Quantum-Resilient Cryptography and Financial Stability in Economic Systems

Robin Deniz Algül
American Collegiate Institute

***Abstract*—The accelerating adoption of quantum computing poses both unprecedented opportunities and systemic risks for global financial systems. While quantum algorithms promise breakthroughs in portfolio optimization, risk modeling, and economic forecasting, the potential compromise of classical cryptographic infrastructures threatens the confidentiality, integrity, and stability of digital financial ecosystems. This study examines the interplay between quantum-resilient cryptography and macro-financial stability, proposing a dual-layer security-economic framework to guide the transition toward post-quantum financial architectures. We evaluate leading post-quantum cryptographic (PQC) standards—including lattice-based, hash-based, and code-based schemes—and assess their performance within high-frequency trading networks, interbank settlement systems, and blockchain-enabled financial platforms. Simulation-based analyses demonstrate that PQC integration introduces measurable computational overheads but significantly strengthens resistance against quantum-enabled cyberattacks, thereby mitigating systemic vulnerabilities that could cascade across financial markets. Our findings highlight that timely migration to quantum-safe cryptography is essential for preserving economic stability, protecting financial institutions from existential cyber risks, and ensuring the long-term resilience of digital economies in the quantum era.**

The rapid advancement of quantum computing represents a profound technological shift with far-reaching implications for financial systems worldwide [2]. While quantum algorithms offer the potential to transform computational finance—enhancing portfolio optimization, improving risk analytics, and accelerating macroeconomic simulations—they simultaneously pose critical security challenges [6]. Many foundational cryptographic schemes used in banking, digital payments, insurance, central-bank infrastructure, and blockchain networks rely on mathematical problems that could be efficiently broken by quantum algorithms such as Shor's and Grover's. A sufficiently powerful quantum computer could render widely deployed encryption methods obsolete, exposing global financial systems to catastrophic vulnerabilities [3].

This emerging quantum threat has direct consequences for financial stability. The digital economy depends on secure communication channels, authenticated transactions, and tamper-resistant records [4]. A quantum-enabled breach could undermine institutional trust, disrupt market operations, enable fraudulent asset transfers, and trigger systemic contagion across interconnected financial networks. Central banks and regulatory

Digital Object Identifier 10.62802/dkahxv90

Date of publication 26 11 2025; date of current version 26 11 2025

