Q→NU

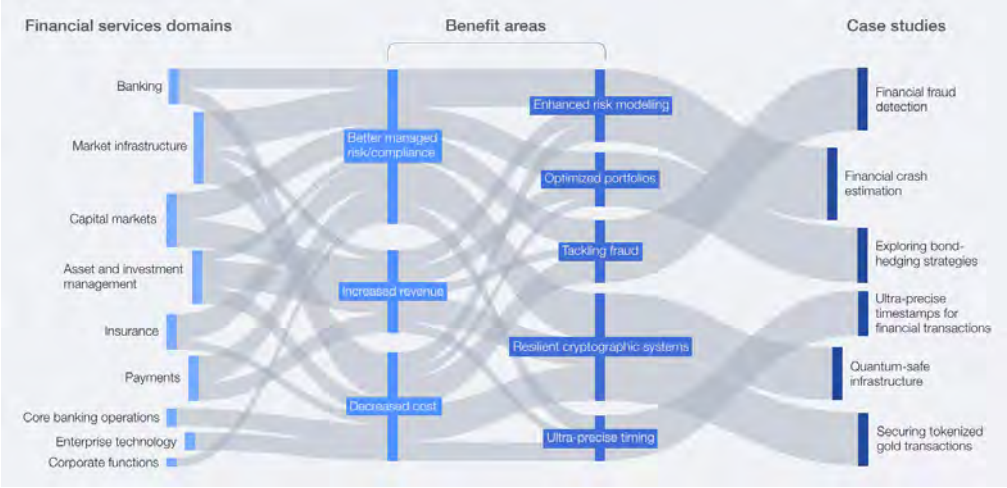
Secure Your Financial Communication Before Quantum Breaks It

Protect your 'Financial Transactions and Communications' from 'Evolving Cyber Threats'. Power up with the '**World's Only Full-Stack Integrated Quantum-Safe Platform**'.

Digital Resilience must move from Early detection and Faster Response to anticipation of future threats much ahead of time. Time has come for enterprises to prioritize proactive immunity.

The Urgency of Quantum Cybersecurity in BFSI

- Protect your 'Financial Transactions and Communications' from '**Evolving Cyber Threats**'. Power up with the '**World's Only Full-Stack Integrated Quantum-Safe Platform**'.
- NIST standardised new quantum-resistant algorithms in August 2024 and have defined the implementation window between 2025 (**Aggressive**) to 2030 (**Pessimistic**)
- NIST's transition roadmap clearly states that RSA-based key establishment (and digital signatures at 112-bit strength) is slated to be deprecated after 2030 and disallowed after 2035. **(Source: appviewx)**
- The National Quantum Mission (NQM) is establishing a task force to help banks adopt quantum-safe technologies for cybersecurity, financial modelling, and data analysis **(Source: Reserve Bank Innovation Hub)**
- Q-Day when quantum computers break classical security—will cause major losses and compliance breaches, making early QComm adoption crucial. The $1B market in 2023 is growing rapidly at a 22–25% CAGR.
- The U.S. views quantum computing as a national security priority, with advisor Jake Sullivan naming it a key technology the government aims to safeguard over the next decade. **(AOShearman)**
- Total Quantum Communication is projected to reach **$10.5B–$14.9B** by 2035 with a CAGR of 22–25% **(McKinsey, June 2025)**. India's BFSI cybersecurity market is expected to reach $3.5B by 2027. **(Source: Research and Markets)**
- SEBI's CSCRF addresses emerging threats like quantum-computing **("harvest-now, decrypt-later")** with guidance on cryptographic inventory and post-quantum readiness. It sets a unified framework for India's financial stability, requiring Regulated Entities to meet five resilience goals and submit annual Cyber Capability Index reports. **(RBI, Apr 2025)**



Mapping of financial services domains to benefits and case studies **(source: WEF, July 2025)**

RBI Tightens Cyber & Data Sovereignty Norms – Mandates '.bank.in' domains by Oct 31, 2025 **(Source: RBI Circular, 2025)**; it also mandated data localisation, cybersecurity audits, and operational resilience under ORMF to protect India's digital sovereignty of sensitive financial data and bolstering public trust in India's rapidly evolving digital financial landscape. **(RBI, Apr 2025)**

With the above information, we are not trying to scare you, but to help you prepare for Q-Day as efficiently as possible. How?

QNu Labs: Built for the Quantum Threat. Trusted for What's Next.

Pioneering Vision: QNu Labs foresaw the quantum threat nine years ago and proactively developed solutions from the ground up.

Aligned with Global Standards: Today, global bodies like NIST have advanced PQC standards, recently approving HQC for key encapsulation.

Indigenous Innovation: QNu's entire quantum-safe technology stack is fully homegrown—designed, built, tested, and deployed in India.

Proven and Protected: The technology is certified, patented (10 granted, including 3 in the USA; 15 pending), and deployed in real-world settings.

Strategic Partnerships: Backed by NQM, QNu leads in quantum security, supporting widespread adoption with strong use cases. (CBDC-ready, NIST/RBI compliant)

Trusted Implementation: QNu's methodology is proven globally, delivering scalable, plug-and-play integration for Govt. and enterprise infrastructure.

Quantum threats are real - QNu provides BFSI leaders proven, ready-to-deploy solutions. We help upgrade your digital infrastructure to quantum-safe standards, secure against classical and quantum computing.

Q→NU

QVerse

The Quantum Question Every CIO, CTO & CISO Must Now Confront

- Are our internal chats, client communications, and sensitive files protected against quantum-enabled breaches?
- Can we prove end-to-end compliance and audit-readiness?
- Is our messaging platform flexible enough for on-premises deployment?
- How do we future-proof our infrastructure before any data breach happens?
- How do we currently track and audit data exchanges on public messaging platforms?
- How do we guarantee that confidential data exchanges are accessible exclusively to authorised parties, and only after the proper legal procedures have been followed?
- How do we handle obtaining consent when employees within the bank share customer data for operational purposes?

Introducing QVerse for BFSI (Powered by QNu Labs) that ensures quantum-resilient, regulatory-ready, end-to-end secure messaging, collaboration and communication for the BFSI sector with zero data leaks.

Ensure your critical messages, files, voice recordings, and videos remain encrypted, compliant, and audit-ready across devices and teams.

QVerse Key Differentiators

Consent-based file sharing with granular admin controls

100% forward secrecy for all communications

Built-in DLP, containerized security for file, voice, and video

Post-quantum encryption using CRYSTALS-Kyber and lattice cryptography

AES-256 plus PQC hybrid encryption for next-gen security

100% indigenous technology, designed and built in India for global markets

Secure Message Vault with no-screenshot policy

Remote wipe and advanced session management capabilities

Flexible on-premise, private cloud, or SaaS deployment options

Fully compliant with RBI, SEBI, NIST, FIPS; easy to deploy, integrate, and scale

QVerse Key Features

- **Secure Messaging:** One-to-one, group, and broadcast with quantum-safe encryption
- **Data Privacy & DLP:** Files stay within the app; no screenshots, screen recording blocked
- **Vault Storage:** Sensitive OTPs, passwords stored in secure, access-controlled vault
- **Robust Admin Controls:** Manage users, enforce file restrictions, and maintain comprehensive audit logs.
- **Remote Wipe Capability:** Instantly revoke access and erase app data from lost devices.
- **Flexible Deployment & Access:** Available as SaaS, on-premises, or private cloud, with seamless mobile and web sync.

Q→NU

QVerse

Why Our Customers Win with QVerse?

Platform	Quantum-Safe	Admin Control	India Compliant	Cloud/On-Prem Support
QVerse	✔ CRYSTALS-Kyber + Lattice cryptography (PQC + Advanced)	✔ DLP, remote wipe, granular messaging	✔ NIST	✔ All options
Apple iMessage	✘ (Partial, Level 3)	Consumer-grade	✘ Partial	✔ Apple ecosystem
Signal	✘ (Level 2)	✘ Limited	✘ Partial	✔ Cloud only
MS Teams	✘	✔ Basic	✘ Not India-native	✔ Cloud only
WhatsApp**	✘ ECC only	✘ No admin logs	✘ Foreign cloud	✔ Cloud only

** Other traditional messaging and collaboration platforms viz. Slack, Telegram, Google Chat have same issues.

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025

CIN: U72900KA2016PTC096629

India USA Australia Global