing houses, and payment processors should start planning for quantum-resilient operations now. This includes:

- Inventorying where current cryptography is used,
- Prioritizing upgrades for the most critical communication paths,
- Testing fall-back procedures for delayed or failed settlements.

The work also aligns with broader research on multi-cloud and distributed ledger integration for secure, high-integrity financial data flows (Uzoma et al., 2025).

Governance, Policy, and International Coordination

Technical fixes alone are not enough. Effective resilience requires:

- Clear governance frameworks that define roles, responsibilities, and escalation paths,
- Coordination between regulators, FMIs, and large market participants to avoid fragmented or inconsistent transitions,
- Cross-border cooperation, since many clearing and settlement systems serve multiple jurisdictions (Saguato, 2025; Zafar, 2025).

These elements help ensure that quantum-safe upgrades do not themselves become a source of instability.

Conclusion

This project develops a resilience analysis framework for clearing and settlement systems facing quantum-enabled cybersecurity threats. By mapping system components, defining realistic attack scenarios, and identifying pressure points, it shows how quantum risks can interact with existing operational dependencies and systemic vulnerabilities.

The proposed layered defence architecture—combining post-quantum cryptography, cryptographic agility, real-time monitoring, and strong governance—aims to protect transaction finality, data integrity, and market stability in a future where quantum-capable attackers may be present. Overall, the study contributes to the growing discussion on quantum-safe finance and offers concrete starting points for designing a quantum-resilient financial ecosystem.

REFERENCES

1. Bishnoi, R. & Pomeroy, J. (2025). AI and quantum computing: Transforming information security protocols for the future. ResearchGate.
2. Columbus Chinnappan, C. & Thanaraj Krishnan, P. & Elamaran, E. & Arul, R. & Sunil Kumar, T. (2025). Quantum Computing: Foundations, Architecture and Applications. Engineering Reports. 7(8). e70337.
3. Elmisery, A. M. & Sertovic, M. & Zayin, A. & Watson, P. (2025). Cyber Threats in Financial Transactions – Addressing the Dual Challenge of AI and Quantum Computing. arXiv preprint arXiv:2503.15678.
4. Saeed, M. M. (2025). An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption. IEEE Access.
5. Saguato, P. (2025). Regulation of clearing and settlement. In Comparative Financial Regulation (pp. 239–254). Edward Elgar Publishing.
6. Uzoma, E. & Enyejo, J. O. & Motilola Olola, T. (2025). A Comprehensive Review of Multi-Cloud Distributed Ledger Integration for Enhancing Data Integrity and Transactional Security. International Journal of Innovative Science and Research Technology. 10(3). 1953–1970.
7. Xu, Y. (2025). Research on Computer Information Network Security Technology and Development Direction. Journal of Computing and Electronic Information Management. 16(2). 21–24.
8. Zafar, A. (2025). Quantum computing in finance: Regulatory readiness, legal gaps, and the future of secure tech innovation. European Journal of Risk Regulation. 1–32.