Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515

Quantum Computing Readiness in Financial Services: Security Implications, Post-Quantum Cryptography and Future Banking Infrastructure

M Ravi Kumar

Research Scholar
Department of Management
Osmania University, Hyderabad

Abstract:
Quantum computing represents one of the most significant emerging technological opportunities and cybersecurity challenges for the financial-services industry. Although large-scale, fault-tolerant quantum computers had not been achieved by September 2024, the potential ability of sufficiently powerful quantum computers to compromise widely used public-key cryptographic systems creates a long-term security risk for banks, payment systems, financial markets and central-bank infrastructure. Financial institutions are particularly exposed because they manage large volumes of sensitive information, depend extensively on cryptographic authentication and digital signatures, and operate infrastructure that must remain secure for decades.

This research examines quantum-computing readiness in financial services, focusing on security implications, post-quantum cryptography (PQC), regulatory preparedness and future banking infrastructure.

The present paper states that the financial sector has strong economic incentives to explore quantum technologies while simultaneously facing significant cryptographic risks. The study states that quantum readiness should not be regarded as a future-only cybersecurity project. Financial institutions should begin cryptographic inventories, identify long-lived sensitive data, develop cryptographic agility, test PQC algorithms, modernize legacy infrastructure and establish governance frameworks. A phased migration toward quantum-resistant banking infrastructure is essential to protect confidentiality, authentication, payment integrity and financial stability.

Keywords: Quantum Computing, Financial Services, Post-Quantum Cryptography, PQC, Cybersecurity, Quantum Readiness, Cryptography, Digital Banking, Financial Infrastructure.

Introduction

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515

The financial-services industry is undergoing continuous technological transformation. Digital banking, mobile payments, cloud computing, artificial intelligence, open banking, distributed systems and real-time payment infrastructures have increased the speed and convenience of financial transactions. At the same time, these developments have created a greater dependence on cybersecurity, cryptographic authentication and secure communications.

Cryptography is fundamental to modern banking. Public-key cryptography is used in secure communications, digital signatures, authentication, certificates, payment infrastructure and numerous other applications. Banks therefore depend on cryptographic mechanisms not only to keep information confidential but also to establish trust between customers, financial institutions, payment providers and regulators.

Quantum computing introduces a fundamentally different computational model. Classical computers process information using bits, whereas quantum computers use quantum bits, or qubits, that exploit quantum mechanical properties such as superposition and entanglement. Although quantum computers are still developing and had not reached the scale required to break today's widely used cryptographic systems by September 2024, quantum algorithms have demonstrated why the financial sector must prepare in advance.

The financial industry is especially sensitive to this problem because financial data frequently has long-term value. Account information, transaction records, identity information, corporate financial data, payment instructions, securities information and central-bank communications can remain sensitive for many years. The threat known as "harvest now, decrypt later" is therefore particularly important. Attackers can collect encrypted information today and potentially decrypt it in the future if sufficiently capable quantum computers become available.

The urgency of the issue increased substantially in 2024 when NIST finalized the first three major post-quantum cryptographic standards. On 13 August 2024, NIST approved FIPS 203, FIPS 204 and FIPS 205. FIPS 203 specifies ML-KEM for key establishment, while FIPS 204 and FIPS 205 specify ML-DSA and SLH-DSA for digital signatures.

This development is important for financial institutions because it moves post-quantum cryptography from a primarily research-oriented topic toward a practical migration issue. Organizations can now begin planning around standardized algorithms rather than waiting indefinitely for the technology to mature.

However, the same technological development that creates opportunities can create cybersecurity risks. The WEF warned that quantum computing could undermine existing encryption and potentially threaten the trust and stability upon which financial services depend.

Consequently, financial institutions face a dual challenge. They must explore how quantum computing can improve financial modelling, optimization, risk analysis and other computational tasks while simultaneously preparing their infrastructure for a future in which existing cryptographic mechanisms may no longer provide adequate protection.

Research Objectives

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515

- To examine the security implications of quantum computing for financial institutions and banking infrastructure.
- To analyse the role of post-quantum cryptography in protecting financial data, payment systems and digital banking infrastructure.
- To evaluate the readiness of the financial sector for the transition from classical cryptography to quantum-resistant cryptographic standards.
- To examine the organizational, technological and regulatory challenges associated with implementing quantum-safe banking infrastructure.
- To propose a future-oriented quantum-readiness framework for financial institutions based on cryptographic inventory, migration planning, cryptographic agility, hybrid security and continuous risk management.

Quantum Computing and Financial Services

Quantum computing has potential applications across financial services.

Portfolio optimization

Portfolio optimization involves selecting combinations of financial assets while considering risk, return and constraints.

Quantum optimization algorithms may eventually help solve complex optimization problems that become computationally expensive as the number of assets and constraints increases.

Fraud detection and Risk management

Quantum computing may eventually support complex optimization and machine-learning tasks relevant to financial fraud detection. However, this area should be distinguished from the immediate cybersecurity issue.

The most urgent quantum-related financial risk before October 2024 was not that quantum computers were already replacing fraud-detection systems. It was the possibility that future quantum computers could undermine the cryptography securing financial transactions and data.

Quantum algorithms could potentially support complex financial simulations and optimization. This could improve stress-testing and risk-management capabilities if scalable quantum hardware becomes available.

Security Implications of Quantum Computing

Threat to RSA-RSA security depends on the computational difficulty of factoring large integers using classical computers.

Shor's algorithm theoretically changes this situation because a sufficiently powerful quantum computer can factor integers much more efficiently.

"Harvest Now, Decrypt Later"

One of the most important security concepts is Harvest Now, Decrypt Later (HNDL).

The attack does not require an adversary to possess a powerful quantum computer today.Instead:

An attacker collects encrypted financial data today.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515

The attacker stores the encrypted information.
A sufficiently powerful quantum computer becomes available in the future.
The attacker attempts to decrypt the previously captured information.
This is particularly dangerous for financial information with long-term confidentiality requirements.

Analysis

Quantum investment in financial services

The World Economic Forum's 2024 report estimated that financial-sector investment in quantum innovation could rise from:
US$80 million in 2022 → US$19 billion by 2032
The report also projected that quantum technology could potentially create up to US$850 billion in value over 30 years.

Cryptographic agility

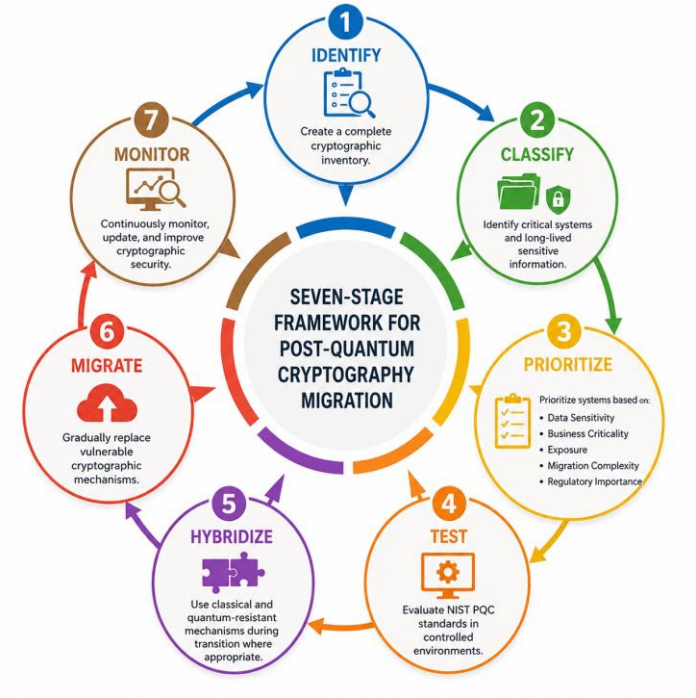
Cryptographic agility means that an institution can change cryptographic algorithms without redesigning its entire infrastructure.
This is essential because cryptographic standards can evolve. A future banking architecture should therefore avoid deeply embedding a single cryptographic algorithm into applications.

Future Banking Infrastructure

Future banking infrastructure is expected to evolve toward a quantum-resilient and cryptographically agile architecture, where classical and quantum technologies operate together. Quantum computing may support portfolio optimization, financial risk modelling, fraud detection and complex financial simulations, while classical systems will continue to manage routine banking operations. Financial institutions will increasingly adopt cloud-based quantum computing and hybrid architectures to explore these applications without immediately replacing existing infrastructure.
Security will remain the primary requirement of future banking infrastructure. Banks should gradually introduce post-quantum cryptography (PQC), cryptographic agility, secure key management and quantum-resistant payment systems to protect sensitive financial data and transactions. The BIS Project Leap initiative demonstrated the feasibility of integrating quantum-resistant cryptography into financial communication systems, highlighting the importance of beginning the transition before large-scale quantum computers can threaten existing cryptographic systems

Proposed Quantum-Ready Banking Framework

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515



Research Findings:

- Quantum risk is strategic rather than purely technological-The risk affects confidentiality, authentication, payment integrity and potentially financial stability.
- The financial sector has strong incentives to adopt quantum technology WEF projected financial-sector quantum investment could grow from US$80 million in 2022 to US$19 billion by 2032.
- The security transition has already begun-NIST finalized FIPS 203, 204 and 205 in August 2024, providing standardized PQC mechanisms.
- "Harvest now, decrypt later" makes preparation urgent-The absence of a cryptographically relevant quantum computer today does not eliminate the need for migration because sensitive encrypted information can be collected today and potentially decrypted later.
- Quantum readiness requires infrastructure transformation-Replacing one cryptographic algorithm is insufficient. Banks must address applications, certificates, keys, hardware, cloud systems, vendors and payment infrastructure.

Recommendations

- Begin a comprehensive cryptographic inventory immediately.
- Identify sensitive data requiring long-term confidentiality.
- Assess exposure to RSA and ECC-based cryptography.
- Develop a formal post-quantum migration strategy.
- Evaluate NIST FIPS 203, 204 and 205 for appropriate applications.
- Develop cryptographic agility so algorithms can be replaced efficiently.
- Use hybrid classical/PQC approaches during migration where appropriate.
- Conduct PQC performance and interoperability testing.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515

- Include third-party vendors in quantum-readiness assessments.
- Create quantum-risk governance at board and senior-management level.
- Train cybersecurity and infrastructure teams in quantum-safe cryptography.
- Coordinate with central banks, payment networks and regulators.
- Protect long-lived financial data against harvest-now-decrypt-later attacks.
- Integrate quantum risk into existing operational-resilience and cybersecurity frameworks.
- Continuously review emerging quantum developments rather than relying on a fixed migration plan.

This architecture emphasizes that PQC should be integrated throughout the banking ecosystem rather than implemented only at the network perimeter.

Conclusion

Quantum computing presents financial institutions with a unique combination of opportunity and risk. On one side, quantum technologies could potentially improve complex financial calculations, portfolio optimization, simulation and other computationally intensive activities. On the other side, sufficiently powerful quantum computers could threaten the public-key cryptography on which modern financial infrastructure depends. RSA and elliptic-curve systems are particularly important because of their widespread use in authentication, encryption and digital signatures.

The research demonstrates that the quantum threat should not be considered exclusively a distant future problem. The possibility of harvest-now-decrypt-later attacks means that sensitive financial information transmitted or stored today may have future security implications.

Financial institutions should not wait until a cryptographically relevant quantum computer exists before beginning migration. Instead, banks should establish cryptographic inventories, identify critical systems, prioritize long-lived sensitive information, develop cryptographic agility, test PQC algorithms and implement hybrid approaches where appropriate.

The future banking infrastructure should consequently be designed around five principles:

Quantum resilience + cryptographic agility + interoperability + continuous monitoring + regulatory governance.

The conclusion is not simply to make banks resistant to a future quantum computer. It is to ensure that financial services remain confidential, authentic, available, resilient and trustworthy throughout the transition from the classical computing era to the quantum era.

REFERENCES:

1. Wilkens, S., & Moorhouse, J. (2023). Quantum computing for financial risk measurement. Quantum Information Processing, 22, 51.
2. Aboussalah, A. M., Chi, C., & Lee, C.-G. (2023). Quantum computing reduces systemic risk in financial networks. Scientific Reports, 13, 3990.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1515

3. Li, Y., et al. (2023). BQ-Bank: A quantum software for finance and banking. Quantum Engineering, 2023, Article 7810974.
4. Schiansky, P., Kalb, J., Sztatecsny, E., Roehsner, M.-C., Guggemos, T., Trenti, A., Bozzio, M., & Walther, P. (2023). Demonstration of quantum-digital payments. Nature Communications, 14, 3849.
5. Kumar, M. (2022). Post-quantum cryptography algorithm's standardization and performance analysis. Array, 15, 100242.
6. Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., Pistoia, M., & Alexeev, Y. (2023). Quantum computing for finance. arXiv.
7. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41.
8. Mosteanu, N. R., & Faccia, A. (2021). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 7(1), 19.
9. A review of the present cryptographic arsenal to deal with post-quantum threats. (2022). Procedia Computer Science, 215, 834–845.