Crypto & TradFi

Special Edition - Quantum: ACPR, G7 and ESMA face the cryptographic threat

Deciphering the regulations for investors

From Law to Cryptography

Previous editions of our Regulatory Brief have described how Europe is restructuring its regulation of artificial intelligence (Seqlense Regulatory Brief 7) and linking it to data protection (Seqlense Regulatory Brief 8). This ninth edition tackles another infrastructure issue, one that has been largely overlooked but is now identified as a priority by financial authorities: the financial sector's transition to post-quantum cryptography.

Three successive publications, within the space of less than four weeks, have transformed this 'research horizon' topic into an operational project. On 23 April 2026, the ACPR published a communication inviting French financial institutions to begin preparing for the migration immediately. On 11 May 2026, the G7 central banks, meeting within the Quantum Technologies Working Group (QTWG) co-chaired by the Banque de France and the Bank of Canada, published their first joint report, "Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants". On 13 May 2026, ESMA published a TRV analysis entitled "Quantum computing in financial markets: applications, investments and prospects", accompanied by a webinar scheduled for 2 June 2026.

This convergence is no coincidence. It reflects a shift in institutional thinking: the quantum threat is no longer treated as a theoretical cybersecurity issue, but as a matter of operational resilience and financial stability, to be addressed using the familiar tools of the supervisor, such as governance, risk mapping, technology investment plans and business continuity requirements. This framework aligns directly with the DORA framework, which has been in force since 17 January 2025.

For both investors and regulated entities, the emerging timeline is now clear: migration of critical systems by 2030–2032 (according to the G7 Cyber Expert Group's roadmap published in January 2026 and relayed by the Banque de France on 19 January 2026), followed by other systems by 2035. This trajectory is consistent with the European roadmap for the transition to post-quantum cryptography. This edition offers an integrated analysis of these three publications, as well as the technological context and practical implications for the financial sector.

The main signal

Post-quantum cryptography is moving out of the laboratory and into the operational vocabulary of the prudential supervisor.

The new development in spring 2026 is not the quantum threat itself—which has been known since the start of the standardisation process launched by NIST in 2016—but the fact that the ACPR, the French prudential supervisory authority, is now explicitly addressing it as a matter of operational resilience. The term 'crypto-agility' thus enters the supervisor's lexicon, alongside more familiar concepts such as cyber risk governance, IT mapping and technology investment plans.

This lexical shift is an important operational signal. Whereas the quantum threat was previously discussed by technical departments (CISOs, cryptography teams), it **is now being raised to executive level and the risk committee**, on a par with climate risk or AI risk. For senior management, this means placing the issue on their risk governance agenda before it becomes the subject of formal supervisory expectations.

It is also worth noting the approach chosen by the ACPR: a "series of meetings with stakeholders in the financial ecosystem" launched in 2026, supplemented by an explicit invitation to contact the Fintech-Innovation Division. This dialogue-based approach foreshadows what could eventually become a structured supervisory framework, but at this stage, it remains firmly incentive-based rather than prescriptive.

Focus 1: The ACPR's communication of 23 April 2026

On 23 April 2026, the ACPR published a news item entitled "The ACPR raises awareness within the ecosystem to prepare for post-quantum cryptography". This publication is neither a standard nor a recommendation in the official sense, but a structured educational communication outlining the Authority's forward-looking approach to the subject.

The threat described by the ACPR

The ACPR points out that cryptographically relevant quantum computers (CRQCs) are likely, once they reach maturity, to break public-key cryptography and compromise digital signatures or communications. In practical terms, banking or interbank transactions could be intercepted and payment systems compromised.

The Authority has identified **2035** as the likely date for the advent of these relevant quantum computers, a date it refers to as 'Q-day'. However, it immediately highlights a key point: **the threat is already a reality** via the retroactive attack mechanism known as 'Harvest now, decrypt later'; encrypted data stolen today could be decrypted later, after Q-day, using quantum computers. This logic means we must focus not on the date of the quantum computer's arrival, but on the **lifespan of data sensitivity**: payment transactions have a shorter sensitivity period than contractual documents, for example.

The solution: post-quantum cryptography (PQC)

The ACPR highlights an important practical point: post-quantum cryptography algorithms can be deployed on computers with classical architecture. Resilience to the quantum threat can therefore be prepared for right now, by implementing a project to adapt information systems. Several algorithms have already been selected by standardisation bodies. NIST launched its process in 2016, selected four algorithms in 2022, published draft versions in 2023, and then finalised the first three standards in August 2024: ML-KEM (derived from CRYSTALS-Kyber), ML-DSA (derived from CRYSTALS-Dilithium) and SLH-DSA (derived from SPHINCS+). Falcon, renamed FN-DSA, remains in the standardisation process.

The six operational challenges of a PQC migration project

The ACPR details the specific challenges of a PQC migration project, which, in practice, form an applicable roadmap:

- **Internal awareness-raising among decision-makers**: moving the issue from the technical level to the executive level.
- **Inventory of cryptographic resources** to be migrated and assessment of the sensitivity lifecycle of confidential data.
- **Prioritising tasks**, in a context where the entire information system is potentially affected.
- **Crypto-agility**: the ability to quickly replace, if necessary, post-quantum algorithms that do not yet have a production track record with new, more resilient ones.
- **Hybridisation**: the ability to simultaneously maintain classical cryptographic algorithms alongside new post-quantum algorithms, in the event of the latter failing.
- **Coordination with the authorities**, to align with national and international roadmaps.
-

Efforts already underway since 2022

The ACPR notes that both the Banque de France and the ACPR have been working on these issues since 2022. In particular, in 2026 the Authority launched a series of discussions with stakeholders in the financial ecosystem, in addition to its participation in European supervisory initiatives. The Fintech-Innovation Division has been designated as the point of contact for stakeholders wishing to engage with the ACPR on this subject.

Impact on financial stakeholders

- For **banks and insurers**, the subject must be placed on the agenda of the operational risk committee or the technology committee, ideally integrated into the ICT mapping as defined by DORA. A presentation to the Executive Committee at least once a year is becoming a best practice for proactive management.
- **The cryptographic inventory** is the most urgent investment: without a precise mapping of cryptographic dependencies (where, which algorithm, what sensitivity lifespan), no

prioritisation is possible. Stakeholders who do not yet have an inventory should launch this project as early as 2026.

- For **MiCA CASPs and cryptographic stakeholders**, the issue ties directly into DORA: cryptographic assets are, by design, dependent on signature schemes that could be vulnerable to quantum attacks. The long-term credibility of a protocol now hinges on its PQC strategy.

Focus 2: The first report from the G7 Quantum Technologies Working Group (11 May 2026)

On 11 May 2026, the G7 Central Banks' Quantum Technologies Working Group (QTWG), co-chaired by the Banque de France and the Bank of Canada, published its first public report: 'Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants'.

Origins and composition of the group

The QTWG was established in June 2025, following the G7 summit in Kananaskis and the "Kananaskis Common Vision for the Future of Quantum Technologies" declaration of 17 June 2025. It is a multi-year working group mandated to examine the implications of quantum technologies for central banks and the financial system. In addition to the Banque de France and the Bank of Canada (co-chairs), it comprises the Deutsche Bundesbank, the Bank of England, the Banca d'Italia, the Bank of Japan, the Federal Reserve Board and the European Central Bank. The co-chairs report on the group's progress to the G7 finance ministers and central bank governors.

Scope and approach of the report

The report adopts an explicitly non-prescriptive stance: it does not set out regulatory expectations nor does it recommend specific courses of action. Instead, it proposes what the group describes as a 'structured analytical framework' for assessing the areas where quantum technologies and financial infrastructure intersect.

The report goes beyond the purely cryptographic angle to cover three families of quantum technologies:

- **Quantum computing** and its potential applications in the financial sector (portfolio optimisation, simulation, risk modelling, quantum machine learning).
- **Cryptographic security**, i.e. the threat to current algorithms and the need for a transition to PQC.
- **Quantum sensors** (quantum sensing), a field that is less exposed but which could have precision applications in certain infrastructures.

Four key messages

- Quantum technologies could **call into question certain cryptographic security assumptions** on which payments, digital transactions and financial data are based.
- The risk of **"harvest now, decrypt later"**, already identified by the ACPR, is highlighted as a long-term confidentiality issue, particularly relevant for financial data with a high sensitivity duration (contractual documents, banking records, life insurance files).
- The **timeline remains uncertain**, but the nature and scope of the transformation are now mapped out with sufficient precision to structure the public-private dialogue.
- The report mentions the **potential opportunities** associated with quantum technologies (information processing, solving complex problems) — an important point to ensure the subject is not reduced to its defensive dimension alone.

Alignment with the G7 CEG roadmap of January 2026

The QTWG report differs from the G7 Cyber Expert Group (CEG) published in January 2026, announced by the US Treasury on 12 January 2026 and relayed by the Banque de France on 19 January 2026, which focused specifically on coordinating the transition to post-quantum cryptography with a migration timeline from 2030 to 2035. The QTWG report takes a broader view, covering quantum computing, cryptographic security and quantum sensors, as well as sector-level systemic dependencies. The two publications are complementary: the first sets out an operational agenda, whilst the second provides a framework for analysis.

Impact for investors and asset managers

- For **portfolios exposed to market infrastructure** (clearing houses, central securities depositories such as Euroclear, payment platforms such as DTCC or SWIFT), counterparties' PQC roadmaps are becoming a key element of operational due diligence.
- For **technology investors**, the report sheds light on a long-term theme: the PQC migration is a multi-year investment cycle that will benefit players in cybersecurity, cryptographic infrastructure and cryptographic audit solutions.
- For **quantitative management firms**, the 'opportunity' aspect of quantum computing (portfolio optimisation, risk modelling) opens up prospects for innovation in the longer term, but which, according to the report, will remain experimental and far removed from commercial applications in the short term.

Focus 3: The ESMA TRV analysis of 13 May 2026

Two days after the publication of the G7 QTWG report, on 13 May 2026, ESMA published an analysis included in its TRV Risk Analysis (reference ESMA50-481369926-33801) entitled "Quantum computing in financial markets: applications, investments and prospects". A webinar to present the analysis is scheduled for 2 June 2026.

Four key findings from ESMA

- Quantum technologies **remain at an early stage**, but the ecosystem is developing rapidly.
- **Investment in quantum start-ups has risen sharply since 2020**, although it remains significantly lower than the amounts invested in generative AI.
- The financial applications of quantum computing (modelling, portfolio optimisation, quantum machine learning) are currently **experimental and far from commercial use**, according to the findings of ESMA's TRV report for the first half of 2026.
- The **transition to post-quantum cryptography** is described as an urgent, multi-year project to preserve digital security and confidence in the financial system.

The scope of the ESMA analysis

The ESMA analysis examines five areas of interaction between quantum technologies and financial markets: financial modelling, portfolio optimisation, quantum machine learning, cybersecurity and post-quantum cryptography. This perspective is particularly relevant for market infrastructure and asset management players, who are both potential users

(opportunity side) and exposed (risk side).

Specific implications for financial markets

- For **trading platforms, post-trade infrastructures and central securities depositories**, the issue is now on the agenda of the European market regulator. Particular attention will be paid to the cryptographic resilience of settlement and account-keeping systems.
- For **asset managers and investment funds** exposed to technology-related themes, the ESMA report provides an analytical framework for assessing the actual maturity of the quantum market, rather than commercial promises.
- For **blockchain players and CASPs**, ESMA's analysis confirms the urgency—already highlighted by the ACPR—of cryptographic migration to preserve the long-term integrity of protocols.

Cross-cutting reading: quantum, tokenisation and resilience

Three key themes emerge from a combined reading of the ACPR, G7 QTWG and ESMA publications, and their connection to ongoing work on tokenisation and the DORA framework.

Cryptographic resilience is becoming a supervisory focus

The appearance of the term 'crypto-agility' in the ACPR's vocabulary marks a change in status. Whereas cryptography was previously treated as a technical component relating to architectural choices, it is now becoming a subject of supervision in its own right, to be integrated into risk

mapping within the meaning of DORA. This implies an explicit link between the security (CISO), compliance, internal control and business continuity functions.

The convergence of quantum computing and tokenisation is taking shape

Project Pythagore, launched by the Banque de France and Euroclear on 10 October 2025 for the tokenisation of NEU CP, in a market worth around €310 billion, relies, like any DLT system, on cryptographic schemes that may be affected by the quantum threat. A tokenised infrastructure must therefore be designed from the outset with future PQC migrations in mind, which ties in with the concept of **crypto-agility by design**. The project's pilot phase, expected in late 2026, will be scrutinised in this regard.

The quantum opportunity remains a long-term prospect

The assessment shared by ESMA and the G7 QTWG is unambiguous: the financial applications of quantum computing remain experimental. Investment in the sector, which has been growing strongly since 2020, remains modest compared to that in generative AI. For investors, this observation calls for a clear distinction to be made between the defensive dimension (PQC migration, which is an immediate priority) and the offensive dimension (the use of quantum computing for competitive advantage, which remains a longer-term prospect).

Main sources

- ACPR, *"ACPR raises awareness within the ecosystem to prepare for post-quantum cryptography"*, news item published on 23 April 2026, acpr.banque-france.fr.
- Banque de France / ACPR, *"Statement on the progress of a coordinated roadmap for the transition to post-quantum cryptography in the financial sector"*, 19 January 2026.
- G7 Cyber Expert Group, Quantum Roadmap for the Financial Sector, January 2026; US Treasury press release of 12 January 2026 and Banque de France statement of 19 January 2026.
- G7 Quantum Technologies Working Group, *Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants*, report published on 11 May 2026 by the Banque de France (co-chaired with the Bank of Canada).
- Deutsche Bundesbank, institutional page *"G7 Quantum Technologies Working Group"*
- G7 Summit, *Kananaskis Common Vision for the Future of Quantum Technologies*, 17 June 2025.
- ESMA, *"Quantum computing in financial markets: applications, investments and prospects"*, TRV Risk Analysis, reference ESMA50-481369926-33801, published on 13 May 2026. Webinar scheduled for 2 June 2026.
- ESMA, *Trends, Risks and Vulnerabilities (TRV) Report No. 1, 2026*, published on 11 March 2026.

- Banque de France & Euroclear, press release on *Project Pythagore*, a joint initiative to tokenise NEU CP, launched on 10 October 2025.
- Denis Beau (Banque de France), speech on the market for negotiable debt securities (BIS Review), December 2025.
- NIST, *Post-Quantum Cryptography Standardization Project* (csrc.nist.gov/projects/post-quantum-cryptography).
- ANSSI / Cyber.gouv.fr, *FAQ on post-quantum cryptography* (reference cited by the ACPR).
- Regulation (EU) 2022/2554 (DORA), applicable from 17 January 2025 — digital operational resilience framework for the financial sector.