Se préparer aux technologies quantiques : éléments clés à prendre en compte pour les acteurs du secteur financier

Rapport préparé par le Quantum Technologies Working Group (QTWG) des banques centrales du G7, coprésidé par la Banque de France et la Banque du Canada

Mai 2026

Avant-propos

Les technologies quantiques franchissent progressivement le cap de la recherche fondamentale et entrent dans une phase marquée par les premières expérimentations et déploiements, suscitant un intérêt croissant de la part des institutions publiques, des autorités financières et de l'écosystème technologique au sens large. Ces évolutions soulèvent des questions importantes pour le système financier, en particulier dans les domaines où la confiance, la sécurité, la résilience et la stabilité à long terme sont essentielles.

La présente publication est une adaptation publique des travaux analytiques menés dans le cadre de la coopération entre les banques centrales du G7. Elle s'appuie sur l'expertise collective acquise grâce à des activités de recherche, à des expérimentations techniques et à un dialogue continu avec des partenaires universitaires et institutionnels. L'objectif de cette version publique est de mettre à disposition une base analytique commune sur les implications des technologies quantiques pour la finance, tout en garantissant clarté, neutralité et accessibilité à un public plus large.

Le rapport s'adresse aux acteurs du secteur financier, aux institutions publiques et aux décideurs, ainsi qu'à un public averti au sein de l'écosystème des technologies quantiques et de la cybersécurité. Il vise à contribuer à une compréhension commune des risques et des opportunités associés aux technologies quantiques, à encourager un débat éclairé et à servir de point de référence pour un dialogue transcendant les frontières institutionnelles et sectorielles.

Cette contribution ne vise pas à anticiper les décisions réglementaires, à promouvoir des approches spécifiques ou à prescrire des lignes d'action. Compte tenu de la rapidité des évolutions technologiques et de l'incertitude entourant les développements futurs, l'analyse évite délibérément toute affirmation spéculative sur les calendriers ou les résultats qui ne s'appuient pas sur des recherches établies et des tendances observables. Elle met plutôt l'accent sur l'analyse factuelle, les incertitudes clairement identifiées et les arbitrages inhérents aux différentes voies technologiques.

En rendant ce travail public, les institutions participantes visent à favoriser la transparence et un engagement constructif sur un sujet dont l'importance ne cesse de croître pour le système financier. Un débat public bien informé et équilibré est une condition essentielle à la préparation, à la coordination et à la confiance alors que les technologies quantiques continuent d'évoluer.

Résumé

Les technologies quantiques, notamment l'informatique quantique, la communication quantique et les technologies de capteurs quantiques, relevant initialement d'une recherche essentiellement académique, entrent dans une phase marquée par les premières expérimentations et déploiements. Si de nombreuses applications en sont encore au stade exploratoire, ces évolutions revêtent une importance croissante pour un système financier qui repose sur la sécurité des données, des communications fiables et des calculs complexes.

Le présent rapport examine deux domaines dans lesquels les technologies quantiques pourraient avoir des implications importantes pour la finance. Le premier concerne **la sécurité des données et des communications**, compte tenu des progrès attendus en informatique quantique qui, à terme, devraient remettre en cause les techniques cryptographiques largement utilisées qui sous-tendent la confiance numérique. Le second se concentre sur **les applications potentielles des technologies quantiques sur les marchés financiers, les systèmes de paiement et les activités des banques centrales**, ainsi que leurs effets plus larges au niveau du système.

En matière de sécurité, les évaluations d'experts suggèrent qu'il existe une **probabilité non négligeable qu'un ordinateur quantique cryptographiquement pertinent (CRQC – Cryptographically Relevant Quantum Computer) puisse voir le jour** au cours de la prochaine décennie, bien qu'aucun système de ce type n'existe actuellement. Parallèlement, la possibilité d'attaques dites de « harvest now, decrypt later » (collecter aujourd'hui, déchiffrer demain) souligne l'importance de la confidentialité des données à long terme, en particulier pour les informations qui doivent rester sécurisées bien au-delà des cycles de vie cryptographiques actuels. Ces considérations expliquent pourquoi les risques liés à l'informatique quantique sont de plus en plus intégrés dans les discussions sur la résilience du système financier.

Plusieurs approches résistantes aux attaques quantiques (*quantum-safe*) sont en cours d'élaboration pour relever ces défis. **La cryptographie post-quantique, soutenue par des efforts de normalisation internationale, s'impose comme un élément central de la transition vers une sécurité résiliente face à l'informatique quantique**. La mise en œuvre de la cryptographie post-quantique n'est toutefois pas un simple exercice de substitution. Dans la pratique, les efforts de migration peuvent nécessiter de recenser les dépendances cryptographiques, de tester la compatibilité avec les systèmes existants et de coordonner les mises à jour avec les contreparties externes et les prestataires de services. Telle est la position centrale du Groupe d'experts cyber du G7 (Cyber Expert Group, CEG), qui soutient la coordination de la cryptographie post-quantique à la suite de la publication, en janvier 2026, de sa feuille de route pour la transition vers des technologies résistantes aux attaques quantiques. D'autres approches, notamment les technologies de communication quantique et les architectures de distribution de clés symétriques, peuvent compléter les solutions cryptographiques dans des contextes spécifiques. Ces autres options impliquent des arbitrages liés à la maturité technologique, au passage à l'échelle, à l'interopérabilité, à la complexité opérationnelle et au coût, ce qui suggère qu'aucune approche unique n'est universellement applicable.

Au-delà de la sécurité, les technologies quantiques pourraient également influencer le fonctionnement des systèmes financiers. La recherche et les premières expérimentations indiquent que **les capacités de calcul quantique pourraient, à terme, surpasser les ordinateurs classiques pour certaines tâches de calcul pertinentes en finance, telles que l'optimisation, la simulation et l'analyse des risques**. Les domaines susceptibles d'être concernés comprennent les marchés financiers, les systèmes de paiement et de règlement, ainsi que les fonctions analytiques (par exemple, les simulations macroéconomiques, la modélisation de la stabilité financière ou les tests de résistance à grande échelle) au sein des banques centrales et des institutions financières. Dans le même temps, l'adoption de capacités quantiques avancées pourrait introduire de nouvelles formes de dépendance, de concentration et de vulnérabilités communes.

Les implications des technologies quantiques dépassent le cadre des cas d'usage individuels, soulevant des considérations plus larges liées à la gouvernance, à la résilience et aux compétences. L'adoption de ces technologies devrait rester variable selon les institutions et les juridictions, en fonction de la maturité technologique et de l'accès à l'expertise.

Pris ensemble, ces éléments soulignent l'importance d'une compréhension structurée et fondée sur des faits des technologies quantiques et de leurs effets potentiels sur le système financier. Clarifier les impacts, les risques et les arbitrages peut favoriser un dialogue éclairé entre les parties prenantes du secteur financier, les institutions publiques et les communautés plus larges des technologies quantiques et de la cybersécurité, à mesure que ces technologies continuent d'évoluer.

Introduction

À mesure que les technologies quantiques passent du stade de la recherche à celui des premiers déploiements, leurs implications pour le paysage financier et économique mondial deviennent de plus en plus tangibles. Bien que de nombreuses capacités soient encore en cours de développement, les progrès réalisés dans les domaines de l'informatique quantique, de la communication quantique et des technologies de capteurs quantiques ont suscité une attention accrue de la part des institutions publiques, des autorités financières et des acteurs du marché. Pour le système financier, ces évolutions soulèvent des questions qui vont au-delà des performances technologiques, et qui s'étendent à la confiance, à la sécurité, à la résilience et à la stabilité à long terme.

Les systèmes financiers s'appuient sur des infrastructures numériques dont l'intégrité dépend de communications sécurisées, de mécanismes cryptographiques robustes et de la capacité à traiter et analyser de grands volumes de données. **Les technologies quantiques interagissent avec ces fondements de multiples façons**. D'une part, les progrès de l'informatique quantique pourraient, à terme, compromettre certaines techniques cryptographiques qui garantissent actuellement la confidentialité, l'authentification et l'intégrité des données. D'autre part, les méthodes quantiques pourraient également, à terme, améliorer la sécurité des communications et des transferts de données, ainsi que certaines tâches de calcul pertinentes pour la finance, notamment l'optimisation, la simulation et la modélisation.

Le présent rapport se concentre sur les implications des technologies quantiques là où elles ont une incidence la plus directe sur le fonctionnement du système financier. Il examine deux domaines prioritaires. Le premier concerne **la sécurité des données et des communications**, qui reste un pilier de la confiance dans les infrastructures et les institutions financières. Le second explore **les applications potentielles des technologies quantiques dans le domaine financier**, y compris leurs effets possibles sur les marchés financiers, les systèmes de paiement et de règlement, ainsi que les fonctions analytiques au sein des banques centrales et des institutions financières.

Les technologies quantiques englobent trois domaines distincts mais interdépendants : l'informatique quantique, la communication quantique et les capteurs quantiques. L'informatique quantique exploite les propriétés de la mécanique quantique pour traiter des classes spécifiques de problèmes de calcul difficiles à résoudre avec des ordinateurs classiques. La communication quantique [1] s'appuie sur les principes physiques de la mécanique quantique pour permettre de nouvelles approches en matière d'échange sécurisé d'informations. Les technologies de capteurs quantiques utilisent les effets quantiques pour réaliser des mesures très précises de grandeurs physiques telles que le temps, les champs magnétiques ou les signaux électromagnétiques. Chacun de ces domaines peut affecter les systèmes financiers de différentes manières et se trouve à des stades de maturité différents.

À la lumière de ces évolutions, **l'objectif du présent rapport est de fournir un cadre analytique structuré pour faciliter la compréhension des risques, des opportunités et des arbitrages liés aux technologies quantiques, et qui concernent le système financier**. Plutôt que de formuler des prévisions ou des positions à adopter, il vise à clarifier les domaines dans lesquels les technologies quantiques interagissent avec les infrastructures et les activités financières, et à mettre en évidence les considérations susceptibles d'influencer les évolutions futures.

[1] Un canal de communication quantique fondé sur la distribution de clés quantiques est sécurisé d'un point de vue théorique en matière d'information. En cryptographie, cela signifie que la sécurité ne peut être compromise même si l'adversaire dispose de ressources illimitées en termes de puissance de calcul, de mémoire et de temps. Cependant, la sécurité de bout en bout dans les déploiements concrets dépend également des composants classiques, des choix de mise en œuvre et des contrôles opérationnels, qui peuvent introduire des vulnérabilités supplémentaires.

En se concentrant sur une analyse factuelle et des incertitudes clairement identifiées, **le rapport vise à contribuer à un débat éclairé entre les parties prenantes du secteur financier, les institutions publiques et les communautés plus larges de la cybersécurité et de l'informatique quantique**. Une compréhension commune de ces enjeux peut favoriser un dialogue constructif et renforcer la préparation collective à mesure que les technologies quantiques continuent d'évoluer.

Domaine prioritaire 1 : Sécurité des données et des communications

La sécurité des données et des communications est un élément fondamental de la confiance dans le système financier. Les infrastructures financières s'appuient sur des mécanismes cryptographiques pour garantir la confidentialité, l'intégrité, l'authentification et la non-répudiation dans un large éventail d'activités, du traitement et du règlement des paiements aux déclarations d'informations prudentielles et à l'échange transfrontière d'informations.

Les progrès des technologies quantiques introduisent de nouvelles considérations pour ce cadre de sécurité. Bien que les technologies quantiques en soient encore à différents stades de maturité, leur potentiel à remettre en cause les hypothèses cryptographiques existantes a suscité une attention accrue dans l'ensemble du secteur financier. Cette section examine comment les technologies quantiques affectent la sécurité des données et des communications, en se concentrant sur la nature du paysage émergent des menaces, les implications pour la confidentialité à long terme et l'éventail des approches techniques explorées pour renforcer la résilience quantique.

L'analyse dans ce domaine ne repose pas sur une trajectoire technologique ou un calendrier spécifique. Elle fournit plutôt un aperçu structuré des risques, des incertitudes et des arbitrages pertinents pour les infrastructures financières, dans le but de favoriser une évaluation éclairée et un dialogue constructif.

1.1 Perspectives d'évolution des technologies quantiques

La perspective de menaces quantiques pesant sur la sécurité des données et des communications est principalement liée aux progrès de l'informatique quantique. Certains algorithmes cryptographiques largement utilisés aujourd'hui — en particulier ceux qui sous-tendent le chiffrement à clé publique et les signatures numériques — reposent sur des problèmes mathématiques considérés comme insolubles pour les ordinateurs classiques. Des recherches ont toutefois démontré que des ordinateurs quantiques suffisamment puissants pourraient résoudre certains de ces problèmes de manière bien plus efficace, remettant ainsi en cause les hypothèses de sécurité sur lesquelles s'appuient les systèmes cryptographiques actuels.

À l'heure actuelle, il n'existe aucun ordinateur quantique capable de briser les schémas de chiffrement couramment déployés. Néanmoins, **les évaluations d'experts et les enquêtes indiquent une attente croissante quant à l'émergence de telles capacités au cours de la prochaine décennie**. Les estimations varient considérablement, reflétant une incertitude importante concernant les progrès scientifiques, les contraintes techniques, les défis liés à l'évolutivité et les avancées potentielles dans la conception et l'optimisation des algorithmes quantiques. Ces évaluations n'impliquent pas une inévitabilité dans un délai fixe, mais elles suggèrent que **les risques liés aux technologies quantiques ne sont plus purement théoriques, en particulier si l'on tient compte des effets combinés des progrès matériels et des améliorations algorithmiques**.

Une autre dimension importante des menaces émergentes découle des caractéristiques temporelles des données sensibles. Dans de nombreux contextes financiers et institutionnels, les informations doivent rester confidentielles pendant de longues périodes, parfois des décennies. Cela crée une exposition à des scénarios dits de « harvest-now, decrypt-later », dans lesquels des données chiffrées sont interceptées et stockées aujourd'hui dans l'intention de les déchiffrer à l'avenir, une fois que des capacités de calcul plus avancées seront disponibles. Les infrastructures et institutions financières échangent un large éventail de données susceptibles d'être affectées par ces dynamiques. Cela inclut les communications entre les institutions financières et les infrastructures de marché, les interactions avec les banques centrales et les autorités publiques, ainsi que les données sous-tendant les systèmes de paiement, les processus de règlement et les fonctions de surveillance prudentielle.

Au-delà de la confidentialité, des considérations temporelles similaires s'appliquent aux mécanismes cryptographiques sous-tendant l'authentification, l'intégrité et la non-répudiation. Si les systèmes de signature numérique actuellement utilisés venaient à devenir vulnérables à des capacités de calcul quantique suffisamment avancées, cela pourrait, à terme, permettre la falsification de signatures ou l'usurpation d'identité d'entités de confiance. Les technologies financières numériques émergentes, notamment les actifs tokenisés, les cadres d'identité numérique et les systèmes basés sur des registres distribués, s'appuient largement sur des mécanismes cryptographiques pour l'authentification, l'intégrité et la non-répudiation [2]. À ce titre, leur robustesse à long terme pourrait également être affectée si les vulnérabilités liées à l'informatique quantique ne sont pas traitées en temps opportun.

Bien que de tels scénarios dépendent de l'émergence de capacités de calcul quantique pertinentes sur le plan cryptographique, ils illustrent le fait que les risques liés à l'informatique quantique ne concernent pas seulement la protection des données stockées, mais aussi la robustesse à long terme des mécanismes de confiance qui sous-tendent les infrastructures financières numériques.

Les impacts potentiels de ces vulnérabilités pourraient s'étendre au-delà des systèmes ou institutions individuels. Une confidentialité compromise, la falsification de signatures numériques, l'usurpation d'identité d'entités de confiance ou la manipulation de données de transaction pourraient nuire à la confiance dans les infrastructures financières et, si elles se poursuivaient, affecter la confiance générale dans le système financier. Ces risques ne sont pas propres aux technologies quantiques, mais l'informatique quantique introduit une catégorie distincte de défis en ciblant les fondements cryptographiques plutôt que les failles de mise en œuvre ou les faiblesses opérationnelles.

1.2 Transition cryptographique et approches de résistance quantique

La cryptographie post-quantique ou PQC [3] désigne une nouvelle catégorie d'algorithmes cryptographiques conçus pour rester sécurisés face aux attaques rendues possibles par les ordinateurs quantiques, tout en pouvant être mis en œuvre sur des infrastructures informatiques classiques. Ces algorithmes visent à remplacer ou à compléter les schémas cryptographiques à clé publique largement déployés dont la sécurité pourrait être remise en cause par des ordinateurs quantiques suffisamment avancés.

La sécurité numérique moderne repose sur deux fonctions cryptographiques essentielles : l'échange de clés, qui permet aux parties de s'accorder sur des secrets partagés sur des réseaux non fiables, et les signatures numériques, qui garantissent l'authentification, l'intégrité et la non-répudiation des données et des transactions. Plusieurs des algorithmes à clé publique actuellement utilisés à ces fins reposent sur des problèmes mathématiques considérés comme extrêmement difficiles à résoudre pour les ordinateurs classiques, mais qui pourraient être résolus efficacement par des algorithmes quantiques dans certaines conditions. Les schémas cryptographiques post-quantiques s'appuient sur des fondements mathématiques alternatifs qui ne sont pas connus pour être vulnérables à de telles attaques quantiques.

Les efforts de normalisation internationale jouent un rôle central dans le développement et l'évaluation de la cryptographie post-quantique. En particulier, le National Institute of Standards and Technology (NIST) a mené un processus ouvert et concurrentiel s'étalant sur plusieurs années pour évaluer les algorithmes candidats, ce qui a abouti à la sélection et à la normalisation de plusieurs schémas post-quantiques pour l'échange de clés et de signatures numériques. Ces normes sont progressivement intégrées dans les bibliothèques cryptographiques, les piles logicielles et les produits de sécurité, fournissant ainsi une base technique pour une adoption plus large dans tous les secteurs.

---

[2] Une signature numérique est une garantie mathématique que le contenu provient d'une source particulière et n'a subi aucune altération avant d'arriver à destination. Elle garantit également que l'expéditeur ne peut pas prétendre ne pas avoir envoyé le message après coup.

[3] La cryptographie post-quantique (PQC) désigne le développement d'algorithmes cryptographiques conçus pour rester sûrs face aux attaques menées par des ordinateurs quantiques.

Du point de vue du système financier, la cryptographie post-quantique est souvent considérée comme une approche pragmatique et déployable à grande échelle pour renforcer la résistance aux attaques quantiques, car elle peut, en principe, être déployée sur les réseaux et les infrastructures de communication existants. Dans le même temps, la transition vers des algorithmes cryptographiques post-quantiques implique tout un ensemble de considérations techniques et opérationnelles. Celles-ci comprennent les impacts sur les performances, l'augmentation de la taille des clés et des signatures, l'intégration avec les systèmes existants, ainsi que la nécessité de garantir l'interopérabilité entre les institutions et les juridictions pendant des périodes de transition potentiellement longues.

La mise en œuvre de la cryptographie post-quantique n'est donc pas un simple exercice de substitution. Les infrastructures financières sont fortement interconnectées, et les mécanismes cryptographiques sont profondément intégrés au matériel, aux logiciels, aux protocoles et aux processus opérationnels. Dans la pratique, les efforts de migration peuvent nécessiter de recenser les dépendances cryptographiques, de tester la compatibilité avec les systèmes existants et de coordonner les mises à jour avec les contreparties externes et les prestataires de services. Pendant les phases de transition, des systèmes utilisant des normes cryptographiques différentes peuvent devoir coexister, ce qui soulève des défis supplémentaires liés à l'interopérabilité et à la complexité opérationnelle.

La cryptographie post-quantique interagit également avec des questions plus larges d'agilité cryptographique et de gouvernance. Compte tenu des recherches en cours et de la nature évolutive de la cryptanalyse classique et quantique, la capacité à adapter les mécanismes cryptographiques au fil du temps est un facteur important à prendre en considération. Cela implique de conserver la flexibilité nécessaire pour mettre à jour les algorithmes, les paramètres et les implémentations à mesure que les normes évoluent ou que de nouvelles informations apparaissent concernant leurs propriétés de sécurité.

Dans l'ensemble, la cryptographie post-quantique constitue un élément clé de l'ensemble émergent d'approches de sécurité résistantes aux attaques quantiques. Son développement et sa normalisation reflètent un effort collectif de la communauté cryptographique mondiale visant à faire face aux risques à long terme associés à l'informatique quantique, tout en reconnaissant que les choix de mise en œuvre impliquent des arbitrages et des incertitudes qui doivent être soigneusement évalués en fonction du contexte.

Les travaux récents menés au sein du Groupe d'experts cyber (CEG) du G7 ont examiné plus en détail les aspects pratiques de la transition vers la cryptographie post-quantique. La feuille de route du CEG du G7 sur la préparation à l'ère quantique présente les activités clés que les organisations peuvent envisager pour se préparer à cette transition, notamment l'identification des dépendances cryptographiques, l'évaluation des risques, la planification de la migration et la mise en œuvre de l'agilité cryptographique. Des informations supplémentaires sont disponibles dans la feuille de route publiée par le CEG du G7 [4].

Outre la cryptographie post-quantique, **d'autres approches complémentaires sont à l'étude** pour renforcer la résilience quantique dans des contextes spécifiques. Il s'agit notamment des architectures d'échange de clés symétriques distribuées (*Distributed Symmetric Key Exchange*, DSKE), qui s'appuient sur des modèles coordonnés de distribution de clés symétriques, et de la distribution quantique de clés (*Quantum Key Distribution*, QKD), qui exploite les techniques de communication quantique pour établir des clés cryptographiques selon des hypothèses de sécurité alternatives. **Bien qu'elles diffèrent en termes de maturité, d'exigences de déploiement et d'implications opérationnelles, ces approches montrent que la sécurité face au quantique ne repose pas sur une seule voie technologique**. Un aperçu plus détaillé de ces options complémentaires est fourni à l'annexe 1.

1.3 La sécurité des données au-delà de la cryptographie

Si les mécanismes cryptographiques sont essentiels à la sécurisation des données et des communications, les

[4] [4] G7-CEG-Quantum-Roadmap.pdf.

technologies quantiques soulèvent également des considérations de sécurité qui vont au-delà du simple chiffrement et de l'échange de clés. À mesure que les capacités quantiques sont explorées pour le calcul, la communication et la mesure de phénomènes physiques, de nouvelles interfaces, architectures et modèles opérationnels émergent, chacun soulevant des questions distinctes en matière de sécurité et de résilience.

Un domaine d'intérêt concerne la protection des données pendant le calcul. Comme les ressources de l'informatique quantique devraient être accessibles principalement via des plateformes cloud ou distantes, les données sensibles pourraient devoir être traitées hors du contrôle direct du propriétaire des données. Cela a conduit à un intérêt croissant pour des techniques souvent décrites comme l'informatique quantique confidentielle ou aveugle (confidential quantum computing and blind quantum computing). Ces approches visent à garantir que les données et l'intention de calcul restent cachées au fournisseur de services quantiques, même pendant l'exécution des calculs.

En informatique classique, des objectifs analogues sont poursuivis grâce à des technologies telles que les environnements d'exécution fiables et le chiffrement entièrement homomorphe, qui permettent de calculer sur des données chiffrées au prix d'une complexité supplémentaire et d'une perte de performance. Dans le contexte quantique, la recherche explore comment les états et protocoles quantiques peuvent être utilisés pour limiter les informations exposées à la plateforme de calcul. Bien que ces approches soient prometteuses sur le plan conceptuel, elles restent largement expérimentales et sont soumises à d'importantes contraintes techniques. En pratique, les architectures hybrides combinant des composants classiques et quantiques introduisent de multiples points où les données peuvent être exposées, ce qui nécessite une réflexion approfondie sur la sécurité de bout en bout.

Les interfaces entre les systèmes classiques et quantiques constituent un autre domaine d'intérêt important. Les processeurs quantiques ne fonctionnent pas de manière isolée ; ils dépendent de systèmes de contrôle classiques, de pipelines de données, de canaux de stockage et de communication. Ces composants classiques peuvent rester vulnérables aux cybermenaces conventionnelles, même si les opérations quantiques elles-mêmes bénéficient de propriétés physiques intrinsèques. Par conséquent, la sécurité globale du système dépend non seulement des propriétés des dispositifs quantiques, mais aussi de la robustesse de l’infrastructure classique environnante, de la gouvernance et des dispositifs de sécurité de l’information et de l’intégrité des interactions entre les composants.

Les technologies de capteurs quantiques (quantum sensing) soulèvent un ensemble supplémentaire de considérations. Les capteurs quantiques exploitent les effets quantiques pour atteindre une précision extrêmement élevée dans la mesure de grandeurs physiques telles que le temps, les champs électromagnétiques ou les signaux magnétiques. Certaines applications de capteurs quantiques sont déjà déployées dans des domaines tels que la chronométrie et la navigation, qui sous-tendent des éléments de l’infrastructure financière, notamment l’horodatage et la synchronisation des transactions. Une précision accrue pourrait contribuer à améliorer l’intégrité et la surveillance des systèmes.

Dans le même temps, les progrès des capteurs quantiques peuvent faire naître de nouveaux risques. Une sensibilité accrue pourrait permettre des formes de mesure ou de surveillance qui remettent en cause les hypothèses existantes concernant la vie privée, la détectabilité ou la résistance aux interférences. Par exemple, la capacité à détecter des signaux électromagnétiques faibles ou à fonctionner dans des environnements résistants au brouillage pourrait avoir des implications pour la sécurité des communications et la protection des données. Ces développements en sont encore à des stades de maturité variables, mais ils soulignent que les considérations de sécurité liées au quantique ne se limitent pas aux seuls algorithmes cryptographiques.

Dans l'ensemble, les développements au-delà de la cryptographie soulignent l'importance d'adopter une approche holistique de la sécurité à l’ère quantique. La protection des données et des communications dans un environnement quantique implique non seulement de sélectionner des primitives cryptographiques appropriées, mais aussi de comprendre les architectures de système, les limites de confiance, les dépendances opérationnelles et les capacités de détection. Avec le développement de la recherche et de l'expérimentation, ces dimensions plus larges joueront un rôle de plus en plus important dans l'évaluation de la manière dont les technologies quantiques interagissent avec les

fondements de sécurité du système financier.

1.4 Considérations transversales

Les implications des technologies quantiques en matière de sécurité des données et des communications vont au-delà des technologies ou des cas d'usage individuels. Elles sont déterminées par un ensemble de facteurs transversaux qui influencent la manière dont les approches résistantes aux attaques quantiques sont évaluées, déployées et maintenues au sein d'infrastructures financières complexes. Le tableau ci-dessous résume ces dimensions clés. Des détails analytiques supplémentaires sont fournis à l'annexe 2.

Dimension transversale	Enjeux clés	Implications pour le système financier
Interopérabilité et complexité de la transition	Coexistence de systèmes hérités et de systèmes à résistance quantique ; intégration entre les juridictions et les infrastructures ; dépendances cryptographiques intégrées dans les protocoles et les chaînes de traitement	Des phases de transition prolongées peuvent nécessiter l'application parallèle de plusieurs normes de sécurité, ce qui accroît la complexité et les difficultés de coordination
Dépendances opérationnelles et risque liés aux tiers (non spécifique au domaine quantique)	Dépendance vis-à-vis des fournisseurs, des prestataires de services et des infrastructures spécialisées ; risque de concentration ; exposition aux chaînes d'approvisionnement ; relation entre les dépendances et les fonctions critiques	Les choix en matière de technologies de sécurité peuvent influencer les structures de dépendance et la résilience face aux perturbations ; Capacités en matière de sécurité, expertise et coûts pouvant être corrélés à la taille du prestataire de services
Agilité cryptographique et gouvernance	Nécessité de mettre à jour les algorithmes, les paramètres et les implémentations au fil du temps ; flexibilité architecturale ; processus décisionnels institutionnels	Des mécanismes de gouvernance et de coordination efficaces sont essentiels pour gérer l'évolution cryptographique à long terme
Compétences et état de préparation opérationnelle	Pénurie d'expertise interdisciplinaire ; inventaire des dépendances cryptographiques ; capacité à gérer des transitions complexes	Des différences en matière de compétences et de ressources peuvent influencer le rythme et l'ampleur de l'adoption au sein des institutions

Domaine prioritaire 2 : Applications des technologies quantiques dans le secteur financier

Au-delà de leurs implications pour la sécurité des données et des communications, **les technologies quantiques peuvent également influencer la manière dont certaines fonctions du système financier sont exécutées**. Les progrès de l'informatique quantique ont suscité un intérêt croissant pour les applications potentielles liées à certaines tâches nécessitant une grande puissance de calcul, telles que l'optimisation, la simulation et l'analyse de données. Ces applications en sont encore au stade exploratoire ou expérimental, mais leur possible pertinence pour la finance est devenue un sujet de recherche et de discussion actif.

Ce domaine examine comment les technologies quantiques pourraient interagir avec les marchés financiers, les systèmes de paiement et de règlement, ainsi qu'avec les fonctions analytiques et opérationnelles au sein des banques centrales et des institutions financières. **L'analyse porte à la fois sur les gains d'efficacité potentiels et sur les implications plus larges au niveau du système qui pourraient découler de l'exploration ou de l'adoption de capacités quantiques**. Une attention particulière est accordée aux questions de maturité, d'évolutivité et d'intégration avec les infrastructures existantes, ainsi qu'aux dépendances et aux risques pouvant accompagner ces nouveaux paradigmes de calcul.

Il est important de noter que le développement et l'adoption d'applications quantiques dans le secteur financier ne se font pas en vase clos. Ils s'inscrivent dans des tendances plus larges de la numérisation, notamment les progrès en matière de calcul haute performance, d'intelligence artificielle et de services fondés sur le cloud. Par conséquent, de nombreux cas d'usage à court terme impliquent des approches hybrides combinant des ressources classiques et quantiques. Il est essentiel de comprendre ces interactions pour évaluer où les technologies quantiques pourraient apporter une valeur ajoutée, où elles pourraient introduire de nouvelles vulnérabilités, et où leur impact serait susceptible de rester limité dans un avenir prévisible.

Cette section ne prévoit pas le déploiement généralisé d'applications quantiques dans le secteur financier, ni ne donne la priorité à des cas d'usage spécifiques. **Elle vise plutôt à fournir un aperçu structuré des domaines dans lesquels les technologies quantiques sont explorées et à clarifier la nature des impacts potentiels**. Ce faisant, elle entend favoriser une évaluation et un dialogue éclairés sur la manière dont les technologies quantiques pourraient, à terme, façonner certains aspects du système financier. À ce stade, les applications des technologies quantiques aux enjeux du secteur financier demeurent principalement expérimentales, car la technologie n'a pas encore atteint un niveau de maturité permettant des applications pratiques économiquement viables.

2.1 Techniques quantiques d'intérêt

L'informatique quantique diffère de l'informatique classique par la manière dont l'information est représentée et traitée. Au lieu de fonctionner uniquement sur des états binaires, les ordinateurs quantiques s'appuient sur des bits quantiques, ou qubits [5], qui peuvent encoder et manipuler l'information en utilisant les propriétés de la mécanique quantique. Cela permet d'aborder certains types de calculs de manière fondamentalement différente par rapport aux architectures classiques.

Les processeurs quantiques ne sont pas des substituts polyvalents aux ordinateurs classiques. Il s'agit plutôt de dispositifs spécialisés conçus pour traiter des classes spécifiques de problèmes mathématiques. À cet égard, les unités de traitement quantique peuvent être comparées à d'autres accélérateurs de calcul spécialisés, tels que les processeurs graphiques, qui sont aujourd'hui largement utilisés pour des tâches comme la simulation numérique ou l'apprentissage automatique. La pertinence potentielle de l'informatique quantique pour la finance dépend donc de la possibilité de formuler les problèmes financiers de manière à tirer parti de ces capacités spécialisées. La recherche a identifié plusieurs catégories de problèmes de calcul pour lesquels les approches quantiques pourraient présenter des avantages sous certaines conditions.

Pour les lecteurs à la recherche d'un aperçu plus technique, l'annexe 3 fournit un tableau non exhaustif des principaux algorithmes quantiques fréquemment abordés dans la littérature, ainsi que leurs principales caractéristiques computationnelles et leurs domaines d'application.

2.1.1. Méthodes mathématiques

Un certain nombre d'algorithmes quantiques visent à accélérer des opérations mathématiques fondamentales, telles que l'inversion de matrices ou la résolution de systèmes d'équations linéaires [6]. Ces opérations jouent un rôle important dans la modélisation financière, l'analyse des risques et les routines d'optimisation. En théorie, certains algorithmes quantiques pourraient effectuer ces tâches avec plus d'efficacité que les méthodes classiques pour des structures de problèmes spécifiques. Dans la pratique, cependant, la possibilité d'appliquer ces algorithmes dépend de facteurs tels que les coûts de préparation des données, les taux d'erreur et l'échelle du matériel quantique disponible.

[5] Les qubits peuvent ainsi être visualisés comme des vecteurs dans un espace linéaire complexe, représentés par deux nombres complexes. Alors qu'un système classique n'occupe qu'un seul état à un moment donné, un système quantique à n qubits existe sous la forme d'une superposition de tous les 2^n états de base, nécessitant 2^n amplitudes complexes pour décrire son état complet.
[6] En particulier, le célèbre algorithme HHL, qui, dans des conditions générales, offre en théorie un gain de vitesse exponentiel par rapport aux méthodes classiques.

Les approches quantiques de l'échantillonnage statistique ont également suscité l'intérêt. L'échantillonnage à partir de distributions de probabilité complexes est une exigence courante dans les applications financières, en particulier dans la modélisation stochastique et les simulations de Monte Carlo. Les techniques quantiques pourraient permettre des stratégies d'échantillonnage alternatives difficiles à reproduire de manière classique, bien que la traduction de ces avantages théoriques en gains pratiques reste une question de recherche ouverte.

2.1.2. Optimisation

Les problèmes d'optimisation sont omniprésents dans le secteur financier, allant de la construction de portefeuilles et de la gestion des risques à l'allocation de liquidité et à la planification opérationnelle. Ces problèmes impliquent souvent un grand nombre de variables et de contraintes, ce qui entraîne une complexité de calcul croissante. Le calcul quantique a été testé comme un moyen d'identifier heuristiquement des solutions satisfaisantes dans de tels espaces de grande dimension.

Les recherches actuelles se concentrent sur l'identification de formulations de problèmes dans lesquelles les techniques d'optimisation quantique peuvent compléter les heuristiques classiques. Les premières expériences portent généralement sur des cas à petite échelle et servent principalement à tester des algorithmes et des chaînes de traitement plutôt qu'à démontrer des performances compatibles avec des enjeux de déploiement en production.

2.1.3. Apprentissage automatique quantique (Quantum Machine Learning - QML)

L'apprentissage automatique quantique désigne une famille d'approches visant à combiner les techniques de calcul quantique avec les méthodes d'apprentissage automatique. L'objectif n'est pas de remplacer l'apprentissage automatique classique, mais d'explorer si certaines sous-tâches — telles que la représentation des caractéristiques, l'estimation du noyau ou l'optimisation — pourraient être améliorées à l'aide de ressources quantiques.

2.1.4. Méthodes inspirées du quantique

Parallèlement aux développements en matière de matériel quantique, un nombre croissant de travaux ont vu le jour autour de ce que l'on appelle les méthodes inspirées du quantique. Ces méthodes n'impliquent pas réellement de composants quantiques, mais s'appuient sur des concepts initialement développés en physique quantique, tels que les réseaux de tenseurs, pour concevoir des algorithmes classiques efficaces destinés à résoudre des problèmes de haute dimension. Contrairement à l'informatique quantique, les approches d'inspiration quantique ne nécessitent pas de matériel quantique et peuvent souvent être déployées sur l'infrastructure classique existante.

2.2 Domaines d'application

Cette section examine certains domaines dans lesquels des techniques quantiques, telles que celles mentionnées ci-dessus, font l'objet de recherches en vue de leur contribution potentielle aux activités financières. L'objectif n'est pas de prédire leur adoption ni de hiérarchiser les cas d'usage, mais de clarifier la nature des problèmes traités, le degré de maturité des approches actuelles et les implications potentielles au niveau du système si ces techniques devaient évoluer davantage.

2.2.1 Marchés financiers

Les marchés financiers se caractérisent par des volumes de transactions élevés, des interdépendances complexes et de fortes incitations à l'efficacité et à la rapidité. Historiquement, les progrès des technologies informatiques et de communication ont joué un rôle important dans la détermination des structures de marché, des stratégies de négociation et des cadres réglementaires. Dans ce contexte, les technologies quantiques sont explorées comme un complément potentiel à l'ensemble des outils utilisés dans les activités liées aux marchés.

La recherche et les premières expérimentations se sont concentrées sur plusieurs domaines dans lesquels les techniques de calcul quantique pourraient, en principe, s'avérer pertinentes. Il s'agit notamment de **l'optimisation de portefeuille,** de **la valorisation des actifs et** de **la modélisation des risques, ainsi que** de **la simulation de dynamiques de marché**

complexes. Bon nombre de ces tâches impliquent de vastes espaces combinatoires ou des modèles probabilistes, ce qui les rend très exigeantes sur le plan computationnel si l'on utilise uniquement des méthodes classiques.

À l'heure actuelle, les applications quantiques sur les marchés financiers en sont encore au stade exploratoire, généralement limitées à des cas à petite échelle ou stylisés. Les méthodes classiques continuent de surpasser les techniques quantiques dans la plupart des contextes pratiques, et tout avantage potentiel reste fortement dépendant du contexte. Si, à l'avenir, les applications quantiques étaient largement mises en œuvre, les intervenants de marché et les régulateurs devraient examiner comment l'adoption de cette technologie pourrait potentiellement affecter la structure des différents marchés, ce qui pourrait avoir un impact sur les dépendances vis-à-vis des tiers et des fournisseurs.

Si les recherches suggèrent que les techniques quantiques pourraient, à terme, contribuer à certaines tâches d'analyse ou d'optimisation, **leur pertinence pour les opérations de marché réelles reste subordonnée aux progrès technologiques, aux dispositifs de gouvernance et aux considérations systémiques** plutôt qu'à la seule capacité de calcul brute.

2.2.2 Systèmes de paiement

Les systèmes de paiement et de règlement constituent un élément central de la stabilité financière. Ils sont conçus pour fonctionner avec des niveaux élevés de fiabilité, de sécurité et d'efficacité, souvent dans le cadre de contraintes strictes en temps réel ou quasi-temps réel. Même des améliorations ou des perturbations mineures de ces systèmes peuvent avoir des implications importantes pour la gestion de la liquidité, la résilience opérationnelle et la confiance dans le système financier.

Dans ce contexte, les technologies quantiques sont étudiées principalement pour leur contribution potentielle à **l'optimisation**, au **suivi** et à **la résilience**, plutôt que pour remplacer les infrastructures de paiement existantes. Jusqu'à présent, les recherches ont eu pour objet de déterminer si les techniques d'informatique quantique pouvaient prendre en charge des tâches de calcul spécifiques au sein des systèmes de paiement, dont on sait déjà qu'elles mobilisent d'importantes ressources lorsqu'elles sont traitées uniquement par des méthodes classiques.

L'optimisation de la liquidité dans les systèmes de paiement et de règlement de montants élevés constitue un domaine d'intérêt. Ces systèmes doivent trouver un équilibre entre le règlement rapide des transactions et l'utilisation efficace de la liquidité. Les problèmes d'optimisation qui se posent dans ce contexte peuvent rapidement gagner en complexité à mesure que le nombre de participants, de transactions et de contraintes augmente. Les techniques d'optimisation quantique sont étudiées comme un complément possible aux heuristiques classiques afin d'explorer plus efficacement les champs de solutions. À l'heure actuelle, ces travaux restent largement expérimentaux et se limitent généralement à des modèles simplifiés ou à petite échelle, servant principalement à tester des algorithmes plutôt qu'à démontrer des solutions déployables.

Un autre domaine à l'étude concerne **le suivi et la détection d'anomalies** au sein des flux de paiement à grande échelle. La détection de schémas inhabituels — tels que des erreurs opérationnelles, des fraudes ou des tensions émergentes — nécessite l'analyse de volumes élevés de données transactionnelles en temps quasi réel. Des techniques assistées par l'informatique quantique, souvent combinées à des méthodes classiques d'apprentissage automatique, ont été proposées pour améliorer la reconnaissance de schémas ou l'échantillonnage dans des ensembles de données complexes. Ces approches en sont encore à un stade précoce, et leur pertinence pratique dépend des progrès continus tant au niveau du matériel quantique que de la conception d'algorithmes hybrides.

Comme dans d'autres domaines financiers, **les avantages potentiels pour les systèmes de paiement sont étroitement liés à des défis opérationnels et d'intégration**. Dans un avenir prévisible, les technologies quantiques dans ce domaine resteront principalement expérimentales plutôt que transformatrices.

2.2.3 Analyse et opérations des banques centrales

Les applications potentielles des technologies quantiques au sein des banques centrales diffèrent à plusieurs égards importants de celles des marchés financiers ou des institutions financières commerciales. Les banques centrales mènent

toute une série d'activités analytiques et opérationnelles qui sont très gourmandes en ressources informatiques, qui s'inscrivent par nature sur le long terme et sont étroitement liées à la formulation des politiques, à la surveillance des systèmes et aux opérations internes. Dans ce contexte, les technologies quantiques sont principalement explorées en tant **qu'outils d'analyse et d'optimisation**, plutôt que comme vecteurs d'avantage concurrentiel.

Un domaine d'intérêt concerne **la modélisation économique et financière**. Les banques centrales s'appuient sur des modèles complexes pour analyser la dynamique macroéconomique et des marchés financiers, ainsi que les risques pour la stabilité financière. Ces modèles impliquent souvent de vastes systèmes d'équations intégrant des anticipations, et certaines applications telles que les simulations stochastiques et les routines d'optimisation peuvent être très gourmandes en ressources informatiques. Les recherches suggèrent que certaines techniques de calcul quantique pourraient, en principe, faciliter certains aspects de ces tâches, comme l'accélération des simulations, l'amélioration de l'échantillonnage à partir de distributions de probabilité complexes, ou la résolution de sous-problèmes d'optimisation spécifiques. À l'heure actuelle, cependant, ces applications restent **largement expérimentales**, et leur pertinence dépend des progrès continus en matière de fiabilité du matériel, de conception d'algorithmes et de chaînes de traitement hybrides classiques-quantiques.

Un domaine connexe est celui de **l'analyse des risques et de l'estimation des risques extrêmes**. L'évaluation d'événements rares mais graves constitue un défi persistant dans l'analyse de la stabilité financière, en particulier lorsque les données historiques sont limitées ou que les distributions présentent des queues épaisses. Des techniques d'échantillonnage assisté par la physique quantique et de modélisation générative sont à l'étude comme moyens possibles d'explorer plus efficacement des paysages de risques complexes. Si les premiers résultats de la recherche présentent un intérêt académique, **leur contribution pratique à l'analyse pertinente pour l'élaboration des politiques reste à établir**, et d'importants défis méthodologiques et de validation subsistent.

Au-delà de la modélisation analytique, les technologies quantiques pourraient également s'avérer pertinentes pour **l'optimisation opérationnelle au sein des banques centrales**. Citons par exemple les problèmes d'optimisation liés à la gestion de la liquidité, à l'allocation des ressources, à la planification des fonctions critiques ou aux processus logistiques tels que la distribution de liquidités. Ces problèmes possèdent des caractéristiques communes avec ceux étudiés dans d'autres parties du secteur financier, à savoir une dimensionnalité élevée et des contraintes complexes. Comme dans d'autres domaines, les travaux actuels se concentrent sur des expériences à petite échelle et des études de validation de concept, **sans hypothèse de déploiement à court terme**.

L'apprentissage automatique assisté par l'informatique quantique est un autre domaine à l'étude. Les banques centrales recourent de plus en plus aux techniques d'apprentissage automatique pour des tâches telles que la classification des données, la reconnaissance de formes et l'analyse de texte, la détection d'anomalies et la prévision. Les approches d'apprentissage automatique quantique cherchent à déterminer si les ressources quantiques pourraient améliorer certains aspects de ces chaînes de traitement, par exemple grâce à des représentations alternatives des données ou à des étapes d'optimisation. À l'heure actuelle, **l'apprentissage automatique quantique en est encore à un stade précoce de la recherche**, et ses avantages potentiels par rapport aux techniques classiques avancées restent incertains.

Dans tous ces domaines, **les approches hybrides combinant l'informatique classique et l'informatique quantique dominent la recherche et l'expérimentation actuelles**. Les technologies quantiques ne sont pas considérées comme des substituts aux cadres analytiques existants, mais plutôt comme de possibles compléments susceptibles, à terme, de renforcer des tâches de calcul spécifiques. L'intégration avec les systèmes établis, les exigences en matière de gouvernance des données et les normes de validation constituent donc un élément central d'appréciation.

Dans l'ensemble, l'exploration des technologies quantiques dans l'analyse et les opérations des banques centrales met en évidence une approche prudente et progressive. **L'accent est mis sur la compréhension des capacités, des limites et des implications potentielles**, plutôt que sur l'accélération de l'adoption. Comme pour les autres applications abordées dans ce domaine, la pertinence des technologies quantiques pour les banques centrales dépendra non seulement des progrès techniques, mais aussi de la robustesse méthodologique, de l'explicabilité et de l'alignement avec les mandats institutionnels

2.3 Implications au niveau systémique

Si les applications potentielles des technologies quantiques dans la finance sont souvent examinées à travers des cas d'usage individuels, leurs implications plus larges s'appréhendent mieux au niveau du système financier dans son ensemble. Les impacts potentiels des technologies quantiques pourraient aller au-delà de simples gains d'efficacité isolés, qui influenceraient la structure du marché, la résilience opérationnelle et les dispositifs de gouvernance. Une considération importante concerne **les effets de concentration et d'asymétrie**. Si les technologies quantiques devaient offrir des avantages significatifs dans des tâches spécifiques d'analyse ou d'optimisation, cela pourrait renforcer les asymétries existantes entre les institutions ou contribuer à une concentration autour d'un nombre limité de fournisseurs de technologies. Une question étroitement liée concerne **les dépendances partagées et les points de défaillance communs**. L'accès aux ressources de calcul quantique devrait se faire principalement par l'intermédiaire de fournisseurs spécialisés, souvent via des plateformes en nuage. Ces fournisseurs spécialisés pourraient offrir les avantages des technologies quantiques à un plus large éventail d'entreprises clientes, à des coûts moindres et avec des niveaux de qualité et de sécurité supérieurs à ceux obtenus si les entreprises financières développaient leurs propres capacités quantiques en interne. Toutefois, le recours généralisé à un petit nombre de fournisseurs, de piles logicielles ou d'architectures matérielles, dans la mesure où celles-ci sous-tendent des opérations critiques, pourrait entraîner une exposition à des risques corrélés, notamment des pannes techniques, des incidents cyber ou des perturbations de la chaîne d'approvisionnement. D'un point de vue systémique, la résilience peut dépendre non seulement de la robustesse des institutions individuelles, mais aussi, en partie, de la gamme de solutions proposées au sein de l'écosystème technologique sous-jacent.

L'opacité et l'explicabilité constituent un autre défi transversal. Certaines techniques quantiques, en particulier lorsqu'elles sont associées à des méthodes avancées d'optimisation ou d'apprentissage automatique, peuvent être difficiles à interpréter ou à valider à l'aide d'approches traditionnelles.

Le **calendrier et la diffusion des effets risquent également de rester inégaux selon les applications et les juridictions**, ce qui renforce la nécessité d'éviter toute hypothèse d'adoption uniforme ou synchronisée. Prises dans leur ensemble, ces implications au niveau du système suggèrent que la pertinence des technologies quantiques pour le système financier ne peut être évaluée uniquement à l'aune d'indicateurs de performance technologique. **Les questions de concentration, de dépendance, de transparence et de résilience peuvent influencer les résultats autant que la capacité de calcul elle-même**. La prise en compte de ces dimensions peut aider à orienter les discussions sur les technologies quantiques de manière à tenir compte de la complexité, de l'interdépendance et de l'incertitude.

Synthèse

3.1 Principales conclusions analytiques

L'analyse menée dans les deux domaines principaux du présent rapport met en évidence que les technologies quantiques présentent un ensemble de défis et d'opportunités pour le système financier qui sont moins définis par une disruption immédiate que par des horizons temporels potentiellement longs et incertains ainsi que de fortes interdépendances.

Un premier point clé concerne la nature temporelle des risques liés au quantique, en particulier dans le domaine de la sécurité des données et des communications. La possibilité que les futures capacités de l'informatique quantique puissent compromettre les mécanismes cryptographiques largement utilisés représente un risque pour la confidentialité et l'intégrité. Cette dimension temporelle, combinée à la longue durée de conservation de certains types de données financières sensibles, souligne l'importance de prendre en compte les risques quantiques bien au-delà des capacités technologiques actuelles.

Un deuxième enseignement concerne la maturité inégale des technologies et des applications quantiques. Dans les cas d'usage liés à la sécurité comme dans ceux liés à la finance, les progrès sont très hétérogènes. Alors que la cryptographie post-quantique progresse grâce à la normalisation et aux efforts d'intégration précoce, d'autres approches, telles que

les techniques de communication quantique ou les applications de l'informatique quantique, restent largement expérimentales. En pratique, la plupart des cas d'usage explorés s'appuient sur des architectures hybrides classiques-quantiques, et leur pertinence dépend de la structure du problème, de l'intégration du système et des contraintes opérationnelles plutôt que de la performance de calcul brute.

Un troisième enseignement concerne les implications au niveau des systèmes associées aux technologies quantiques. L'accès à des ressources de calcul spécialisées et la dépendance vis-à-vis d'un nombre limité de fournisseurs peuvent contribuer à des effets de concentration et à des dépendances partagées.

Enfin, l'analyse met en évidence le rôle central de l'incertitude en tant que caractéristique structurelle du paysage quantique. Les progrès scientifiques, la faisabilité technique et les délais de déploiement restent difficiles à prévoir, et les hypothèses d'un développement linéaire ou uniforme ont peu de chances de se vérifier. Par conséquent, il est tout aussi important de comprendre les arbitrages, les limites et les voies alternatives que d'identifier les domaines potentiels de bénéfices.

3.2 Défis en matière de compétences, de gouvernance et de surveillance

Au-delà des considérations technologiques, l'exploration des technologies quantiques dans le secteur financier soulève un ensemble de défis transversaux liés aux compétences, à la gouvernance et à la surveillance. Ces défis ne constituent pas un domaine d'impact distinct, mais façonnent plutôt la manière dont les évolutions liées au quantique sont comprises, évaluées et gérées au sein des institutions.

L'expérimentation des technologies quantiques s'appuie actuellement sur une expertise hautement spécialisée et interdisciplinaire, combinant des éléments de cryptographie, de cybersécurité, d'informatique, de physique et de mathématiques appliquées. Dans le contexte financier, cette expertise doit s'appuyer sur une compréhension des infrastructures financières, de la gestion des risques et des cadres réglementaires. Les différences d'expertise entre les institutions peuvent influencer à la fois la portée de l'expérimentation et la capacité à évaluer de manière critique les solutions externes.

Les dispositifs de gouvernance jouent un rôle tout aussi important. Les décisions relatives aux technologies quantiques recoupent souvent plusieurs fonctions organisationnelles, notamment les domaines technologiques, de la gestion des risques, du droit et des politiques. La gestion de ces interactions nécessite des structures de gouvernance capables de tenir compte de l'incertitude technique tout en restant en phase avec les mandats institutionnels et la tolérance au risque.

Du point de vue de la surveillance, les techniques quantiques peuvent accentuer les défis existants. L'utilisation croissante d'outils analytiques complexes, en particulier lorsqu'ils sont combinés à des méthodes avancées d'optimisation ou d'apprentissage automatique, soulève des questions de transparence, de validation et de responsabilité des modèles. Pour les autorités de surveillance, l'évaluation de ces outils nécessite non seulement une compréhension technique, mais aussi des cadres appropriés pour la documentation, les tests et l'auditabilité. Ces considérations peuvent être encore aggravées lorsque les outils ou composants quantiques sont fournis par des prestataires externes ou dans le cadre d'accords de services transfrontaliers.

Dans l'ensemble, les défis à relever en matière de compétences, de gouvernance et de surveillance montrent que les implications des technologies quantiques pour le système financier vont bien au-delà de la faisabilité technique. Elles influencent la manière dont les risques sont identifiés, dont les avantages sont évalués et dont la confiance et la responsabilité sont préservées à mesure que de nouvelles technologies sont explorées.

Conclusion – Vers une préparation éclairée et coordonnée

4.1 Réaffirmer le rôle d'un dialogue éclairé

Les technologies quantiques continuent d'évoluer dans un contexte marqué par l'incertitude scientifique, des progrès inégaux et des horizons à plus long terme. Dans un tel environnement, une compréhension commune et structurée des implications potentielles pour le système financier est essentielle. Le présent rapport a cherché à contribuer à cet objectif en examinant comment les technologies quantiques peuvent interagir avec les infrastructures, les activités et les cadres institutionnels du secteur financier.

Ce document vise à clarifier les enjeux clés sans anticiper les résultats technologiques ni les décisions des autorités. n dialogue public et professionnel fondé sur une compréhension partagée peut favoriser un engagement constructif, réduire le risque d'interprétation erronée et renforcer la préparation collective au sein des institutions.

4.2 Perspectives

À l'avenir, les technologies quantiques devraient demeurer un domaine de recherche et d'expérimentation intense au sein des communautés scientifiques, industrielles et institutionnelles. Leur pertinence pour le système financier continuera de dépendre des progrès technologiques, des efforts de normalisation et des pratiques de gouvernance, ainsi que des tendances plus générales en matière de numérisation et de calcul intensif de données.

Dans ce contexte en constante évolution, la préparation s'apparente davantage à un effort analytique continu qu'à un plan d'action figé. Une veille continue, l'échange de connaissances et le dialogue intersectoriel resteront essentiels en vue d'une évaluation éclairée et coordonnée.

Annexes

Annexe 1 – Approches complémentaires résistantes aux attaques quantiques

Outre la cryptographie post-quantique, plusieurs autres approches sont à l'étude pour renforcer la sécurité des données et des communications face à d'éventuelles menaces quantiques. Ces approches diffèrent par leurs principes sous-jacents, leur maturité technique et leurs modèles de déploiement, et peuvent compléter les solutions cryptographiques dans des contextes spécifiques plutôt que de les remplacer.

L'une de ces approches est l'échange de clés symétriques distribuées (DSKE). Le DSKE s'appuie sur des techniques cryptographiques symétriques, généralement considérées comme moins affectées par l'informatique quantique que les schémas à clé publique largement utilisés, combinées à un réseau de composants de confiance chargés de coordonner la distribution des clés. Cependant, le maintien de marges de sécurité adéquates dans un contexte quantique peut encore nécessiter des ajustements tels que l'augmentation de la longueur des clés et la révision des implémentations. Dans ce modèle, les parties communicantes établissent des clés secrètes partagées par le biais d'un aléatoire pré-distribué et de mécanismes d'échange contrôlés, plutôt que par le biais de la cryptographie à clé publique.

Parallèlement, le DSKE introduit des considérations opérationnelles spécifiques. Il nécessite généralement de s'appuyer sur des intermédiaires ou des prestataires de services de confiance pour gérer la fourniture des clés, la coordination et la gestion de leur cycle de vie. Cela soulève des questions liées à la gouvernance, aux dépendances vis-à-vis de tiers et à la résilience, en particulier dans les environnements où la haute disponibilité et la tolérance aux pannes sont essentielles. En conséquence, le DSKE peut s'avérer plus adapté à des cas d'usage ciblés impliquant des échanges de données hautement sensibles, plutôt qu'en tant que remplacement généralisé des infrastructures cryptographiques existantes.

Une autre approche qui retient l'attention est la distribution de clés quantiques (QKD), qui utilise les propriétés fondamentales de la mécanique quantique pour permettre l'échange de clés cryptographiques offrant de solides garanties de sécurité. Dans les systèmes QKD, toute tentative d'interception ou de mesure des états quantiques pendant la transmission introduit des perturbations détectables, permettant aux parties en communication d'identifier une éventuelle écoute clandestine. Une fois qu'une clé secrète partagée a été établie via un canal quantique, des

techniques cryptographiques symétriques classiques peuvent être utilisées pour chiffrer les données [7] .

La QKD offre un modèle de sécurité conceptuellement distinct, souvent décrit comme une sécurité fondée sur la théorie de l'information sous certaines hypothèses spécifiques. Cependant, les implémentations actuelles se heurtent à des limites pratiques. Les déploiements de QKD nécessitent généralement une infrastructure physique dédiée, telle que des liaisons par fibre optique ou des connexions par satellite, et sont souvent limités par la distance, le coût et le passage à l'échelle. L'intégration avec les réseaux de communication existants peut s'avérer complexe, et un déploiement à grande échelle peut nécessiter des investissements et une coordination importante. Comme pour d'autres solutions basées sur des infrastructures, les considérations liées à l'interopérabilité, aux écosystèmes des fournisseurs et à la maintenance à long terme sont essentielles pour évaluer la faisabilité.

Le DSKE comme la QKD montrent que la sécurité quantique ne se limite pas à une seule voie technologique. Au contraire, différentes approches peuvent être combinées ou appliquées de manière sélective, en fonction de la sensibilité des données, du niveau d'assurance requis et du contexte opérationnel. Dans certains cas, on peut envisager des architectures de sécurité en couches, où l'agilité cryptographique, le chiffrement symétrique et des canaux sécurisés dédiés sont utilisés conjointement pour renforcer la résilience globale.

Au-delà des mécanismes d'échange de clés, d'autres domaines de recherche sont également pertinents pour la sécurité quantique. Il s'agit notamment d'approches visant à protéger les données pendant le calcul, telles que l'informatique quantique confidentielle ou aveugle, ainsi que l'utilisation des technologies de capteurs quantiques susceptibles d'influencer la détection d'interférences ou d'altérations dans les systèmes de communication. Bien que bon nombre de ces techniques en soient encore à un stade précoce, elles soulignent l'ampleur des recherches en cours pour répondre aux défis de sécurité liés à l'informatique quantique.

Prises dans leur ensemble, ces approches complémentaires soulignent que le renforcement de la résilience quantique implique des arbitrages plutôt que des solutions universelles. Les différences en matière de maturité, de coût, d'évolutivité et d'exigences de gouvernance impliquent que l'adéquation de chaque approche doit être évaluée en fonction du contexte. La compréhension de ces caractéristiques constitue donc un élément important pour évaluer la manière dont les technologies quantiques peuvent interagir avec les fondements de la sécurité du système financier.

Annexe 2 – Considérations transversales

Les implications des technologies quantiques en matière de sécurité des données et des communications ne peuvent être pleinement comprises à travers les technologies individuelles ou les seuls cas d'usage. Elles sont déterminées par un ensemble de facteurs transversaux qui influencent la manière dont les approches résistantes aux attaques quantiques sont évaluées, déployées et maintenues au sein d'infrastructures financières complexes. Ces facteurs concernent en particulier l'interopérabilité, les dépendances opérationnelles, les dispositifs de gouvernance et la disponibilité des compétences pertinentes.

L'interopérabilité et la complexité de la transition constituent une considération centrale. Les systèmes financiers sont fortement interconnectés et impliquent souvent de multiples institutions, infrastructures et prestataires de services opérant dans différentes juridictions. Les mécanismes cryptographiques sont profondément intégrés dans les protocoles, les composants logiciels et les chaînes de traitement opérationnels. À mesure que des approches résistantes aux attaques quantiques sont mises en place, des systèmes s'appuyant sur des normes cryptographiques ou des architectures de sécurité différentes pourraient devoir coexister pendant de longues périodes. Garantir une interaction sécurisée et fiable entre ces systèmes constitue donc un défi majeur, en particulier pendant les phases de transition au cours desquelles des composants hérités et mis à jour fonctionnent en parallèle.

[7] Dans un contexte quantique, le maintien de marges de sécurité adéquates pour le chiffrement symétrique implique généralement d'augmenter la longueur des clés (par exemple, passer de clés de 128 bits à des clés de 256 bits) et de revoir les implémentations associées. De tels ajustements peuvent nécessiter de recenser les dépendances cryptographiques et de mettre à jour les configurations si nécessaire.

Les dépendances opérationnelles et les risques liés aux tiers constituent une autre dimension importante. De nombreuses approches résistantes aux attaques quantiques, qu'elles soient cryptographiques ou basées sur une infrastructure, s'appuient sur des fournisseurs externes pour la mise en œuvre, la maintenance ou des services clés. Cela inclut les bibliothèques logicielles, les composants matériels, l'infrastructure de communication et les prestataires de services spécialisés. Par conséquent, les choix liés aux technologies de sécurité peuvent influencer les structures de dépendance, le risque de concentration et la résilience face aux perturbations. L'évaluation de ces dépendances nécessite de prêter attention non seulement aux performances techniques, mais aussi aux modèles de gouvernance, aux dispositions contractuelles et à la viabilité à long terme des écosystèmes de fournisseurs.

L'agilité cryptographique et la gouvernance jouent également un rôle critique. Compte tenu des recherches en cours en matière de cryptanalyse classique et quantique, aucune solution cryptographique ne peut être considérée comme sécurisée indéfiniment. La capacité à adapter les mécanismes de sécurité au fil du temps, en mettant à jour les algorithmes, les paramètres ou la mise en œuvre, est donc une propriété importante des systèmes résilients. Cette agilité est influencée par les choix de conception effectués au niveau architectural, ainsi que par les processus de gouvernance institutionnelle qui déterminent la manière dont les changements sont évalués, testés et déployés. Des rôles, des structures décisionnelles et des mécanismes de coordination clairs peuvent favoriser une gestion plus efficace de l'évolution cryptographique.

Les compétences et l'état de préparation opérationnelle constituent un autre défi transversal. Une sécurité à l'épreuve du quantique requiert une expertise couvrant la cryptographie, la cybersécurité, l'architecture des systèmes et, de plus en plus, les technologies quantiques elles-mêmes. Ces compétences interdisciplinaires restent rares, et la demande devrait croître à mesure que les considérations liées au quantique prendront de l'importance. Au-delà de l'expertise technique, les organisations ont également besoin de capacités opérationnelles pour recenser les dépendances cryptographiques, surveiller les risques émergents et gérer des transitions complexes. Les limites en matière de compétences et de ressources peuvent donc déterminer à la fois le rythme et l'ampleur de l'adoption.

Prises dans leur ensemble, ces considérations transversales soulignent que la sécurité quantique n'est pas uniquement une question technique. Elle est étroitement liée à des facteurs organisationnels, opérationnels et de gouvernance qui influencent la manière dont les risques sont évalués et gérés dans l'ensemble du système financier. La compréhension de ces dimensions peut aider à encadrer les discussions sur la résilience quantique d'une manière qui tienne compte de la complexité, de l'interdépendance et de l'incertitude, sans présumer de solutions ou de trajectoires uniformes.

Annexe 3 – Algorithmes quantiques d'intérêt

L'annexe 3 fournit un aperçu non exhaustif et purement informatif d'une sélection d'algorithmes quantiques fréquemment cités dans la littérature universitaire. Le tableau n'implique pas d'applicabilité pratique, de maturité technologique ou de déploiement à court terme dans des contextes financiers. Il vise uniquement à faciliter la compréhension technique des concepts couramment abordés dans le cadre de la recherche sur l'informatique quantique.

Algorithme	Objectif principal	Pertinence	État de maturité
Algorithme de Shor	Factorisation efficace et logarithmes discrets	Menace pour RSA, ECC et les systèmes à clé publique associés	Théorique ; nécessite des ordinateurs quantiques tolérants aux fautes
Algorithme de Grover	Accélération quadratique pour la recherche non structurée	A un impact sur les considérations relatives à la longueur des clés en cryptographie symétrique	Théorique ; limité par l'échelle matérielle

HHL (Harrow–Hassidim–Lloyd)	Résolution de systèmes d'équations linéaires	Intérêt théorique pour la modélisation financière et l'analyse des risques	Expérimental ; fortes contraintes sur les entrées/sorties
Estimation de l'amplitude quantique (QAE)	Amélioration de l'échantillonnage et de l'estimation des probabilités	Simulations de Monte Carlo, estimation des risques	Expérimental ; hypothèses fortes sur le codage des données et les propriétés des matrices
Algorithme d'optimisation approximative quantique (QAOA)	Optimisation combinatoire	Optimisation de portefeuille, allocation des ressources	Recherche expérimentale à l'ère NISQ
Recuit quantique	Optimisation heuristique	Planification, problèmes de portefeuille	Matériel disponible dans le commerce (portée limitée)
Algorithmes d'apprentissage automatique quantique (divers, par exemple QSVM)	Méthodes du noyau, cartographie des caractéristiques	Reconnaissance de formes, détection d'anomalies	Très expérimental
Méthodes de réseaux de tenseurs (d'inspiration quantique)	Approximation classique efficace des systèmes à haute dimension	Optimisation, apprentissage automatique	Classique ; déjà déployable