

Role of Quantum Cryptography in the Financial Sector: How is the World Preparing for a New Era of Computing?

Hamsini Mopuru

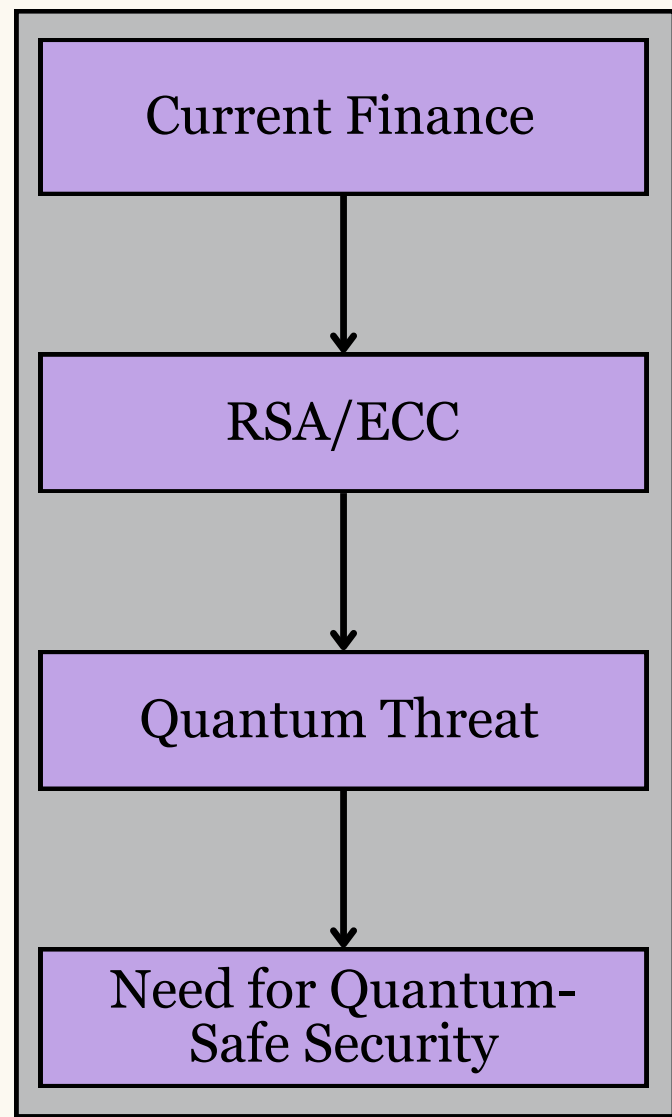
Abstract

Quantum computing presents a long-term cybersecurity challenge for the financial sector because widely used public-key systems such as RSA and ECC are vulnerable to sufficiently capable quantum computers. This review examines how governments, regulators, and financial institutions are preparing for the transition to quantum-resilient security. Academic literature, institutional reports, technical standards, and organizational case studies were synthesized to evaluate post-quantum cryptography (PQC), quantum key distribution (QKD), regulatory responses, and global readiness. The literature suggests that PQC will provide the most scalable foundation for quantum-safe security, while QKD may complement it in high-value communications. However, readiness remains uneven across countries and institutions. Coordinated standards, phased implementation, crypto-agility, and continued investment will therefore be central to financial resilience in the quantum era.

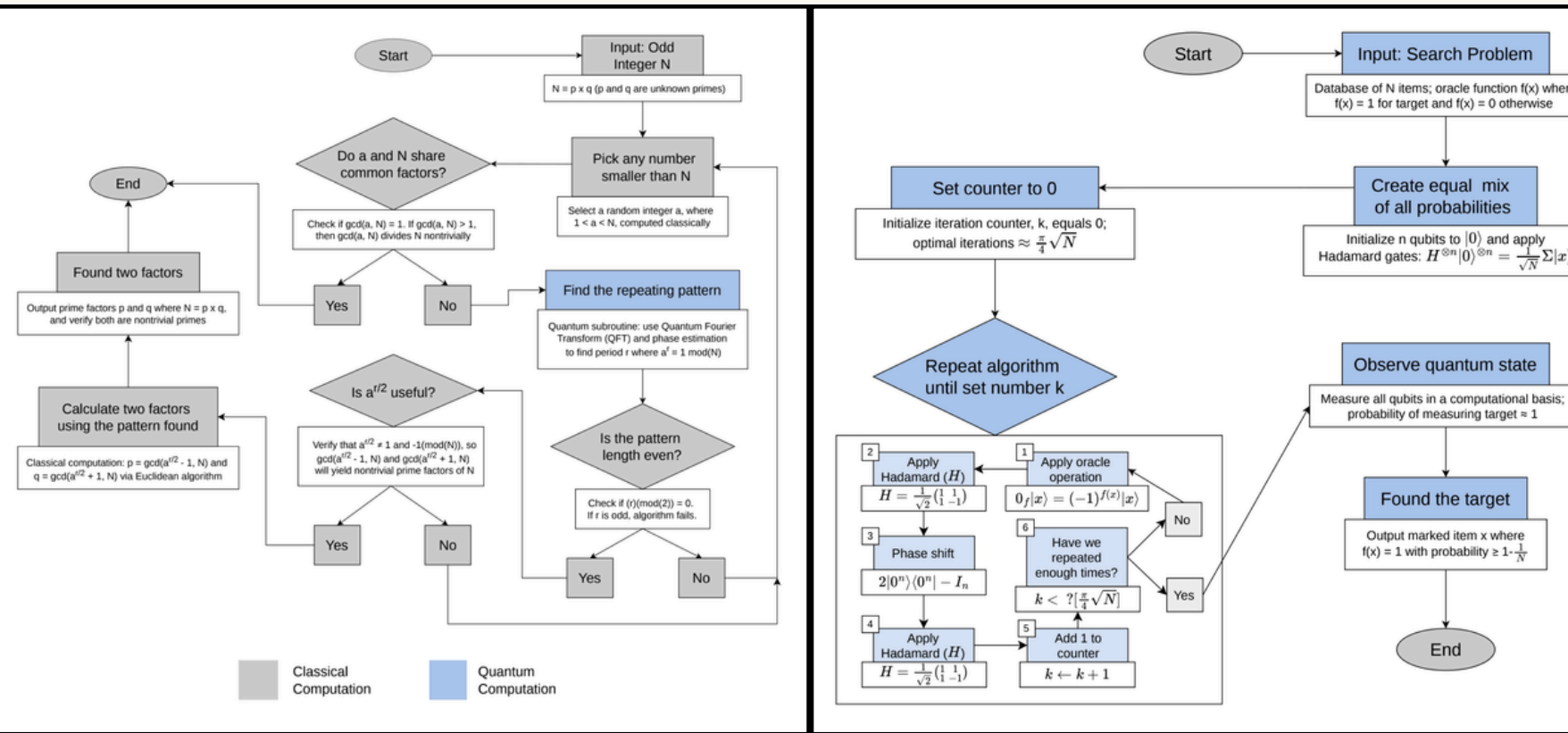
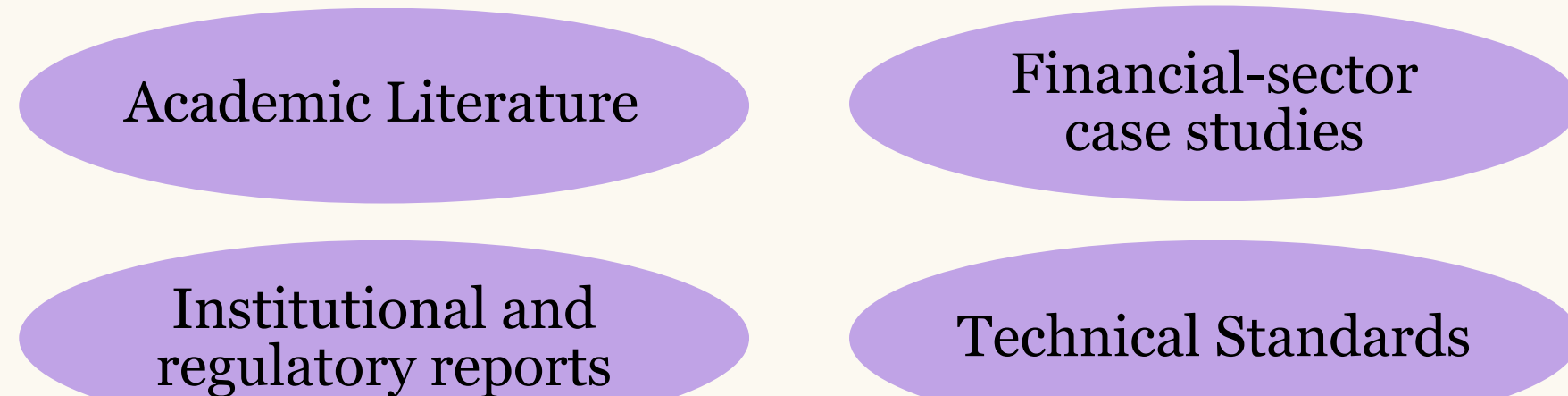
Background

Why does quantum computing matter?

- Financial systems rely heavily on RSA and ECC
- These systems are secure because certain mathematical problems are difficult for classical computers
- Shor’s algorithm can undermine those assumptions
- Long-term risk: “harvest now, decrypt later”
- Quantum threats could affect payments, authentication, interbank communication, and stored financial data



How are governments and financial institutions preparing for quantum-era cybersecurity risks?



Shor’s Algorithm → replacement problem

Grover’s Algorithm → key-strength problem

Quantum-Secure Solutions

Financial institutions are primarily evaluating two quantum-safe approaches: *post-quantum cryptography* (PQC) and *quantum key distribution* (QKD). PQC is more scalable because it can be deployed on existing classical networks, while QKD provides stronger key-exchange protection but requires specialized infrastructure. The literature therefore treats them as complementary rather than interchangeable.

PQC	QKD
Software-based	Hardware-based
Quantum-resistant math	Uses quantum mechanics
Existing classical networks	Optical/fiber links
More scalable	More limited scalability
Lower deployment burden	Higher deployment burden
Best for broad migration	Best for high-value links

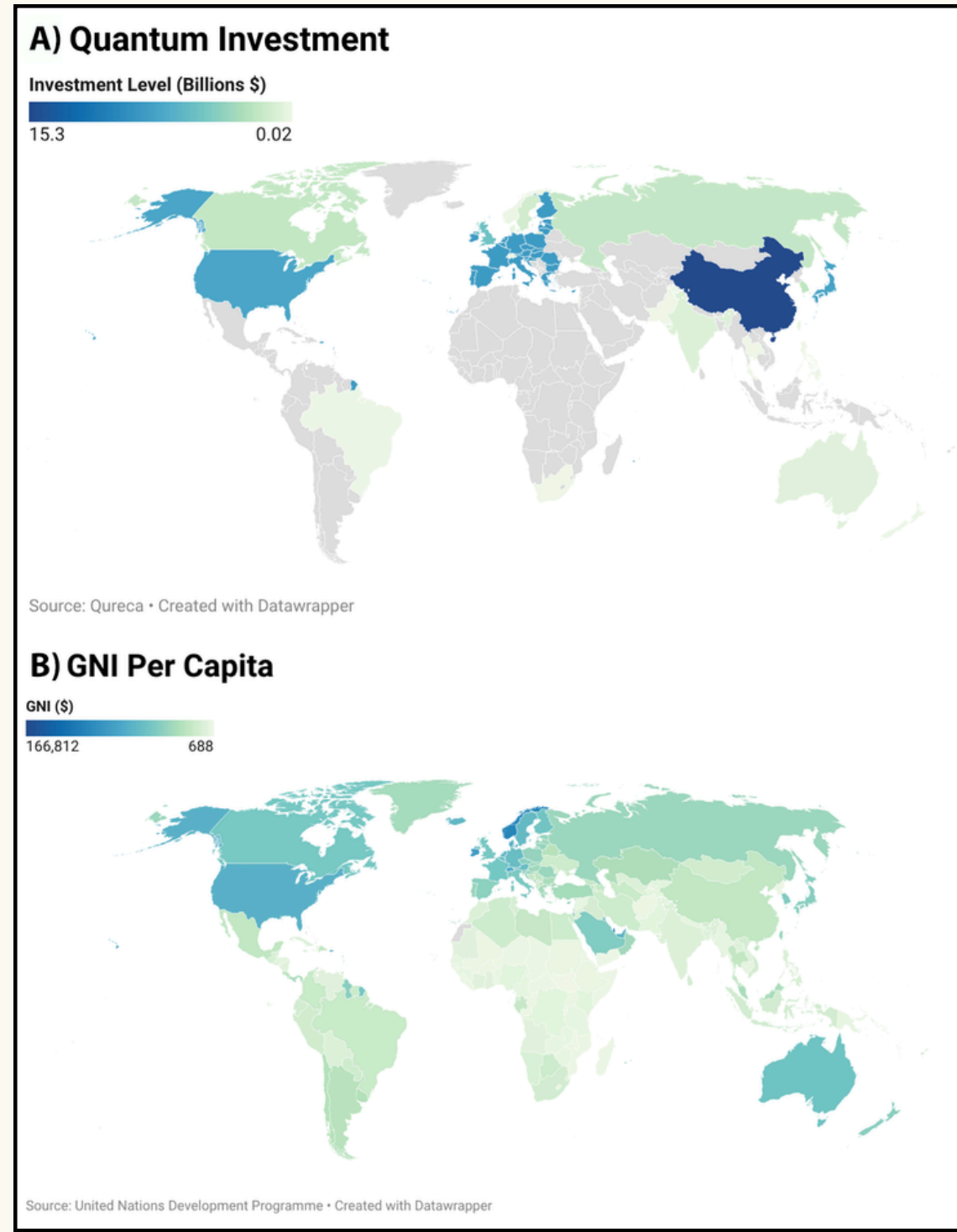
→ Hybrid systems combine strong key exchange with fast classical encryption, making them a practical transitional model for financial institutions

Institution	Readiness	Example Initiative
JPMorgan Chase	Actionable	QKD over live fiber; crypto-agile infrastructure for future PQC migration
HSBC	Actionable	QKD testing in trading; PQC-secured tokenized assets
Goldman Sachs	Conceptual	Internal quantum simulations for pricing and risk modeling
Fidelity	Conceptual	Quantum research for financial modeling and investment applications
Barclays	Conceptual → Actionable	Quantum research in settlement and financial optimization
Wells Fargo	Conceptual → Actionable	QKD-based key-generation proof-of-technology

Global Response

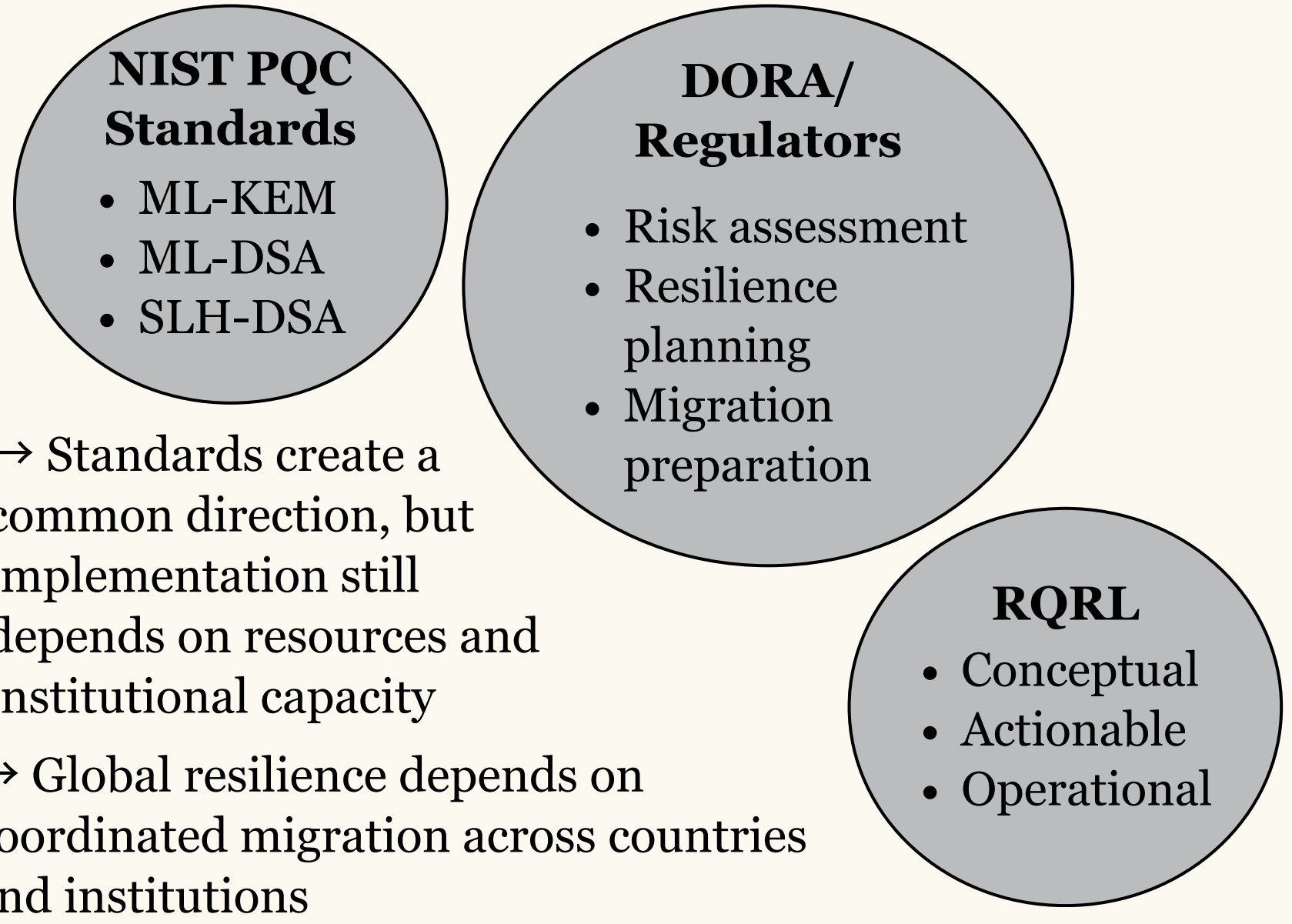
Quantum investment is concentrated in higher-capacity economies, which also tend to have stronger research ecosystems, cybersecurity infrastructure, and technical workforces. This creates uneven levels of quantum readiness across the global financial system.

Global Distrubution of Quantum Investment vs GNI Per Capita



Higher capacity → Earlier migration → Stronger readiness

Lower capacity → Slower migration → Longer exposure



→ Standards create a common direction, but implementation still depends on resources and institutional capacity

→ Global resilience depends on coordinated migration across countries and institutions

References

[1] Naik et al. (2025), Financial Innovation; [3] Gorbanev et al. (2021), IMF; [6] Mehta et al. (2024), IEEE QCE; [15] QURECA (2025), Quantum Initiatives Worldwide. [16] UNDP (2024), HDR Data Center; [20] NIST (2024), PQC Standards; [33] JPMorgan Chase (2022), QKD network; [34] HSBC (2024), quantum-safe tokenized gold.

Acknowledgements

Supported in part by NSF Award DMS-2231533. I thank Daniel Serrano for his mentorship and guidance throughout this project, and Carl Miller for reviewing the manuscript and providing valuable feedback.