Empirical Economics Letters, 25 (Special Issue 2): pp. 295-309, (February 2026) ISSN 1681 8997
https://doi.org/10.5281/zenodo.20446728

Navigating the Quantum Threat: India's Transition to Quantum-Safe Cryptography in Digital Payments

Sai Pranav[*] and S. Shriya[**]

ICFAI Law School, Hyderabad, India

Abstract: As digital payments become the backbone of economies in South Asia, quantum computing threatens to break the cryptography that secures modern financial systems. This paper explains in straightforward terms how cryptography ensures trust in digital payments, and why emerging quantum technologies could render widely used encryption methods such as RSA and ECC vulnerable. It explores the concept of "quantum risk," showing how payment systems require urgent upgrades to prevent future breaches. Focusing on developments in India, the paper reviews the country's regulatory structure, technical innovations, and efforts to build quantum-safe digital infrastructure. It assesses India's preparations in comparison to the FATF guidelines and international best practices, comparing the nation's roadmap with steps already taken by global leaders, including China, the EU, and Singapore. The study highlights the progress made in India and also points out critical challenges in regulation, talent, cost, and cross-border interoperability. A practical set of recommendations is provided for India's path forward, including cryptographic agility, mandatory RBI standards for quantum-safe algorithms, deeper collaboration between government, fin-techs, and academic institutions, & strict alignment with NIST and ISO global standards. The paper emphasizes that India, with its active fintech sector and huge transaction volumes, must accelerate its quantum-proof encryption transition to safeguard consumer trust and financial stability, and sets out clear steps for policymakers and industry to future-proof the payment ecosystem in the coming quantum era.

Keywords: Quantum Computing, Quantum Threats, Quantum-Safe Cryptography, Post-Quantum Cryptography (PQC), Digital Payments

JEL Classification Number: O33, K39

[*] and [**] Students.