Post-Quantum Cryptographic Protocols for Securing Digital Trade and International Payment Systems

Cem Fotocan
American Collegiate Institute

***Abstract*—The advent of scalable quantum computing poses a significant threat to the cryptographic foundations of digital trade, cross-border payment systems, and global financial infrastructures. Current public-key cryptosystems—widely used in digital transactions, payment authorization, and inter-bank messaging—are vulnerable to quantum-based attacks such as those enabled by Shor's algorithm. This review analyzes the emerging domain of post-quantum cryptography (PQC) and quantum-resilient protocol design within the context of international trade and payment gateways. Key themes include the migration of legacy payment and settlement protocols to quantum-resistant formats, the integration of lattice-based key encapsulation mechanisms, stateless hash-based digital signatures, and hybrid classical–quantum key distribution (QKD) within financial messaging standards, as well as system-level design considerations for trade platforms that emphasize forward secrecy, long-term data confidentiality, and regulatory compliance across jurisdictions. By synthesizing standardization efforts and industry transition case studies, this paper offers a roadmap for financial institutions, technology vendors, and regulatory bodies to orchestrate a coordinated shift toward quantum-safe digital trade ecosystems.**

Global digital trade and payment systems form the backbone of the modern economy, enabling instantaneous transfers across borders, real-time settlement, and seamless integration of financial services [4]. These infrastructures rely heavily on public-key cryptography, secure key exchanges, and authenticated digital messaging to ensure confidentiality, integrity, and non-repudiation of transactions. However, the evolution of quantum computing challenges the very foundations of these systems [3]. Large-scale quantum machines—once realized—are expected to efficiently factor large integers and compute discrete logarithms, rendering widely used algorithms such as RSA and elliptic-curve cryptography (ECC) insecure.

Financial trade systems face unique vulnerabilities in this context. Many trade and payment transactions require long-term confidentiality, meaning data transmitted today may remain sensitive for decades, creating a "harvest-now, decrypt-later" threat model [6] Furthermore, the interoperability demands of global finance imply that even a single vulnerable node

Digital Object Identifier 10.62802/q1h2xg17

Date of publication 19 11 2025; date of current version 19 11 2025

