COMPTE RENDU, INNOVATION MEET-UP FINANCE INNOVATION

Finance et quantique : entre menace immédiate et souveraineté à construire

Cryptographie post-quantique, cas d'usage et autonomie stratégique

Date 3 novembre 2026, 9h00 à 11h30 **Lieu** Palais Brongniart, Paris **Format** Présentiel et à distance, une table ronde

MISE EN CONTEXTE

Après la tokenisation et l'IA agentique, le quantique s'impose comme la prochaine frontière pour les acteurs financiers. Finance Innovation, pôle de compétitivité de la filière finance qui fédère environ 400 membres dont 300 fintechs et insurtechs, a réuni des experts du quantique pour confronter leurs regards. Le constat de départ est sans ambiguïté : des données chiffrées aujourd'hui pourraient être déchiffrées demain. La matinée s'est organisée autour de trois axes : la menace immédiate et la crypto-agilité, quelle que soit la date du « Q Day » ; les opportunités ouvertes par l'hybridation entre calcul quantique, calcul classique et IA ; enfin la position de la France et de l'Europe, avec le risque de reproduire la dépendance technologique déjà observée sur l'IA.

OUVERTURE ET INTRODUCTION, 9H30 À 9H45

La deep tech est morte, vive la néo deep tech

Samuel Cohen Directeur du développement, Finance Innovation

Emmanuel Papadacci-Stephanopoli Directeur général délégué, Le Village by CA Paris

TABLE RONDE, 9H45 À 11H00

Menace immédiate, opportunités et souveraineté

ANIMATION

Achraf Ayadi Président, Altavo Partners

Olivier Lantran Responsable du Lab d'innovation, Banque de France

Iordanis Kerenidis Cofondateur et CTO, Quantum Signals ; directeur de recherche, CNRS

Lionel Rigaud Cofondateur et CEO, QbitSoft

EXECUTIVE SUMMARY

Six enseignements à retenir

1 La menace est déjà là

Des données chiffrées peuvent être captées aujourd'hui et déchiffrées plus tard. Toute donnée dont la durée de vie dépasse dix ans est exposée dès maintenant.

2 Le calendrier se précise : 2030, puis 2035

Les feuilles de route du G7, de l'Europe et du NIST convergent vers une migration des systèmes critiques au tournant de 2030 et de l'essentiel du secteur vers 2035. Le secteur n'est pas en avance : il est juste à l'heure, à condition de commencer maintenant.

3 La barre technique baisse plus vite que prévu

On estimait à des millions le nombre de qubits nécessaires pour casser RSA. Des travaux récents le ramèneraient à environ 22 000.

4 Le quantique rapporte déjà en optimisation

Quelques pourcents de gain en logistique ou en allocation de portefeuille, sur des machines existantes. Monte Carlo et cryptanalyse relèvent encore de la recherche.

5 Penser processus métier, pas technologie

Un cas d'usage à ROI mesurable conduit jusqu'en production vaut mieux qu'une preuve de concept. Le quantique devient un outil de plus, à côté de l'IA.

6 La souveraineté se joue sur l'adoption

Recherche et startups européennes sont solides, le passage à l'échelle reste le point faible. Un secteur financier client exigeant est le levier décisif.

Introduction : le quantique, une troisième informatique

Il y aurait neuf chances sur dix que le quantique devienne une filière comparable à l'aéronautique ou au microprocesseur. La deep tech d'hier, qui justifiait dix à quinze ans de déploiement, laisse place à des startups qui doivent réussir leur mise sur le marché en deux à quatre ans. Le quantique en est au stade du microprocesseur des années 80, avec une chaîne de valeur à construire et un enjeu clair : que l'« IBM du quantique » naisse en France. Après la logique procédurale et l'IA, il forme une troisième informatique, adaptée à la combinatoire explosive, aux systèmes où tout dépend de tout et à la détection de structures cachées.

TABLE RONDE, LA MENACE

Protéger dès maintenant le socle de la confiance

Un point d'inflexion

Le quantique n'est ni un accélérateur ni un nouveau type de GPU, mais une autre manière de traiter l'information : certains problèmes n'y gagnent rien, d'autres ont un vrai potentiel. Le basculement viendra de la première application réelle qu'une banque paiera.

Trois risques pour la finance

Le quantique est d'abord une question de confiance, car c'est la cryptographie qui garantit l'origine d'un ordre de paiement ou la confidentialité d'une donnée. Trois risques ressortent. La confidentialité d'abord, car des données interceptées et stockées aujourd'hui pourront être déchiffrées demain. L'authenticité ensuite, toute la finance reposant sur des signatures électroniques. Le risque systémique enfin : un seul maillon non protégé, éditeur, prestataire ou infrastructure de marché, fragilise tout le réseau.

Une feuille de route désormais claire

Les calendriers ont convergé (feuille de route du Cyber Expert Group du G7 publiée en janvier, feuille de route européenne, recommandations de l'ANSSI, standards du NIST) : la ligne d'arrivée se rapproche alors que la course est déjà partie. Les feuilles de route publiques convergent sur cinq actions : porter le sujet au niveau du plan stratégique, et non dans un coin de la DSI ; inventorier où se trouve la cryptographie et quels algorithmes sont utilisés ; prioriser les systèmes sensibles et les données à longue durée de vie ; embarquer les fournisseurs en inscrivant leur feuille de route post-quantique dans les contrats, dans la ligne de DORA ; enfin bâtir une crypto-agilité durable, pour changer d'algorithme au fil de l'eau.

Convaincre des DSI déjà saturées

Comment justifier un ou deux millions d'euros sur une application qui tourne à 99,999 % pour un risque à cinq ou dix ans ? L'argument n'est pas technique mais relève de l'analyse de risque : une signature de virements compromise, c'est une perte totale de confiance. Et la démarche n'a rien de pharaonique. On commence par l'inventaire, les nouvelles applications intègrent d'emblée la cryptographie post-quantique, et il suffit d'ajouter deux cases aux fiches de lancement de projet : algorithme post-quantique et données sensibles.

Un secteur déjà un peu en retard

Le secteur commence à être en retard. L'algorithme de Shor date de 1994 ; il ne manquait que la machine. Les principaux standards post-quantiques reposent sur d'autres problèmes mathématiques, dont les réseaux euclidiens, avec moins de recul que RSA : d'où l'intérêt de l'hybridation et de la crypto-agilité pour rester prêt à de futures évolutions. Or machines et algorithmes progressent ensemble : les ressources estimées pour casser RSA seraient passées de millions de qubits à environ 22 000. Les banques mettant dix ans à migrer, le temps presse.

TABLE RONDE, LES OPPORTUNITÉS

L'optimisation d'abord, l'hybridation avec l'IA ensuite

Ce qui fonctionne déjà

Des algorithmes quantiques prêts à l'emploi sont déjà utilisés au quotidien par des clients payants, sans compétence quantique ni changement de système d'information. Sur des machines existantes, les gains sont réels en optimisation sous contrainte : quelques pourcents de mieux que les solveurs en place sur le transport, des résultats meilleurs ou plus rapides en allocation d'actifs et en chargement de containers, une modélisation plus fine du risque qui réduit le capital immobilisé, de la détection de fraude documentaire sans entraînement préalable. En hyper-clustering, 200 groupes sont obtenus en 30 secondes là où le calcul classique demanderait des siècles. Pour une banque, cela ouvre l'hyper-personnalisation et une segmentation plus fine du risque de crédit, voire du risque systémique.

Mieux optimiser, sans promettre l'optimum

Face à la recherche opérationnelle classique, il faut rappeler que ni le solveur classique ni le quantique ne garantissent l'optimum exact : chacun livre la meilleure solution trouvée à un instant donné. Le quantique pousse plus loin les heuristiques, au prix d'une découpe des problèmes, les machines n'étant pas extensibles à l'infini. Les gains progresseront avec le matériel, à algorithme constant.

IA et quantique, une synergie

Il ne faut pas opposer les deux technologies. Pour les banques, on distingue trois familles de problèmes : les simulations Monte Carlo, dont l'accélération est prouvée mais exige des machines plus grosses ; l'optimisation, où les heuristiques quantiques enrichissent la boîte à outils ; la prédiction de marché, où le quantique peut extraire des structures qu'une IA classique ne voit pas. À terme, un agent choisira lui-même entre IA classique et machine quantique, comme on ignore aujourd'hui si un calcul tourne sur CPU ou GPU.

Un regard lucide

Pour les calculs lourds (scénarios de risque, tests de résistance), ce que le quantique fait mieux aujourd'hui ? Souvent « pas encore », ce qui est déjà utile. Trois chantiers n'attendent pas les machines : les compétences, les approches hybrides et la formulation des problèmes à partir des besoins. Se protéger est urgent, explorer est nécessaire, promettre serait prématuré.

Nouvelles infrastructures : la crypto-agilité dès la conception

Tokenisation d'actifs, règlement en monnaie de banque centrale sur registre distribué, projets de monnaie numérique : ces infrastructures dureront bien au-delà de 2035. Les bâtir sur la cryptographie actuelle créerait une dette de sécurité ; elles doivent donc intégrer dès leur conception la cryptographie post-quantique et la crypto-agilité. Les blockchains sont particulièrement exposées, leurs signatures sur courbes elliptiques pouvant être cassées avec moins de 500 000 qubits selon des travaux de Google, sur une machine qui n'existe pas encore. Les agents IA capables d'initier des paiements devront aussi disposer d'identités et de signatures post-quantiques.

Du POC au Proof of Value

Mieux vaut éviter la preuve de concept coûteuse sans retour sur investissement. Il faut lui préférer un cas d'usage unique, à ROI mesurable, conduit jusqu'en production, dont le gain finance le projet suivant. La grille pour les dirigeants : consacrer une heure non pas au quantique mais à chaque processus métier. L'allocation de portefeuille relève de l'optimisation, donc du quantique ; la fraude carte, qui exige de la réactivité, de l'IA ; la traçabilité, de la blockchain.

TABLE RONDE, LA SOUVERAINETÉ

De l'excellence scientifique au passage à l'échelle

L'autonomie stratégique, trois conditions

La souveraineté n'est pas un gros mot. Maîtriser ses choix technologiques ne signifie pas tout produire soi-même, mais réunir trois conditions : comprendre les standards en participant à leur élaboration, savoir évaluer ce que l'on achète pour ne pas dépendre aveuglément de ses fournisseurs, et garantir la réversibilité. La crypto-agilité est aussi une forme de souveraineté.

Des atouts réels

Les standards post-quantiques du NIST prennent racine dans la recherche européenne. La France dispose d'un écosystème académique de premier plan (CNRS, CEA, Paris-Saclay) et de startups reconnues à l'international, comme Pasqal, Quandela ou Alice & Bob. Le secteur financier peut accélérer leur passage à l'échelle en expérimentant avec des acteurs européens sur des besoins précis et en coopérant, comme sur le post-quantique avec la BRI et Swift : un client exigeant est aussi un levier industriel.

Se fédérer et adopter

Il faut une recherche qui reste ouverte et une fédération des efforts au niveau européen face à des États-Unis portés par Google, IBM, Microsoft ou Amazon. Mais la bataille se joue sur l'adoption plus encore que sur le financement : des normes adoptées par une minorité d'utilisateurs finissent par tomber, et sans clients, les startups disparaissent ou se font racheter.

PERSPECTIVES

Pour agir dès demain

Inscrire la transition post-quantique dans le plan stratégique et lancer l'inventaire cryptographique sans attendre. Prioriser les données à longue durée de vie et embarquer les fournisseurs. Concevoir toute nouvelle infrastructure en crypto-agilité. Côté opportunités, partir d'un processus métier précis, viser un ROI mesurable plutôt qu'une démonstration et expérimenter avec des acteurs européens.

Prochain rendez-vous InsurDay, le 19 novembre 2026.

À noter La Banque de France organise le 27 novembre la conférence internationale "The Quantum Transition : Anticipate · Secure · Cooperate", en lien avec les travaux du groupe de travail du G7 sur les technologies quantiques.