ALTAIR & ALANG

www.altairalang.com
Strategy ➥ Consulting ➥ Redefined

FEATURED INSIGHTS

12 November 2025

Quantum Computing, Operational Resilience and the Future of Financial Market Infrastructures (FMI)

Executive-level briefings that provide timely, sector-specific analysis on global market developments. These insights are published to provide high-level insights across the financial services, capital markets, clearing, technology, fintech, cyber, and other sectors.

REF: AA_FEATURED_INSIGHTS_20251112V1

CONTENTS

FEATURED INSIGHTS

QUANTUM COMPUTING, OPERATIONAL RESILIENCE AND THE FUTURE OF FINANCIAL MARKET INFRASTRUCTURES (FMI)

Date: 2025-11-12

Prepared by: Altair & Alang

For any questions regarding this report, please contact: info@altairalang.com

This publication is also available online at the Altair & Alang website: www.altairalang.com/featured-insights

1. KEY THEMES

1. Quantum Computing – The Next Frontier
Exploring the use cases of quantum computing as a new wave of innovation in financial services and assessing the timeline for the practical adoption of this technology;

2. Quantum Risk: The Fragility of Cryptography and Cyber Resilience
Examining the fundamental threat that quantum computing imposes on the global financial system, the specific systemic risks for FMIs, as well as how regulators and central banks are beginning to frame a coordinated response to quantum risk;

3. Quantum Readiness: The Road to Quantum-Resilient Infrastructure
Mapping the industry's path toward Post-Quantum Cryptography (PQC) readiness and exploring the governance, risk assessment, and transition priorities FMIs should look to adopt today in order to safeguard operational resilience and maintain trust in the post-quantum era.

2. QUANTUM COMPUTING - THE NEXT FRONTIER

Quantum Computing as a Transformative Technology: Quantum computing has a significant upside for reshaping the fundamentals of our global financial systems.

Background:
Quantum computers use qubits, instead of classical computers' reliance on bits (0 or 1), which allows simultaneous existence in multiple states. Qubits follow the superposition principle where they can exist as both "0" and "1" at the same time, in addition to state of "0" or "1". This unlocks parallel computation on an unprecedented scale when combined with entanglement and quantum interference.

Evolution recap of financial innovation:
The Bank of England[1] has characterised quantum computing as part of the "fourth wave" of financial innovation, following:

1. The digitization of payments and mobile finance post the 2008 financial crisis
2. The rise of blockchain and Distributed Ledger Technology (DLT)
3. The adoption of Artificial Intelligence (AI) / Machine Learning (ML) in market analytics and supervision

The 4th wave is broadly expected to amplify and enhance the predictive and analytical power of AI and ML models, thus enabling faster, deeper, and more adaptive risk intelligence.

Potential Benefits for Financial Services Firms:

- Portfolio optimisation and risk simulations: quantum computing could perform complex Monte Carlo simulations within milliseconds, optimising collateral and margining decisions in near real-time

1 https://www.bankofengland.co.uk/report/2025/the-boes-approach-to-innovation-in-ai-dlt-quantum-computing

- Credit and liquidity risk modelling: quantum computing-enhanced algorithms could analyse thousands of correlated exposures simultaneously. Thus, this would refine market participants' stress-testing capabilities
- Cyber Resilience and fraud detection: When harnessed securely, quantum computing could empower more sophisticated anomaly detection and data encryption techniques

Trajectory Prediction and Strategic Implication for FMIs:

- There is still no consensus on when commercially viable quantum computers will emerge, however, it is expected to be a transitional approach. Nonetheless, progress in quantum error correction and scalable quantum architectures indicate a more compressed timeline than expected. This could take place within this decade rather than in several decades, as previous predication models indicated.
- CCPs and clearing members must treat quantum computing as an emerging strategic inflection point rather than distant technology. It could reshape market structures, risk management frameworks, and operational resilience over the next 5 – 10 years.

3. QUANTUM RISK: THE FRAGILITY OF CRYPTOGRAPHY AND CYBER RESILIENCE

The Fundamental Threat:

Quantum computing poses one of the most profound cybersecurity challenges ever faced by the financial system. In today's interconnected world, we cannot speak about quantum computing, AI and Cyber separately. We believe these issues remain interconnected and must be jointly discussed. Essentially, the core issue lies in encryption. Our modern-day financial ecosystem relies on asymmetric cryptography, primarily Rivest-Shamir-Adleman (RSA) (the well-known, public-private key encryption/decryption method), and Elliptic Curve Cryptography (ECC). These two cryptographies derive security from the computational difficulty of factoring large numbers or solving discrete logarithm.

A capable quantum computer could use Shor's Algorithm (a quantum algorithm for finding the prime factors of an integer, developed 1994, American mathematician Peter Shore) to solve the encryption almost instantaneously, breaking all modern public-key cryptography in the financial system. This would make all current digital certificates, authentication keys, and secure communications obsolete.

Systemic Risks for FMIs:

- *"Harvest Now, Decrypt Later" (HNDL)*: Adversaries could harvest and archive encrypted clearing data today but decrypt it once quantum capabilities mature. This would potentially expose decades of financial records.
- *Operational Resilience Fragmentation*: Uneven adoption of quantum-safe cryptography across market participants could create weak links within multi-party clearing and settlement ecosystems. Broad reliance on third-party providers can pose cliff-hanging risks.
- *Market Stability Risks*: When quantum computing comes to play, ultra-fast, quantum-enhanced trading algorithms could emerge in unsystematic fashion. Thus, traditional price discovery

mechanism could be distorted, impacting order book stability, liquidity provisions, and market volatility.

- *AI-Driven Exploits*: Quantum computing with advanced AI could supercharge cyberattacks and other advanced persistent threats (APT), enabling autonomous and adaptive cyber events against core FMIs and other market participants.

Regulatory Perspectives and Strategic Implication for FMIs

- The BoE, Bank for International Settlements (BIS)[2], and the UK National Cyber Security Centre (NCSC)[3] have all issued early warnings: financial stability could be jeopardized if cryptographic transitions are not initiated well before quantum computers reach critical capability.
- The Dubai Financial Services Authority (DFSA)'s Cyber and AI Resilience Report[4] emphasizes that the financial sector, while supported by strong governance and prudential standards, still have big gaps in supporting the transition to quantum resilience. In their view, Advanced Encryption Standard (AES), generally viewed as a quantum-safe solution, can also be at risk.
- The NCSC has published a timeline urging firms to[5]:
  - Have quantum transition plans in place by 2028
  - Protect high-priority systems with Post-Quantum Cryptography (PQC) by 2031
  - Complete the transition to quantum-safe architecture by 2035
- FMIs must treat quantum risk as a systemic operational resilience issue, not merely a technology advancement.

- **FMIs should:**
  - Map out cryptographic asset inventory to highlight pockets where "Harvest Now, Decrypt Later" risks prevail
  - Stress-test all related internal systems against quantum threat and review their third-party providers' capabilities
  - Develop a coordinated industry playbook to ensure synchronisation across market participant

4. QUANTUM READINESS: THE ROAD TO QUANTUM-RESILIENT INFRASTRUCTURE

Post-Quantum Cryptography (PQC)

Industry leaders are praising PQC as the answer to future risks posed by quantum computing. PQC is a new generation of cryptographic algorithms designed to withstand attacks from both classical and quantum computers. These rely on mathematical problems (lattice-based, hash-based, and multivariate polynomial constructions) that are believed to be unsolvable with quantum resources.

2 https://www.bis.org/publ/othp67.pdf
3 https://www.ncsc.gov.uk/pdfs/blog-post/migrating-to-post-quantum-cryptography-pqc.pdf
4 https://www.dfsa.ae/news/new-dfsa-report-explores-regulatory-insights-cybersecurity-artificial-intelligence-and-quantum-risks
5 https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

Transitioning to PQC is a complex and time-consuming process, which involves extensive planning, resource allocation, and coordination with various stakeholders. Organisations should have a sense of urgency to kickstart the pathway to PQC readiness.

PQC Readiness Pathway:

- Awareness & Inventory
  - Identify quantum-vulnerable cryptographic systems and build a cryptographic inventory
  - Inventory should tack cryptographic algorithm and keys, data ownership, usage, and lifecycle management
- Risk Assessment & Roadmap
  - Evaluate quantum vulnerability of all cryptographic asset across different algorithms and take encrypted data's shelf life and quantum computing's advancement into consideration
  - Define ownership for quantum transition planning, including a hybrid scheme during the transition while classical and PQC would co-exist
- Prioritisation & Resource Management
  - High-risk areas where long-term value data and critical cryptographic mechanisms reside should be prioritised
  - Systems that protect long-lived and sensitive data or have extensive third-party service provider dependencies should be prioritised
- Migration & Remediation
  - Migration of systems to quantum-safe algorithms need to be coordinated among all stakeholders and aligned on agreed standards, timelines, and test plans
  - Financial institutions must ensure owning crypto-agile systems that can adapt to future cryptographic requirements and quantum threats

The quantum shift demands collective action and forward-looking governance, requiring both technological oversight and cross sector collaboration.

Governing Body Leadership:

- The BoE's innovation framework emphasises engagement with industry innovators to assess quantum readiness, to map out quantum technologies' practical implications, and to build relationship with the quantum technology ecosystem
- Collaboration should span beyond domestic border and across participant's role in the market. The BoE[6], for example, is closely working with NCSC, National Quantum Computing Centre, G7, Organisation for Economic Co-operation and Development, and BIS

Industry Priorities for FMIs:

- Develop and recruit talents and expertise, and establish quantum steering committees within current governance frameworks
- Conduct joint scenario analyses simulating post-quantum cyber incidents regularly, and actively monitor the quantum timeline
- Embed quantum computing into broader digital transformation strategies (AI, DLT)
- Review both in-house and third-party service providers' capabilities in quantum resilience; foster public-private communication channels to ensure innovation from both sides are interoperable.

[6] https://www.bankofengland.co.uk/report/2025/the-boes-approach-to-innovation-in-ai-dlt-quantum-computing

5. ABOUT US

Altair & Alang is a boutique UK-based management consulting firm with a global footprint, serving clients across EMEA, APAC, and the Americas. We specialise in business intelligence, financial strategy, and actionable insights tailored to our client's needs. We partner with clients to uncover data-driven opportunities, optimise financial performance, and empower strategic decision-making.

We have worked with over 60 central counterparties (CCPs) worldwide, supporting them on a diverse range of initiatives. Our team has been directly involved in enhancing market transparency standards, advising both CCPs and global regulators. This unique experience positions us as a trusted partner to FMI's seeking to meet international standards while delivering meaningful improvements to governance, resilience, strategies, and stakeholder confidence in the global financial markets.

While our roots are in the financial services and capital markets, our strength lies in data and analytics that translate across all industries. We bring deep functional expertise to a wide range of sectors, including fintech, insurance and cybersecurity. Whether optimising operating models, designing scalable data strategies, or enhancing regulatory insight, we help clients make smarter decisions and deliver measurable results in dynamic environments.

Our deliverables combine deep industry knowledge with advanced analytics to deliver impactful solutions that drive measurable results and long-term success for our clients.

For more information, please contact us: info@altairalang.com

Our website: www.altairalang.com/featured-insights

ALTAIR & ALANG

www.altairalang.com
Strategy ⮡ Consulting ⮡ Redefined