Crypto &TradFi

Spécial Quantique : ACPR, G7 et ESMA face à la menace cryptographique

Décrypter la réglementation pour les investisseurs

Du droit à la cryptographie

Les éditions précédentes de notre Regulatory Brief ont décrit comment l'Europe restructure sa régulation de l'intelligence artificielle (Seqlense Regulatory Brief 7) et l'articule avec la protection des données (Seqlense Regulatory Brief 8). Cette neuvième édition s'attaque à un autre sujet d'infrastructure, silencieux mais désormais identifié comme une priorité par les autorités financières : la transition du secteur financier vers la cryptographie post-quantique.

Trois publications successives, en l'espace de moins de quatre semaines, ont transformé ce sujet d'« horizon de recherche » en un chantier opérationnel. Le 23 avril 2026, l'ACPR a publié une communication invitant les institutions financières françaises à se préparer dès maintenant à la migration. Le 11 mai 2026, les banques centrales du G7, réunies au sein du Quantum Technologies Working Group (QTWG) co-présidé par la Banque de France et la Bank of Canada, ont publié leur premier rapport conjoint, « Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants ». Le 13 mai 2026, l'ESMA a publié une analyse TRV intitulée « Quantum computing in financial markets: applications, investments and prospects », accompagnée d'un webinaire prévu le 2 juin 2026.

La convergence n'est pas fortuite. Elle traduit une bascule institutionnelle : la menace quantique n'est plus traitée comme un sujet théorique de cybersécurité, mais comme une question de résilience opérationnelle et de stabilité financière, à traiter avec les outils familiers du superviseur, tels que la gouvernance, la cartographie des risques, les plans d'investissement technologique et les exigences de continuité d'activité. Cette grille de lecture s'aligne directement sur le cadre DORA, applicable depuis le 17 janvier 2025.

Pour les investisseurs comme pour les acteurs régulés, le calendrier qui se dessine est désormais explicite : migration des systèmes critiques à l'horizon 2030-2032 (selon la feuille de route du G7 Cyber Expert Group publiée en janvier 2026 et relayée par la Banque de France le 19 janvier 2026), puis des autres systèmes d'ici 2035. Cette trajectoire est cohérente avec la feuille de route européenne pour la transition vers la cryptographie post-quantique. Cette édition propose une lecture intégrée de ces trois publications, ainsi que du contexte technologique et des implications pratiques pour le secteur financier.

Le signal faible

La cryptographie post-quantique sort du laboratoire et entre dans le vocabulaire opérationnel du superviseur prudentiel.

L'élément nouveau du printemps 2026 n'est pas la menace quantique elle-même, connue depuis l'origine du processus de standardisation lancé par le NIST en 2016, mais le fait que l'ACPR, autorité de supervision prudentielle française, l'aborde désormais explicitement comme un sujet de résilience opérationnelle. Le terme « crypto-agilité » entre ainsi dans le langage du superviseur, aux côtés de notions plus familières comme la gouvernance du risque cyber, la cartographie des SI et les plans d'investissement technologique.

Cette acculturation lexicale constitue un signal opérationnel important. Là où la menace quantique était jusqu'ici discutée par les directions techniques (CISO, équipes cryptographie), elle **remonte désormais au niveau exécutif et au comité des risques**, au même titre que le risque climatique ou le risque IA. Pour les directions générales, cela suppose d'inscrire le sujet à l'agenda de leur gouvernance des risques avant qu'il ne fasse l'objet d'attentes supervisorielles formalisées.

Il faut également noter le mode d'engagement choisi par l'ACPR : un « cycle d'entretiens avec les acteurs de l'écosystème financier » lancé en 2026, complété par une invitation explicite à contacter le Pôle Fintech-Innovation. Cette approche dialogique préfigure ce que pourrait devenir, à terme, un cadre supervisoriel structuré, mais à ce stade, elle reste résolument incitative et non prescriptive.

Focus 1 : La communication de l'ACPR du 23 avril 2026

Le 23 avril 2026, l'ACPR a publié une actualité intitulée « L'ACPR sensibilise l'écosystème à se préparer à la cryptographie post-quantique ». Cette publication n'est pas une norme ni une recommandation au sens du registre officiel, mais une communication pédagogique structurée qui dessine la doctrine prospective de l'Autorité sur le sujet.

La menace décrite par l'ACPR

L'ACPR rappelle que les ordinateurs quantiques cryptographiquement pertinents (Cryptographically Relevant Quantum Computer, CRQC) sont susceptibles, lorsqu'ils auront atteint leur maturité, de casser les clefs de cryptographie publique et de compromettre les signatures numériques ou les communications. Concrètement, les transactions bancaires ou interbancaires pourraient être interceptées et les systèmes de paiement compromis.

L'Autorité retient l'horizon **2035** comme le moment probable de l'avènement de ces ordinateurs quantiques pertinents, ce qu'elle désigne par l'expression « Q-day ». Mais elle souligne immédiatement un point clé : **la menace est d'ores et déjà effective** via le mécanisme d'attaque rétroactive « Harvest now decrypt later » ; des données chiffrées subtilisées aujourd'hui pourraient être déchiffrées plus tard, après le Q-day, grâce aux ordinateurs quantiques. Cette logique impose de raisonner non pas sur la date d'apparition de l'ordinateur quantique, mais sur la **durée de vie de la sensibilité des données** : les transactions de paiement ont une durée de sensibilité plus courte que les documents contractuels, par exemple.

La solution : la cryptographie post-quantique (PQC)

L'ACPR souligne un point pratique important : les algorithmes de cryptographie post-quantique peuvent être déployés sur les ordinateurs d'architecture classique. La résilience à la menace quantique peut donc se préparer dès maintenant, en mettant en œuvre un projet d'adaptation des systèmes d'information. Plusieurs algorithmes ont déjà été retenus par les organismes de standardisation. Le NIST a lancé son processus en 2016, sélectionné quatre algorithmes en 2022, publié des versions provisoires en 2023, puis finalisé en août 2024 trois premiers standards : ML-KEM (issu de CRYSTALS-Kyber), ML-DSA (issu de CRYSTALS-Dilithium) et SLH-DSA (issu de SPHINCS+). Falcon, renommé FN-DSA, reste en cours de standardisation.

Les six enjeux opérationnels d'un projet de migration PQC

L'ACPR détaille les enjeux spécifiques d'un projet de migration PQC, qui forment, en pratique, une feuille de route applicable :

- La **sensibilisation interne des décideurs** : passage du sujet du niveau technique au niveau exécutif.
- L'**inventaire des ressources cryptographiques** à migrer et l'évaluation de la durée de vie de sensibilité des données confidentielles.
- La **priorisation des tâches**, dans un contexte où l'intégralité du système d'information est potentiellement impactée.
- La **crypto-agilité** : la capacité à remplacer rapidement, en cas de besoin, des algorithmes post-quantiques qui n'ont pas encore d'historique de production par de nouveaux plus résilients.
- L'**hybridation** : la capacité à maintenir simultanément des algorithmes de cryptographie classiques avec les nouveaux algorithmes post-quantiques, en cas de défaillance de ces derniers.
- La **coordination avec les autorités**, pour s'aligner sur les feuilles de route nationales et internationales.
-

Une mobilisation déjà engagée depuis 2022

L'ACPR rappelle que la Banque de France et elle-même sont mobilisées sur ces enjeux depuis 2022. L'Autorité a notamment entamé en 2026 un cycle d'entretiens avec les acteurs de l'écosystème financier, en complément de sa participation aux initiatives des superviseurs européens. Le Pôle Fintech-Innovation est désigné comme point de contact pour les acteurs souhaitant échanger avec l'ACPR sur ce sujet.

Impact pour les acteurs financiers

- Pour les **établissements bancaires et assureurs**, le sujet doit être inscrit à l'agenda du comité des risques opérationnels ou du comité technologique, idéalement intégré à la cartographie ICT au sens de DORA. Une présentation au moins annuelle au COMEX devient une bonne pratique anticipative.
- L'**inventaire cryptographique** est l'investissement le plus urgent : sans cartographie précise des dépendances cryptographiques (où, quel algorithme, quelle durée de vie de sensibilité), aucune priorisation n'est possible. Les acteurs qui n'ont pas encore d'inventaire devraient lancer ce chantier dès 2026.
- Pour les **CASPs MiCA et les acteurs crypto**, la question rejoint directement DORA : les actifs cryptographiques dépendent par construction de schémas de signature qui pourraient être vulnérables aux attaques quantiques. La crédibilité long terme d'un protocole tient désormais à sa stratégie PQC.

Focus 2 : Le premier rapport du G7 Quantum Technologies Working Group (11 mai 2026)

Le 11 mai 2026, le Quantum Technologies Working Group (QTWG) des banques centrales du G7, co-présidé par la Banque de France et la Bank of Canada, a publié son premier rapport public : « Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants ».

Genèse et composition du groupe

Le QTWG a été établi en juin 2025, à la suite du sommet G7 de Kananaskis et de la déclaration « Kananaskis Common Vision for the Future of Quantum Technologies » du 17 juin 2025. Il s'agit d'un groupe de travail pluriannuel mandaté pour examiner les implications des technologies quantiques pour les banques centrales et le système financier. Outre la Banque de France et la Bank of Canada (co-présidence), il réunit la Deutsche Bundesbank, la Bank of England, la Banca d'Italia, la Bank of Japan, le Federal Reserve Board et la Banque centrale européenne. Les co-présidents rendent compte de l'avancement du groupe aux ministres des Finances et gouverneurs de banques centrales du G7.

Périmètre et posture du rapport

Le rapport adopte une posture explicitement non prescriptive : il n'établit pas d'attentes réglementaires et ne recommande pas de cours d'action spécifiques. Il propose plutôt ce que le groupe qualifie de « cadre analytique structuré » permettant d'évaluer les zones d'intersection entre technologies quantiques et infrastructures financières.

Le rapport va au-delà du seul angle cryptographique pour couvrir trois familles de technologies quantiques :

- Le **calcul quantique** et ses applications potentielles dans le secteur financier (optimisation de portefeuille, simulation, modélisation de risques, machine learning quantique).

- La **sécurité cryptographique**, c'est-à-dire la menace pesant sur les algorithmes actuels et la nécessité d'une migration PQC.
- Les **capteurs quantiques** (quantum sensing), domaine moins exposé mais qui pourrait avoir des applications de précision dans certaines infrastructures.

Quatre messages structurants

- Les technologies quantiques pourraient **remettre en cause certaines hypothèses de sécurité cryptographique** sur lesquelles reposent les paiements, les échanges numériques et les données financières.
- Le risque de **« harvest now, decrypt later »**, déjà identifié par l'ACPR, est rappelé comme un enjeu de confidentialité de long terme, particulièrement pertinent pour les données financières dont la durée de sensibilité est élevée (documents contractuels, archives bancaires, dossiers d'assurance vie).
- Le **calendrier reste incertain**, mais la nature et la portée de la transformation sont désormais cartographiées avec une précision suffisante pour structurer le dialogue public-privé.
- Le rapport mentionne les **opportunités potentielles** liées aux technologies quantiques (traitement de l'information, résolution de problèmes complexes) — un point important pour ne pas réduire le sujet à sa seule dimension défensive.

Articulation avec la feuille de route G7 CEG de janvier 2026

Le rapport QTWG se distingue de la feuille de route du G7 Cyber Expert Group (CEG) publiée en janvier 2026, annoncée par le Trésor américain le 12 janvier 2026 et relayée par la Banque de France le 19 janvier 2026, qui se concentrait spécifiquement sur la coordination de la transition vers la cryptographie post-quantique avec un calendrier de migration de 2030 à 2035. Le rapport QTWG adopte une lentille plus large couvrant le calcul quantique, la sécurité cryptographique et les capteurs quantiques, ainsi que les dépendances systémiques au niveau du secteur. Les deux publications sont complémentaires : la première fixe un agenda opérationnel, la seconde structure un cadre d'analyse.

Impact pour les investisseurs et les gestionnaires d'actifs

- Pour les **portefeuilles exposés aux infrastructures de marché** (chambres de compensation, dépositaires centraux comme Euroclear, plateformes de paiement comme DTCC ou SWIFT), la roadmap PQC des contreparties devient un élément de due diligence opérationnelle.
- Pour les **investisseurs technologiques**, le rapport éclaire un thème de long terme : la migration PQC est un cycle d'investissement pluriannuel qui bénéficiera aux acteurs de la cybersécurité, des infrastructures cryptographiques et des solutions d'audit cryptographique.

- Pour les **acteurs de la gestion quantitative**, la dimension « opportunité » du calcul quantique (optimisation de portefeuille, modélisation de risques) ouvre une perspective d'innovation à plus longue échéance, mais qui restera, selon le rapport, expérimentale et éloignée d'usages commerciaux à court terme.

Focus 3 : L'analyse ESMA TRV du 13 mai 2026

Deux jours après la publication du rapport G7 QTWG, l'ESMA a publié le 13 mai 2026 une analyse intégrée à son TRV Risk Analysis (référence ESMA50-481369926-33801) intitulée « Quantum computing in financial markets: applications, investments and prospects ». Un webinaire de présentation est programmé pour le 2 juin 2026.

Quatre constats de l'ESMA

- Les technologies quantiques **restent à un stade précoce**, mais l'écosystème se développe rapidement.
- Les **investissements dans les startups quantiques ont fortement augmenté depuis 2020**, même s'ils restent significativement inférieurs aux montants investis dans l'IA générative.
- Les applications financières du calcul quantique (modélisation, optimisation de portefeuille, machine learning quantique) sont aujourd'hui **expérimentales et éloignées d'usages commerciaux**, selon le constat partagé du TRV report de l'ESMA pour le premier semestre 2026.
- La **migration vers la cryptographie post-quantique** est qualifiée de chantier urgent et pluriannuel pour préserver la sécurité numérique et la confiance dans le système financier.

Le périmètre d'analyse ESMA

L'analyse ESMA examine cinq zones d'interaction entre technologies quantiques et marchés financiers : la modélisation financière, l'optimisation de portefeuille, le machine learning quantique, la cybersécurité et la cryptographie post-quantique. Cet angle est particulièrement pertinent pour les acteurs des infrastructures de marché et de la gestion d'actifs, qui sont à la fois utilisateurs potentiels (côté opportunité) et exposés (côté risque).

Impact spécifique pour les marchés financiers

- Pour les **plateformes de négociation, les infrastructures post-marché et les dépositaires centraux**, le sujet est désormais inscrit à l'agenda du régulateur des marchés européen. Une attention particulière sera portée à la résilience cryptographique des systèmes de règlement-livraison et de tenue de compte.
- Pour les **gestionnaires d'actifs et les fonds d'investissement** exposés aux thématiques technologiques, le rapport de l'ESMA fournit une grille d'analyse permettant d'évaluer la maturité réelle du marché quantique, plutôt que les promesses commerciales.

- Pour les **acteurs blockchain et les CASPs**, l'analyse de l'ESMA confirme l'urgence, déjà soulignée par l'ACPR, de la migration cryptographique pour préserver l'intégrité des protocoles à long terme.

Lecture transversale : quantique, tokenisation et résilience

Trois lignes de force émergent de la lecture combinée des publications ACPR, G7 QTWG et ESMA, et de leur articulation avec les chantiers en cours sur la tokenisation et le cadre DORA.

La résilience cryptographique devient un objet supervisoriel

L'apparition du terme « crypto-agilité » dans le vocabulaire de l'ACPR marque un changement de statut. Là où la cryptographie était traitée comme un composant technique relevant des choix d'architecture, elle devient un objet de supervision à part entière, à intégrer dans la cartographie des risques au sens de DORA. Cela suppose une articulation explicite entre les fonctions sécurité (CISO), conformité, contrôle interne et continuité d'activité.

La convergence quantique / tokenisation se précise

Le *Project Pythagore*, lancé par la Banque de France et Euroclear le 10 octobre 2025 pour la tokenisation des NEU CP, sur un marché de l'ordre de 310 milliards d'euros, repose, comme tout système DLT, sur des schémas cryptographiques susceptibles d'être affectés par la menace quantique. Une infrastructure tokenisée doit donc être pensée dès la conception en tenant compte des migrations PQC à venir, ce qui rejoint la notion de **crypto-agilité by design**. La phase pilote du projet, attendue fin 2026, sera scrutée à ce titre.

L'opportunité quantique reste à un horizon long

Le constat partagé par l'ESMA et le G7 QTWG est sans ambiguïté : les applications financières du calcul quantique restent expérimentales. L'investissement dans le secteur, en forte croissance depuis 2020, demeure modeste rapporté à celui de l'IA générative. Pour les investisseurs, ce constat invite à distinguer rigoureusement la dimension défensive (migration PQC, qui est un chantier immédiat) de la dimension offensive (utilisation du calcul quantique pour des avantages concurrentiels, qui reste à plus long terme).

Sources principales

- ACPR, *« L'ACPR sensibilise l'écosystème à se préparer à la cryptographie post-quantique »*, actualité publiée le 23 avril 2026, acpr.banque-france.fr.
- Banque de France / ACPR, *« Déclaration relative à l'avancement d'une feuille de route coordonnée pour la transition vers la cryptographie post quantique dans le secteur financier »*, 19 janvier 2026.

- G7 Cyber Expert Group, Quantum Roadmap for the Financial Sector, janvier 2026 ; communiqué du U.S. Treasury du 12 janvier 2026 et déclaration de la Banque de France du 19 janvier 2026.
- G7 Quantum Technologies Working Group, *Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants*, rapport publié le 11 mai 2026 par la Banque de France (co-présidence avec la Bank of Canada).
- Deutsche Bundesbank, page institutionnelle *« G7 Quantum Technologies Working Group »*
- Sommet G7, *Kananaskis Common Vision for the Future of Quantum Technologies*, 17 juin 2025.
- ESMA, *« Quantum computing in financial markets: applications, investments and prospects »*, TRV Risk Analysis, référence ESMA50-481369926-33801, publié le 13 mai 2026. Webinaire programmé pour le 2 juin 2026.
- ESMA, *Trends, Risks and Vulnerabilities (TRV) Report No. 1, 2026*, publié le 11 mars 2026.
- Banque de France & Euroclear, communiqué de presse sur le *Project Pythagore*, initiative conjointe de tokenisation des NEU CP, lancée le 10 octobre 2025.
- Denis Beau (Banque de France), discours sur le marché des titres de créances négociables (BIS Review), décembre 2025.
- NIST, *Post-Quantum Cryptography Standardization Project* (csrc.nist.gov/projects/post-quantum-cryptography).
- ANSSI / Cyber.gouv.fr, *FAQ Cryptographie post-quantique* (référence citée par l'ACPR).
- Règlement (UE) 2022/2554 (DORA), applicable depuis le 17 janvier 2025 — cadre de résilience opérationnelle numérique du secteur financier.