The Quantum Countdown: Why India's Financial Sector Can't Wait

Kquanta Research

KQUANTA RESEARCH

- Financial institutions must act urgently as quantum computing threatens to break current cryptographic systems.

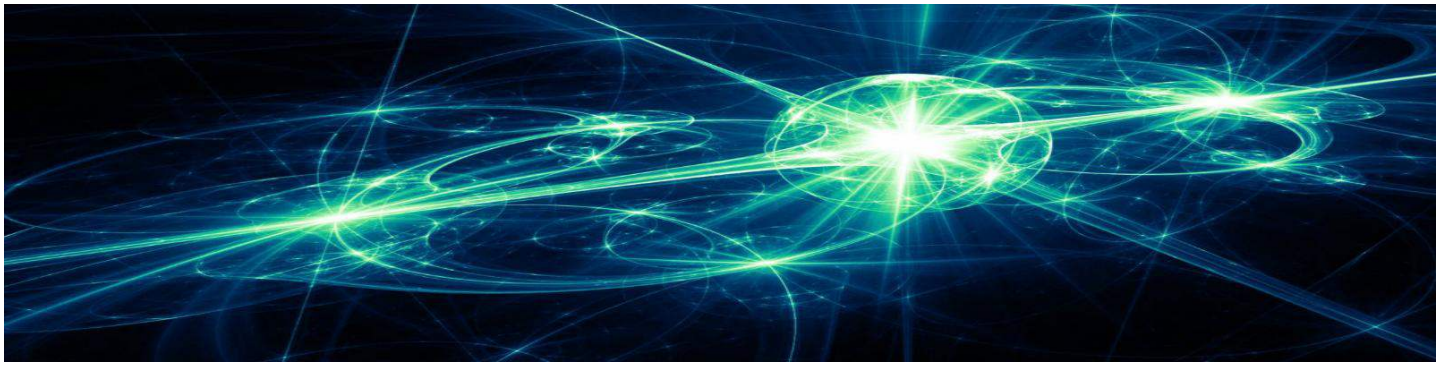
- Europol warns the financial sector to prepare now for post-quantum security, despite capable quantum computers being potentially a decade away.

- A concerning 86% of financial organisations admit being unprepared for quantum computing's cybersecurity implications, according to a 2023 QSFF survey.

Q: Have you heard about the Cloud Security Alliance's (CSA) countdown clock to Quantum Day?

A: The Cloud Security Alliance (CSA) has established a specific date for this threat to materialise - *April 14, 2030*.

This "Quantum Day" or "Q-Day" marks when CSA estimates quantum computers will be able to compromise current cybersecurity infrastructure.



Q: What is quantum technology and how is it relevant to finance?

A: Quantum technology harnesses the principles of quantum mechanics to drive groundbreaking advancements across various sectors.

In finance, quantum technology enables faster processing of complex calculations, secure communications through quantum encryption, and enhanced measurement capabilities through quantum sensing.

Q: How do quantum technology and AI converge in financial services?

A: The merging of artificial intelligence and quantum technology creates a powerful convergence with extraordinary potential. Quantum computing enhances AI algorithm performance, while AI optimises quantum algorithms.

This partnership delivers superior data processing, better risk management, personalised financial offerings and strengthened security measure

Q: Which areas can quantum technology be used for in financial services?

A: Quantum technology can be applied to several key areas in financial services:

- Portfolio Optimisation
- Trading Optimisation
- Treasury Management
- Asset Management

Q: What is the "Harvest Now, Decrypt Later HNDL" attack and why is it concerning?

A: HDNL poses an urgent threat where adversaries collect encrypted data now to decrypt later when quantum computers become powerful enough.

Threat Actors intercept and store data protected by public-key systems like RSA or elliptic curve cryptography, awaiting large-scale quantum computers to rapidly decrypt it.

This especially threatens data needing long-term confidentiality, such as government communications and intellectual property

.

Q: Why Indian Financial Services Entities Are Threatened by Quantum Computing?

A: Indian financial entities face heightened quantum computing risks due to:

High-Value Targets: The financial sector is targeted for cyberattacks due to valuable data and potential economic impact.

Long-Term Data Protection Requirements: Financial data requires security for extended periods, making it vulnerable to the "Harvest Now, Decrypt Later" threat.

Systemic Risk: A breach at a major financial organisation can have cascading effects throughout India's financial system.

Q: What recommendations has the Reserve Bank Innovation Hub made for Indian banks?

A: The Reserve Bank Innovation Hub recommends that Indian banks proactively transition to post-quantum cryptography (PQC) algorithms to address the threat that quantum computing poses to existing encryption methods.

Q: What is SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF)?

A: The Centralised Security and Cyber Resilience Framework (CSCRF) enhances the cybersecurity of entities regulated by SEBI, with a focus on resilience and responsiveness to emerging threats. The incorporation of quantum-safe solutions serves to reinforce compliance and safeguard against future quantum-related threats.

Q: What action plan is recommended for Indian financial services regarding quantum technology?

A: The recommended Q-Action Plan for Indian financial services includes :

- Establishing a National Quantum Finance Task Force
- Investing in quantum education and skill development
- Fostering industry-academia collaboration for quantum finance research
- Developing India-specific use cases and proof-of-concept projects

For access to our reports reach us
contact@kquantaresearch.com