Swiss Banking

QuantumBasel

Quantum Computing in Banking

Fonctionnement, domaines d'application et recommandations pour les banques suisses

Novembre 2024

Rapport d'expertise de l'ASB

Executive Summary

Les systèmes informatiques sont très sollicités par les banques, dont les besoins vont croissant. Avec l'augmentation constante du volume de données et le recours accru à l'intelligence artificielle (IA), ils pourraient atteindre bientôt leurs limites de performance. Dans ce contexte, les regards se tournent de plus en plus vers l'informatique quantique. Cette technologie, qui relevait auparavant de la science-fiction, est devenue ces dernières années une réalité scientifique et elle ne tardera pas à franchir les portes des laboratoires pour s'installer dans notre secteur. Il ne s'agit donc plus de savoir si elle s'imposera, mais quand et de quelle manière.

Même si l'informatique quantique est régie par des principes physiques difficiles à appréhender et si elle n'est pas encore généralisée, ses impacts potentiels sur le secteur financier sont de plus en plus manifestes. Cette technologie constitue une opportunité, mais aussi un défi. Capables d'effectuer des calculs et des simulations complexes avec à la fois davantage d'efficacité et davantage de précision, les ordinateurs quantiques ouvrent de nouvelles perspectives d'utilisation. Le présent rapport d'experts identifie et éclaire à l'aide d'exemples quatre domaines d'application de l'informatique quantique dans le secteur bancaire:

- **En matière de gestion et de surveillance des risques,** les ordinateurs quantiques permettent d'analyser les interdépendances complexes entre actifs et dérivés, ainsi que d'assurer une surveillance quasiment en temps réel.
- **En matière de gestion de portefeuille,** les ordinateurs quantiques facilitent l'optimisation des portefeuilles grâce à des calculs parallèles et à de meilleures simulations, d'où une hausse potentielle des rendements.
- **En matière de trading algorithmique,** les ordinateurs quantiques offrent la possibilité d'utiliser des algorithmes plus efficaces et plus précis pour le négoce sur les marchés financiers.
- Enfin, grâce aux ordinateurs quantiques, il devient possible de **créer et d'entraîner des modèles d'IA** à moindre coût et plus rapidement, ce qui permet ensuite de disposer de modèles prédictifs plus efficaces et plus précis pour les applications professionnelles courantes.

«La question fondamentale n'est plus de savoir si cette technologie s'imposera, mais quand et de quelle manière.»

Si l'informatique quantique crée des opportunités, elle génère aussi de nouveaux risques, qu'il y a lieu de prévenir notamment en prévoyant des procédés cryptographiques post-quantiques. Compte tenu des risques inhérents aux attaques dites «harvest now, decrypt later» et de la longueur des délais nécessaires à la mise en place d'une cryptographie post-quantique, l'informatique quantique constitue d'ores et déjà un défi à ne pas négliger.

Les auteurs recommandent donc aux différents niveaux concernés les mesures suivantes:

- Les **banques** devraient adapter en permanence leurs directives existantes en matière de sécurité et élaborer une feuille de route en vue d'introduire une cryptographie post-quantique. En partenariat avec des organisations et des organismes de recherche spécialisés, elles devraient également assurer un développement continu de leurs compétences en matière d'informatique quantique, afin d'accroître leur agilité dans la perspective du déploiement à large échelle de cette technologie. Entre notamment dans ce cadre le soutien du secteur bancaire à la recherche appliquée au sein des universités et des organismes de recherche suisses, ce qui permettra de renforcer le savoir-faire de part et d'autre et de disposer à l'avenir d'un réservoir de talents suffisant.
- Les **autorités réglementaires et de surveillance** en matière financière devraient nourrir un dialogue régulier avec la branche, afin de connaître les domaines d'application de l'informatique quantique dans le secteur financier et d'identifier en amont les éventuelles mesures à prendre. Sur le plan réglementaire, il ne semble pas nécessaire selon nous d'intervenir dans l'immédiat. La réglementation actuelle, qui est neutre sur le plan de la technologie et fondée sur des principes, couvre suffisamment les risques potentiels liés au recours à l'informatique quantique.
- Afin d'assurer durablement la compétitivité et la capacité d'innovation de la **place financière suisse** ainsi que sa résilience, il est essentiel de s'appuyer sur les nouvelles technologies comme l'informatique quantique, l'IA et la technologie des registres distribués (TRD). Cela suppose une collaboration étroite et pérenne de la branche avec les organismes de recherche, des canaux de communication rapides ainsi qu'une volonté et une capacité d'adaptation solides de la part des établissements financiers. Cette formule gagnante devra être préservée et développée à l'avenir.

Les personnes décisionnaires au sein du secteur financier, des autorités et des milieux politiques doivent poser dès à présent les jalons qui, au cours des décennies à venir, leur permettront non seulement d'exploiter pleinement les opportunités liées à l'informatique quantique dans le secteur financier, mais aussi d'identifier et d'atténuer en temps utile les risques y afférents. Grâce à cette approche proactive, elles créeront des conditions-cadres optimales pour une place financière suisse compétitive, innovante et résiliente – aujourd'hui comme demain.

«Les banques devraient adapter en permanence leurs directives existantes en matière de sécurité et élaborer une feuille de route en vue d'introduire une cryptographie post-quantique.»

1 Bases de l'informatique quantique

L'image d'une pièce de monnaie en rotation rapide sur sa tranche est une excellente métaphore de ce qui constitue le cœur de l'informatique quantique. Dans les ordinateurs conventionnels, le bit est la plus petite unité d'information, comparable aux deux côtés d'une pièce de monnaie – pile ou face, 0 ou 1. Mais dans les ordinateurs quantiques, les informations sont stockées en bits quantiques ou qubits. Comme une pièce de monnaie en rotation, qui semble faire apparaître simultanément son côté pile et son côté face, un qubit peut se trouver dans un état dit de superposition, où il représente simultanément une combinaison de 0 et de 1 (voir encadré: «Le fonctionnement des ordinateurs quantiques»).

Cette superposition constitue la base du développement des algorithmes quantiques, qui résolvent des problèmes de manière totalement inédite – en dépassant de loin les capacités des ordinateurs conventionnels. L'informatique quantique permet d'effectuer plus efficacement et plus rapidement des calculs et des simulations complexes, qui exigeaient jusqu'ici un travail considérable et n'aboutissaient qu'à des approximations. C'est donc une technologie qui pourrait être extrêmement utile dans le secteur bancaire, où les simulations et les analyses par scénarios sont aussi complexes qu'omniprésentes et où l'on traite d'énormes quantités de données.

Mais comme celui d'une pièce de monnaie en rotation, l'état d'un qubit est extrêmement instable et peut très vite changer ou disparaître. Les ordinateurs quantiques doivent donc souvent travailler dans des environnements extrêmement stables et fortement réfrigérés, car même les perturbations les plus minimes risquent d'affecter les fragiles qubits et de rendre les calculs inutilisables. En Suisse, des établissements universitaires comme l'EPFZ, l'EPFL et l'Université de Bâle contribuent grandement à la recherche fondamentale en informatique quantique, notamment dans les domaines de la sensorique quantique, de la cryptographie quantique et de la simulation quantique. De même, des initiatives nouvelles comme QuantumBasel, des start-ups et des entreprises technologiques établies jouent un rôle important dans le développement d'applications. Les Etats du monde entier investissent des sommes considérables dans la recherche quantique, à la fois pour s'assurer des avantages compétitifs et pour prévenir d'éventuelles cyberattaques.[1]

Ces acteurs se concentrent non seulement sur le progrès technologique, mais aussi sur les risques prévisibles. Un de ces risques réside dans la capacité des ordinateurs quantiques de casser certains des procédés cryptographiques courants, utilisés aussi dans les systèmes informatiques des banques. Ces dernières, de même que les autorités réglementaires et de surveillance, s'emploient donc d'ores et déjà à développer une cryptographie post-quantique.

Les évolutions en matière d'informatique quantique et de cryptographie quantique auront sur le système financier un impact aussi fort que celui de l'intelligence artificielle (IA) et de ses grands modèles de langage (*large language models*, LLM) observé aujourd'hui dans divers domaines. Dès lors, c'est l'informatique quantique qui focalise ici l'attention, davantage que d'autres technologies quantiques comme la communication quantique et la sensorique quantique.

---

1 Forbes, Quantum Computing Takes Off With $55 Billion In Global Investments (2024)

Le fonctionnement des ordinateurs quantiques

Les ordinateurs conventionnels traitent des informations sous forme de bits. Ces derniers se matérialisent par des tensions électriques (ou impulsions électriques) qui sont soit supérieures, soit inférieures à un seuil donné, ce qui permet de définir les états binaires 0 et 1. Les calculs s'effectuent grâce à des portes logiques créées par des transistors. Ces portes sont reliées entre elles dans des circuits complexes, qui permettent à l'ordinateur d'exécuter différentes opérations de calcul.

Les ordinateurs quantiques en revanche reposent sur les principes de la mécanique quantique, c'est-à-dire sur les lois physiques qui déterminent le comportement de particules comme les atomes et les électrons. En informatique quantique, les informations sont portées par ce qu'il est convenu d'appeler des qubits. Les qubits peuvent être créés dans différents systèmes physiques – par exemple atomes, ions, photons ou matériaux supraconducteurs. Chacun de ces systèmes a ses avantages et ses inconvénients. Leur point commun, c'est qu'ils utilisent des effets propres à la mécanique quantique comme l'interférence, la superposition et l'intrication pour résoudre des problèmes selon des approches radicalement nouvelles.

Dans l'univers de l'informatique conventionnelle, les combinaisons possibles de deux bits sont 00, 01, 10 et 11, soit quatre états. Mais dans l'univers de l'informatique quantique, deux qubits ne sont pas limités à ces quatre états, ils peuvent les superposer. En d'autres termes, ils peuvent cumuler tous ces états simultanément et ainsi tous les utiliser dans leurs calculs. Cette capacité d'exploiter de nombreux états en parallèle explique les énormes avantages liés aux algorithmes quantiques. La puissance de calcul double à chaque qubit ajouté: un processeur de 51 qubits est théoriquement deux fois plus puissant qu'un autre de 50 qubits. Cette scalabilité exponentielle est l'une des raisons pour lesquelles l'informatique quantique a fait de tels progrès ces dernières années. Elle permet aussi de comprendre pourquoi les banques et d'autres entreprises n'hésitent pas à investir dans cette technologie, malgré sa jeunesse.

Limites technologiques et structurelles de l'informatique quantique

L'informatique quantique opère à la limite de ce qui est techniquement faisable et physiquement possible aujourd'hui. Un ordinateur quantique d'une puissance de 400 qubits, par exemple, est capable de générer davantage d'états qu'il n'y a d'atomes dans l'univers visible. Mais pour développer cette technologie, quelques obstacles restent à être franchis:

- **Correction d'erreurs:** les ordinateurs quantiques étant extrêmement sujets aux erreurs, ils nécessitent de puissants mécanismes de correction. Les algorithmes de correction d'erreurs ne cessent de s'améliorer et l'on développe en permanence de nouveaux procédés plus performants.[2]
- **Scalabilité:** la scalabilité des ordinateurs quantiques crée des difficultés supplémentaires, par exemple en ce qui concerne la correction parallèle d'erreurs ou la fiabilité des portes quantiques – les éléments de base des ordinateurs quantiques, qui permettent de manipuler des qubits dans plusieurs états simultanément.

2 Par exemple, Amazon Web Services (AWS) a présenté en mars 2024 un nouveau procédé qui rend la correction d'erreurs plus performante.

- **Logiciels:** les logiciels, développés initialement pour les ordinateurs classiques, constituent un goulot d'étranglement pour les ordinateurs quantiques. Ces derniers ne déploieront donc pleinement leur potentiel que si l'on améliore les algorithmes, les langages de programmation et les outils d'optimisation.
- **Normes et protocoles:** pour le moment, les diverses plateformes d'ordinateurs quantiques sont rarement compatibles entre elles. Cependant, la tendance qui s'affirme est d'utiliser des systèmes différents pour des applications distinctes.
- **Flux de données:** penser que les ordinateurs quantiques ont pour principale utilité de résoudre des problèmes de *big data* est une idée fausse. En réalité, il reste difficile d'introduire de grandes quantités de données dans ces systèmes. Les progrès réalisés, notamment en ce qui concerne la mémoire vive quantique, sont prometteurs, mais les applications en temps réel ne sont pas forcément pour demain.
- **Pénurie de main d'œuvre qualifiée:** certes, il y a de plus en plus de chercheuses et de chercheurs en informatique quantique en Suisse, mais le nombre des personnes en formation dans ce domaine est insuffisant pour constituer le réservoir de talents nécessaire. Malgré l'engagement d'un certain nombre d'universités comme l'EPFZ, où quelque 500 personnes se consacrent à l'informatique quantique, la pénurie de main d'œuvre qualifiée reste un obstacle majeur.

«Compte tenu des limites technologiques et structurelles actuelles, les ordinateurs quantiques ne remplaceront pas les ordinateurs conventionnels, mais ils les complèteront.»

L'année 2019, où Google a réussi à démontrer que les ordinateurs quantiques permettaient d'accomplir certaines tâches plus rapidement que les ordinateurs conventionnels, marque une étape clé dans le développement des ordinateurs quantiques.[3] Même si ce succès reste pour l'heure sans grande incidence pratique, il démontre le potentiel des ordinateurs dits *noisy intermediate-scale quantum* (NISQ), emblématiques du niveau de développement actuel de cette technologie (voir graphique 1).

Ces évolutions ont incité de nombreuses entreprises technologiques de renom à présenter des feuilles de route ambitieuses en vue de poursuivre le développement d'ordinateurs quantiques. IBM, en particulier, a élaboré une planification détaillée à l'horizon 2029.[4] Les banques et d'autres organisations peuvent s'inspirer de ces feuilles de route afin de déterminer le moment optimal pour développer leurs propres applications et assurer ainsi leur compétitivité à l'ère de l'informatique quantique.

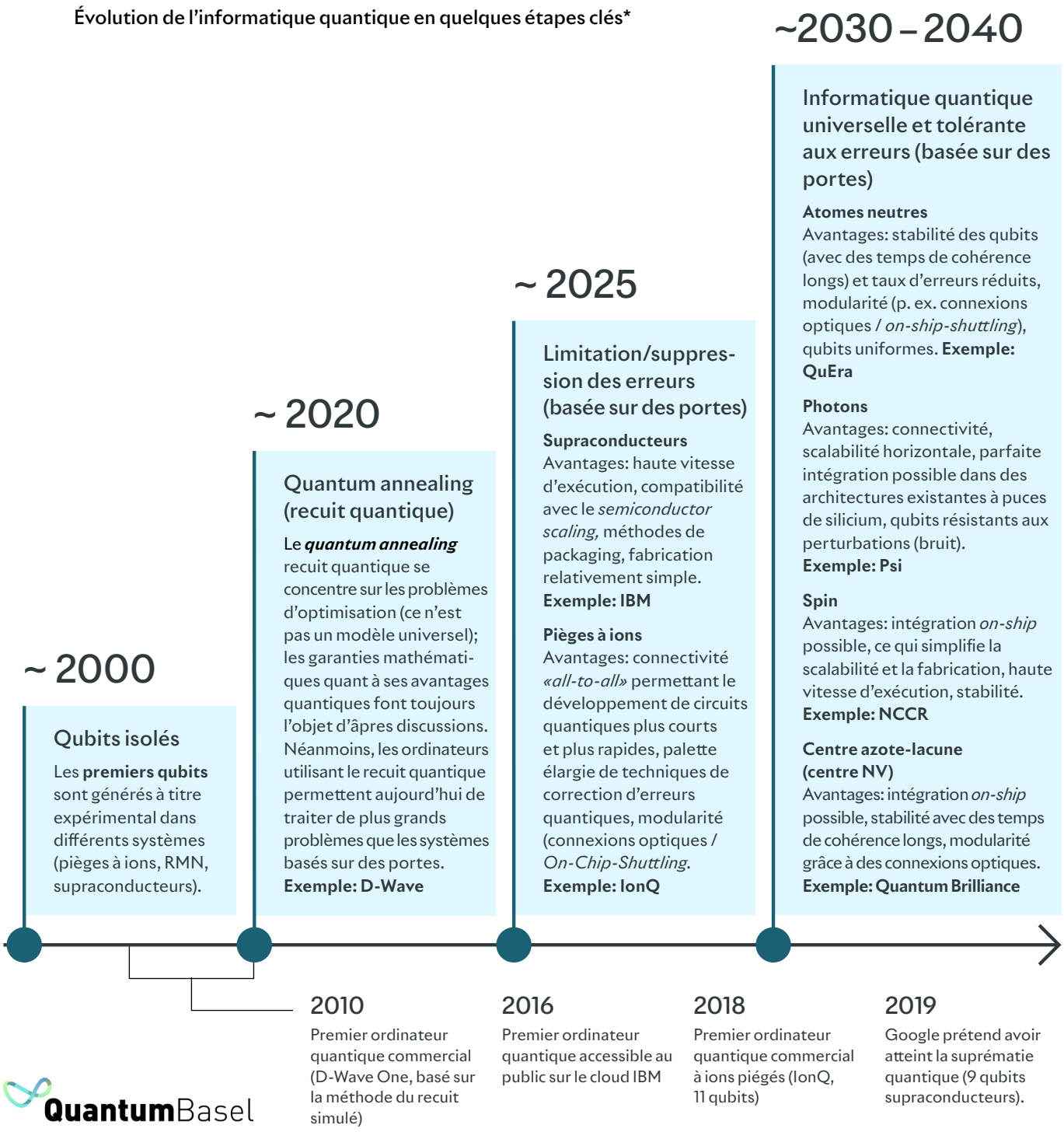
Compte tenu des limites technologiques et structurelles actuelles, les ordinateurs quantiques ne remplaceront pas les ordinateurs conventionnels ces prochaines années, voire ces prochaines décennies, mais ils les complèteront. Leurs avantages se manifesteront principalement dans le traitement des tâches nécessitant une forte puissance de calcul, pour lesquelles des algorithmes quantiques spécifiques ont déjà été développés. Les systèmes dits «hybrides quantiques/classiques», qui associent les deux types d'ordinateurs, tirent le meilleur parti des fonctionnalités des uns et des autres et ouvrent ainsi des perspectives prometteuses dans divers domaines d'application.

3 Nature, Google uncovers how quantum computers can beat today's best supercomputers (2024)

4 IBM, Quantum roadmap (2024)

Graphique 1

Évolution de l'informatique quantique en quelques étapes clés*



* Aperçu non exhaustif. Les évolutions étant opérées sur plusieurs années, les dates indiquées sont de simples repères temporels.

Source: QuantumBasel, sur la base des travaux du Forum économique mondial, de The Quantum Insider et de McKinsey.[5,6,7]

5 World Economic Forum (WEF), State of Quantum Computing (2022)

6 The Quantum Insider, The History of Quantum Computing (2024)

7 McKinsey Digital, Enabling the next frontier of quantum computing (2024)

2 Domaines d'application concrets dans le secteur bancaire

On ignore encore quand précisément les ordinateurs quantiques se déploieront à large échelle. Les prévisions varient entre la fin de la décennie 2020 et la fin de la décennie 2030. Malgré cette incertitude quant à la vitesse du développement technologique, c'est le moment pour les banques de prendre des initiatives. Il leur est déjà possible d'acquérir un savoir-faire et de le tester dans de premières applications. Ces applications reposent sur le choix d'algorithmes quantiques en fonction des problèmes concrets qui se posent au sein de la branche. La littérature spécialisée distingue globalement entre trois catégories principales d'algorithmes quantiques:

1. Simulation chimique et physique
2. Apprentissage machine et IA
3. Optimisation

La première catégorie ne concerne pas les banques. Les algorithmes quantiques des deuxième et troisième catégories, en revanche, se prêtent à de multiples applications dans le secteur financier, qui seront examinées de plus près ci-dessous. Il faut cependant savoir à cet égard que la valeur ajoutée des algorithmes quantiques varie selon les applications – dans certains cas c'est la vitesse, dans d'autres la précision et la qualité des modèles (y compris lorsque les données d'entraînement sont incomplètes), dans d'autres encore l'efficacité énergétique. En conséquence, la clé du succès lorsqu'on utilise un ordinateur quantique est toujours de choisir des algorithmes adaptés aux applications concernées.

D'ores et déjà et sans l'informatique quantique, l'IA a permis au secteur financier de réaliser des progrès considérables, notamment dans les domaines de l'analyse des risques ou des modèles prédictifs statistiques.[8] Avec l'informatique quantique, les avantages de l'IA pourraient être démultipliés, dans la mesure où l'on développerait plus vite et à moindre coût des modèles d'IA plus précis, utilisés ensuite dans des systèmes conventionnels. D'où, potentiellement, une symbiose: les ordinateurs quantiques contribuent à une meilleure qualité et à une plus grande efficacité des modèles d'IA,[9] l'IA favorise quant à elle le développement d'ordinateurs quantiques plus puissants,[10] par exemple en améliorant les procédures ou les méthodes expérimentales.

Par ailleurs, des applications comme la gestion des risques, la gestion de portefeuille ou la fixation du prix des dérivés nécessitent une énorme puissance de calcul. A l'ère des transactions instantanées, les besoins ne cessent d'augmenter en termes de capacité de traitement, de sorte que les banques doivent disposer d'ordinateurs performants pour rester compétitives. Les développements ci-après présentent quelques-uns des domaines d'application immédiatement pertinents de l'informatique quantique dans le secteur bancaire.

---

8 University of Technology Sydney, Australia, AI in Finance: Challenges, Techniques and Opportunities (2021)

9 Jerbi, S., Fiderer, L.J., Poulsen Nautrup, H. et al. Quantum machine learning beyond kernel methods (2023)

10 Krenn M., Landgraf J., Foesel T. and Marquardt F. Artificial intelligence and machine learning for quantum technologies, (2023)

2.1 Gestion et surveillance des risques

Les ordinateurs quantiques recèlent un potentiel particulièrement important en matière de gestion des risques. Selon l'association sectorielle britannique UK Finance, l'analyse des interactions complexes entre les actifs et leurs dérivés constitue aujourd'hui un défi de taille pour les banques.[11] Des établissements comme Goldman Sachs, J.P. Morgan, Citi et HSBC recourent déjà à l'informatique quantique pour tenter d'appréhender plus en amont et plus précisément les risques extrêmes *(tail risks)*. Une fois ces risques identifiés grâce à des algorithmes quantiques, il devient possible de mieux les localiser et les limiter à l'aide d'ordinateurs conventionnels. L'identification précoce des risques pourrait permettre également d'accélérer le reporting correspondant destiné aux autorités de surveillance.

A l'avenir, les ordinateurs quantiques pourraient être capables de surveiller et d'analyser quasiment en temps réel certains acteurs du marché voire des sous-marchés entiers. Mais pour le moment, ils n'ont pas encore la capacité de lire efficacement des volumes suffisants de données classiques, de sorte que les solutions reposeront à moyen terme sur des approches hybrides quantiques/classiques (y compris l'IA). De tels systèmes seraient à même d'analyser plus globalement les interdépendances entre les actifs, les dérivés, les intermédiaires, les gérants de portefeuille et la clientèle.

Dans bien des cas, les systèmes actuels ne peuvent que suivre les évolutions en cascade et, si la situation l'exige, déclencher des ordres stop sur certaines positions. Les systèmes quantiques, parce qu'ils sont capables de reconnaître des modèles complexes, pourraient identifier des déclencheurs, comprendre les mécanismes de propagation et de reproduction, mais aussi prendre en compte des interactions compliquées. Ils pourraient par exemple analyser en quoi les fluctuations de prix des sous-jacents et de leurs instruments de couverture sont liées, tout en intégrant les risques réels de contrepartie et de défaillance. Alors que ces risques sont souvent traités comme de simples constantes dans les systèmes actuels, et qu'il faut des heures, voire des jours, pour que leurs effets se manifestent, leur dynamique pourrait apparaître quasiment en temps réel grâce aux ordinateurs quantiques. Cela permettrait de prendre des décisions plus rapides et plus précises.

Par ailleurs, certaines banques centrales s'intéressent déjà au suivi des flux de paiement et collectent des données dans cette perspective. La Banque des règlements internationaux (BRI) a lancé plusieurs projets de recherche sur ce thème.[12]

2.2 Gestion de portefeuille

Dans le secteur financier, l'optimisation des portefeuilles est une des tâches les plus complexes. C'est aussi une des plus exigeantes en termes de puissance de calcul. Il s'agit à la fois d'aller vite et de prendre en compte simultanément de multiples facteurs interdépendants, qu'il faut recalculer sans cesse au regard de la frontière efficiente du portefeuille. Les banques travaillent sur la capacité d'accroître en permanence les portefeuilles traités tout en améliorant les solutions logicielles, pour arriver par exemple à simuler plusieurs stratégies de portefeuille en même temps. Sur certains marchés, en utilisant l'IA sur des ordinateurs conventionnels,

11 UK Finance, Minimising the risks: quantum technology and financial services (2023)

12 BRI, Project Pyxtrial: monitoring the backing of stablecoins (2024)

elles parviennent déjà à générer de l'alpha, c'est-à-dire un excédent de rendement par rapport à un indice de référence. A l'avenir, les ordinateurs quantiques et l'IA prédictive – une combinaison gagnante – devraient permettre d'atteindre des niveaux de rendement encore plus élevés par rapport aux indices du marché.

2.3 Procédés cryptographiques et approches post-quantiques

Le cryptage est un domaine d'application particulièrement important de l'informatique quantique, mais non dénué de risques – surtout lorsqu'il s'agit de casser des procédés cryptographiques actuels. Beaucoup des méthodes de cryptage utilisées aujourd'hui dans les systèmes informatiques des banques sont vulnérables aux ordinateurs quantiques. Par exemple, l'algorithme quantique de Shor constitue une menace pour les procédés de cryptographie asymétrique comme le cryptage RSA (Rivest-Shamir-Adleman), car il est capable d'accélérer la factorisation en nombres premiers de manière exponentielle. Quant à l'algorithme quantique de Grover, il impacte les procédés de cryptographie symétrique comme le cryptage AES *(advanced encryption standard)* en permettant une accélération quadratique de la vitesse de recherche dans des banques de données ou des listes non classées. Dans le cas des procédés symétriques, on peut certes atténuer cette vulnérabilité en doublant la longueur de la clé, mais cela a alors des effets directs sur la durée et l'efficacité du cryptage.

Le National Institute of Standards and Technology (NIST), leader mondial en la matière, s'attache depuis 2016 à développer de nouveaux procédés dits de cryptographie post-quantique (CPQ) – *post-quantum* en anglais, ou encore *quantum-proof, quantum-safe* ou *quantum-resistant*. En juillet 2022, le NIST a présenté quatre procédés: Crystals-Kyber, Crystals-Dilithium, Sphincs+ et Falcon. Les premiers ont été standardisés officiellement à l'été 2024.[13, 14] Ces procédés reposent toutefois sur des approches cryptographiques classiques auxquelles les ordinateurs quantiques n'apportent – autant que l'on sache – aucune valeur ajoutée.

Il existe également des approches cryptographiques qui s'appuient sur les lois de la mécanique quantique et sont donc même mathématiquement à l'abri des tentatives de décryptage, y compris par des ordinateurs quantiques. En pratique toutefois, ces méthodes sont souvent moins avancées dans leur développement que les protocoles classiques post-quantiques. On citera à titre d'exemple l'échange quantique de clé, où deux parties échangent des chiffres aléatoires et peuvent s'en servir pour communiquer de manière sécurisée via un masque jetable *(one-time pad)* ou d'autres protocoles.[15]

Enfin, des travaux sont déjà en cours pour crypter les données actuellement détenues par des prestataires de services financiers et d'autres institutions importantes selon des procédés post-quantiques. L'objectif est de prévenir les attaques dites «harvest now, decrypt later» dans le contexte de la cybersécurité, c'est-à-dire les vols de données commis aujourd'hui dans la perspective d'un décryptage ultérieur au moyen d'ordinateurs quantiques puissants.

---

13 A noter que le centre de recherche IBM installé à Rüschlikon, en Suisse, a joué un rôle important dans le développement de ces procédés.

14 NIST, NIST Releases First 3 Finalized Post-Quantum Encryption Standards (2024)

15 En Suisse, par exemple, l'entreprise ID Quantique développe la commercialisation de systèmes de communication quantique par échange quantique de clé.

2.4 Trading algorithmique

Le trading algorithmique (en abrégé: algo-trading) est une discipline établie depuis quelques décennies à l'interface entre les marchés financiers d'une part, les systèmes high-tech ultra-rapides et ultra-précis d'autre part. Dans ce cadre, les banques utilisent des algorithmes de plus en plus complexes pour réaliser des plus-values sur le marché des capitaux via un grand nombre de transactions individuelles. En pratique, il est toutefois très difficile de dégager régulièrement des plus-values nettes, car les systèmes d'algo-trading négocient souvent contre d'autres systèmes qui n'ont ni les mêmes perspectives, ni les mêmes paramètres. Certes, les systèmes basés sur l'IA produisent de meilleurs résultats dans certaines situations mais, dans les phases de brusques revirements de tendance, ils réagissent souvent trop lentement.

En matière d'algo-trading, les ordinateurs quantiques promettent des progrès considérables. Leur puissance de calcul permet non seulement de suivre plusieurs marchés en parallèle, mais aussi de remplacer les simulations de Monte-Carlo classiques par la méthode dite de l'estimation d'amplitude. Cette méthode aboutit à des modélisations stochastiques plus précises en traitant de moindres volumes de données.

2.5 IA spécifique aux banques et IA intersectorielle

La plupart des techniques et des méthodes d'IA sont applicables dans quasiment tous les domaines de l'économie, où la numérisation va croissant. De même, les grands modèles de langage sous-jacents peuvent être utilisés à l'identique au niveau intersectoriel. Avec le développement de l'informatique quantique, il est probable que ces systèmes d'IA progresseront encore en termes de vitesse, de précision, de qualité et d'efficacité énergétique.

Outre l'IA générale, il existe aussi des solutions d'IA spécifiques aux banques, axées sur les besoins particuliers du secteur financier – en particulier la gestion des risques et la gestion de portefeuille, les simulations en la matière, ainsi que le remplacement des hypothèses et des méthodes existantes par des approches plus précises. L'intégration de nouveaux facteurs et de nouveaux développements revêt également une importance croissante. Sont concernés notamment les dérivés financiers ainsi que le recours de plus en plus fréquent à la technologie des registres distribués (TRD) et/ou de la blockchain. En Suisse, cette dernière fait actuellement l'objet de tests dans le cadre de projets d'émission d'une monnaie numérique de banque centrale *(central bank digital currency,* CBDC) ou d'un franc suisse numérique.[16, 17]

16 BRI, Project Helvetia: a multi-phase investigation on the settlement of tokenised assets in central bank money (2024)

17 Swiss Banking, Les banques suisses signent un mémorandum d'entente afin d'étudier la faisabilité d'un jeton de monnaie scripturale en francs suisses émis conjointement (2024)

Musique d'avenir! Quelles autres applications peut-on imaginer dans le secteur financier?

Suivi de marchés financiers entiers et connaissance approfondie de l'économie réelle

Dès que les banques commenceront à utiliser des ordinateurs quantiques pour investir sur les marchés, il pourrait être opportun de surveiller ces marchés à la fois en largeur et en profondeur, afin d'être à même de prévenir en temps utile les risques de crise. L'observation ponctuelle de sous-marchés ou de flux de paiement particuliers, telle qu'elle se pratique actuellement, ne suffira plus – sachant qu'elle ne reflète déjà qu'imparfaitement la réalité.

Suivre des marchés financiers entiers ne sert pas qu'à identifier précocement les évolutions à risques. Cela permet aussi aux scientifiques et aux autorités de mieux connaître le fonctionnement de ces marchés et de l'économie réelle, y compris des mécanismes – par exemple la montée et la retombée des tendances inflationnistes – qui sont certes bien décrits, mais peu étudiés au niveau empirique.

Climat, durabilité, catastrophes naturelles et risques financiers en résultant

Les entreprises d'assurance et de réassurance sont souvent les premières à ressentir directement l'impact du changement climatique dans leurs activités opérationnelles et dans leurs bilans – suivies de près, voire accompagnées par les banques et les investisseurs privés, qui n'ont qu'un choix: soit assurer à grands frais les immeubles situés dans des zones à risques, soit les vendre. Les données disponibles, de plus en plus précises et nombreuses, permettent d'affiner les prévisions quant aux risques futurs potentiels. Si ces risques se réalisent et s'accumulent brusquement chez les prestataires de services financiers, il peut en résulter des effets en cascade sur l'ensemble du marché financier.

Dans ce contexte, la puissance des ordinateurs quantiques peut être mise à profit pour effectuer des simulations et des analyses complexes, à différents niveaux. Tout d'abord, elle est précieuse pour élaborer des modèles météorologiques et climatiques ainsi que, sur cette base, des modèles de risque intégrant des facteurs géologiques et topographiques. Elle permet en outre d'évaluer les risques consécutifs pour les particuliers et les entreprises, ainsi que d'analyser les problématiques susceptibles d'en résulter pour certains opérateurs financiers ou pour l'économie dans son ensemble.

Premières expériences dans le secteur bancaire

L'informatique quantique et les nouveaux procédés cryptographiques ne concernent pas seulement les banques à vocation internationale ou les grandes banques. Les petits et moyens établissements, eux aussi, peuvent tirer profit de l'informatique quantique combinée à l'IA. C'est ce qui ressort des expériences d'un certain nombre de précurseurs qui se sont déjà emparés de cette technologie et développent de premières applications.

Quelques exemples suisses

UBS
UBS s'intéresse concrètement à l'informatique quantique depuis 2018. Elle a institué des groupes de travail dédiés qui explorent des applications quantiques afin d'en quantifier les avantages dans le secteur financier et d'identifier les risques potentiels. Divers projets, par exemple en matière d'optimisation des portefeuilles et d'évaluation des dérivés financiers, ont déjà été testés avec des entreprises spécialisées. Dans le cadre d'un groupe de travail spécifique, UBS analyse les risques inhérents à l'informatique quantique et développe des mesures de prévention.

Banque Migros
Dans le cadre de sa gestion des risques et de la priorité qu'elle accorde à l'innovation numérique, la Banque Migros a démarré son «voyage quantique». En partenariat avec QuantumBasel, elle forme du personnel et évalue des applications en matière d'informatique quantique. Ce programme vise, d'une part, à connaître et atténuer les risques de sécurité cryptographique résultant des algorithmes quantiques et, d'autre part, à identifier de nouveaux avantages client au moyen de l'informatique quantique.

Open Quantum Institute
L'Open Quantum Institute (OQI) est une initiative de gouvernance multilatérale qui promeut l'accès mondial et inclusif à l'informatique quantique ainsi que le développement d'applications pour le bien de l'humanité. Dans le cadre de la diplomatie scientifique, l'OQI noue des partenariats avec des prestataires du marché qui acceptent que les capacités disponibles sur leurs ordinateurs quantiques soient utilisées pour développer des applications en vue d'atteindre les objectifs de développement durable (ODD). L'OQI est le fruit d'une coopération entre le CERN et la Geneva Science and Diplomacy Anticipator Foundation (GESDA). Il bénéficie du soutien d'UBS ainsi que de l'accompagnement du Département fédéral des affaires étrangères (DFAE), de l'EPFZ et de l'EPFL.

Swiss Quantum Initiative
Lancée en 2022 par le Conseil fédéral, la Swiss Quantum Initiative (SQI) est l'initiative nationale de promotion de la recherche et de l'innovation suisse dans le domaine des sciences quantiques. Pour la période 2025–2028, CHF 82,1 millions lui ont été alloués. Elle a pour but de renforcer la compétitivité internationale de la Suisse au moyen d'appels à projets compétitifs ainsi que de transferts de savoir et de technologie.

Quelques exemples internationaux

J.P. Morgan

La grande banque américaine J.P. Morgan développe depuis quelques années ses propres projets de recherche dans le domaine de l'informatique quantique.[18] Ces projets concernent notamment la sécurité informatique, l'amélioration du cryptage des données et l'optimisation des opérations de couverture *(hedging)* sur les marchés financiers. Selon ses dires, la banque entend établir des solutions d'informatique quantique dans les domaines importants pour elle, afin de bénéficier des avantages de ces technologies avant la concurrence.[19] Elle explore également les connexions avec la technologie de la blockchain, qui repose sur le cryptage et revêt une importance croissante dans le domaine interbancaire.

HSBC

Dans le domaine de la technologie quantique, cette grande banque britannique d'envergure mondiale s'est fixé trois objectifs.[20] Elle collabore avec des partenaires comme IBM, Fujitsu et Quantinuum pour jouer un rôle de leader dans le secteur financier et apprendre comment intégrer l'informatique quantique dans les produits et services bancaires. Elle a également créé en interne une équipe de spécialistes chargée de mener des travaux de recherche, de développer des produits et de breveter ses propres innovations. Enfin, elle s'efforce de développer des applications pratiques dans tous ses domaines d'activité, afin de se préparer à l'économie numérique post-quantique. Parmi les exemples concrets cités par HSBC figurent l'optimisation de la fixation des prix (notamment ceux des dérivés financiers), l'optimisation des sûretés (car les sûretés inutiles coûtent cher), ainsi que des améliorations dans les simulations prédictives de Monte-Carlo et les modélisations stochastiques.

Banque des règlements internationaux (BRI)

Dans le cadre du projet Leap, la BRI travaille sur des sujets comme les systèmes financiers et la stabilité des marchés financiers dans le contexte post-quantique. Son objectif est que les banques centrales membres soient prêtes à réagir en temps utile aux évolutions à venir.[21] La Banque de France et la Deutsche Bundesbank, notamment, comptent parmi les institutions membres.

---

18 J.P. Morgan, Global Technology Applied Research (2024)

19 J.P. Morgan, JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application (2024)

20 HSBC, HSBC and Quantum (2024)

21 BRI, Project Leap: quantum-proofing the financial system (2024)

3 Conclusions et recommandations opérationnelles

3.1 Pour les banques suisses

Même si l'informatique quantique n'en est qu'à ses débuts, elle rend d'ores et déjà nécessaires des initiatives concrètes de la part des banques et d'autres prestataires de services financiers. Ignorer cette technologie aujourd'hui, ou se contenter de l'observer passivement, n'est pas dénué de risques. Parmi ces risques figurent les vols de données dans le cadre d'attaques «harvest now, decrypt later», la course aux talents dans un contexte de pénurie de main d'œuvre spécialisée (comme dans le domaine de l'IA) et la menace d'être supplanté à terme par des concurrents qui améliorent leurs modèles d'affaires ou en développent de nouveaux sur la base d'algorithmes quantiques. Le nombre des brevets est en augmentation constante dans le domaine de l'informatique quantique, ce qui accroît la pression à l'innovation.[22, 23, 24]

En matière d'informatique quantique, quelles que soient les mesures de sécurité nécessaires, offensives et défensives, le facteur temps est primordial. Même si l'on ignore encore à partir de quand beaucoup des systèmes de cryptage actuels pourraient être menacés, rien ne sert d'attendre pour agir. Il faudra des années aux banques pour adapter leurs architectures informatiques en place, introduire une cryptographie post-quantique et mettre à jour leurs protocoles de sécurité. Combinée à d'autres technologies comme l'IA et la TRD, l'informatique quantique aura potentiellement un impact considérable sur la structure des coûts et des risques ainsi que sur l'offre de produits et services des banques à moyen et long terme.

Afin d'aider les banques à saisir ces opportunités tout en identifiant, en atténuant voire en éliminant les risques en temps utile, les auteurs du présent rapport, membres du groupe d'experts conjoint de l'ASB et de QuantumBasel, ont élaboré les recommandations opérationnelles suivantes:

- **Analyser l'environnement informatique existant et le surveiller:** l'informatique quantique et la cryptographie post-quantique évoluent vite. Les banques devraient effectuer un suivi régulier de ces technologies et analyser leur environnement informatique existant – y compris les applications, les réseaux, la communication avec les partenaires et les composants de sécurité – en vue de détecter ses failles potentielles.
- **Inventorier les données et évaluer les risques:** toutes les données ne nécessitent pas d'être protégées au-delà de cinq ou dix ans, toutes les données et tous les protocoles ne sont pas menacés par les algorithmes quantiques. Il faut donc inventorier les informations disponibles pour déterminer quels sont les données et les processus menacés, dans quelle mesure, et quelle est leur valeur à long terme. Les informations les plus critiques seraient à traiter en priorité, en évaluant les risques auxquels elles sont exposées. Les résultats pourraient faire l'objet d'une carte de chaleur *(heatmap)*, qui permettrait de visualiser clairement les risques majeurs.
- **Elaborer une feuille de route et prévoir des migrations:** sur la base de l'inventaire, il y aurait lieu d'adapter les plans d'architecture et de prévoir des migrations vers une cryptographie post-quantique. La crypto-agilité est essentielle à cet égard, dans la mesure où d'autres migrations pourraient s'avérer

22 The Quantum Insider, EPO: Quantum Computing's Patent Growth is Multiplying, Leads Tech Industry (2023)

23 QED-C, Quantum patent trends update 2022 (2023)

24 Deloitte, Industry spending on quantum computing will rise dramatically. Will it pay off? (2023)

nécessaires ultérieurement, par exemple si des solutions de mécanique quantique sont mises en place comme l'échange quantique de clé. Une feuille de route récapitulant les domaines d'action concernés et les mesures à prendre pourrait servir de guide opérationnel.

Pour amorcer le voyage vers l'ère quantique, les mesures ci-après peuvent être utiles:[25]

- **Commencer à sensibiliser et à former en interne:** les banques devraient informer leur personnel, y compris les cadres, sur les opportunités et les risques inhérents à la technologie quantique. A cet effet, il est possible de mettre en place une communication ciblée, mais aussi des formations – notamment sur les algorithmes et les méthodes de dernière génération – à destination des équipes chargées de la sécurité informatique et de la cryptographie.
- **Mettre à jour les règles de sécurité:** intégrer de nouveaux algorithmes post-quantiques suppose d'adapter en permanence les directives et les processus existants en matière de sécurité. Il s'agit notamment de définir un objectif et de développer une stratégie à long terme, qui fixe les capacités et les technologies requises en matière de sécurité quantique.
- **Contrôler les mesures prises par les fournisseurs et les partenaires:** les banques devraient évaluer les mesures post-quantiques prises par leurs fournisseurs et leurs partenaires, afin de s'assurer qu'elles soient adéquates.

Les banques devraient en outre identifier les opportunités en prenant les mesures suivantes:

- **Chercher à collaborer avec des organisations spécialisées:** pendant la phase expérimentale, cela permettrait aux banques de partager des expériences ainsi que de développer des approches et des cadres de travail communs.
- **Se préparer à l'informatique quantique sur le cloud:** à moyen terme, comme les grandes applications d'IA, l'informatique quantique sera accessible principalement via une infrastructure cloud. Les banques devraient donc se préoccuper activement de leur préparation au cloud *(cloud readiness)*.[26]

3.2 Pour les autorités

La réglementation suisse étant neutre sur le plan de la technologie et fondée sur des principes, les adaptations juridiques et réglementaires à effectuer en vue du déploiement de l'informatique quantique devraient être limitées dans un premier temps. Les principes applicables en Suisse en matière de surveillance et de réglementation sont les mêmes pour l'informatique quantique que pour d'autres nouvelles technologies: neutralité technologique, proportionnalité, protection de la réputation de la place financière et sécurité juridique.

Afin d'identifier les modifications requises, y compris ponctuelles, il faudrait commencer par analyser les conditions-cadres existantes au regard des usages prévus de l'informatique quantique. Avec l'expérience, d'autres failles apparaîtront, que l'on pourra alors traiter en temps opportun. Du point de vue réglementaire, l'informatique quantique se subdivise selon nous en deux domaines principaux: d'une part, les aspects

25 L'office fédéral allemand de la sécurité informatique (Bundesamt für Sicherheit in der Informationstechnik, BSI) propose un guide détaillé sur la migration vers une cryptographie post-quantique: Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen.

26 Nous les invitons à consulter à cet effet le Guide «Cloud» – Recommandations pour sécuriser le cloud banking» publié par l'ASB.

concernant la sécurité, en particulier la cryptographie post-quantique (CPQ), et d'autre part, ceux concernant les nouveaux produits et services issus de cette technologie.[27]

Le passage à la CPQ concernera tous les secteurs, pas seulement le secteur financier. Les banques sont déjà soumises à des prescriptions contraignantes en matière de diligence, de protection des données et de confidentialité. On attend d'elles qu'elles prennent des mesures techniques et organisationnelles pour assurer la sécurité des données et des informations. Mais, au vu de l'évolution constante des exigences de sécurité, on attend d'elles également qu'elles adaptent leurs concepts de sécurité en permanence. Des autorités réglementaires comme l'Autorité fédérale de surveillance des marchés financiers (FINMA) surveillent la mise en œuvre de ces mesures dans le cadre de leurs activités prudentielles.[28]

Si les impacts potentiels de l'informatique quantique sur la cybersécurité sont déjà passablement concrets, les implications liées à l'utilisation quotidienne d'ordinateurs quantiques par les établissements financiers (p. ex. en termes de protection des données) restent floues. Un dialogue régulier entre le secteur financier et les régulateurs demeure donc essentiel pour partager des expériences et identifier en temps utiles les éventuelles mesures à prendre.

Des initiatives nationales et géopolitiques témoignent par ailleurs de l'importance croissante de l'informatique quantique. En septembre 2024, le G7 a organisé un atelier à Rome pour discuter de la mise en place d'un système financier post-quantique et évaluer les rôles respectifs des autorités réglementaires et des acteurs privés. Dans son communiqué final, le G7 encourage les autorités de surveillance financière à collaborer étroitement avec les entreprises et les autres parties intéressées, afin de les sensibiliser à la nécessaire transition vers des technologies post-quantiques.[29] En Suisse, ces échanges transversaux existent déjà via l'Open Quantum Institute, le Quantum Economy Network du Forum économique mondial et la Swiss Quantum Initiative.[30, 31, 32] Ces exemples montrent l'intérêt des milieux politiques pour l'informatique quantique ainsi que l'importance des partenariats dans ce contexte.

3.3 Pour la place financière suisse

Afin d'assurer la compétitivité de la place financière suisse à moyen et long terme et dans un contexte de concurrence mondiale, il est indispensable de s'appuyer sur les nouvelles technologies pour améliorer les produits et les services. L'informatique quantique joue à cet égard un rôle décisif, de même que d'autres technologies comme l'IA et la TRD. En toute logique, les facteurs qui assurent la compétitivité de certaines banques contribuent aussi à renforcer la place financière dans son ensemble. On ne peut donc que se réjouir que des universités et des organismes de recherche suisses se dédient à la fois à la recherche fondamentale

27 L'association sectorielle des opérateurs de téléphonie mobile GSM, la GSMA, tient une liste des initiatives prises par différents pays dans le domaine de la CPQ.

28 La Commission européenne a recommandé en avril 2024 à tous les Etats membres de l'UE d'élaborer une feuille de route commune pour la transition vers la cryptographie post-quantique. L'objectif est de coordonner cette transition en ce qui concerne le secteur public et les infrastructures critiques sur le territoire de l'UE.

29 G7 Cyber Expert Group, Statement on Planning for the Opportunities and Risks of Quantum Computing (2024)

30 Open Quantum Institute (OQI) (2024)

31 WEF Quantum Economy Network (2024)

32 Swiss Quantum Initiative (SQI) (2024)

et à la recherche appliquée. La simplification des processus ainsi obtenue, la rapidité des canaux de communication tant formels qu'informels, le haut niveau de spécialisation des parties prenantes ainsi que leur propension à l'adaptation et au changement, tout cela crée une base solide pour une utilisation fructueuse de l'informatique quantique.

4 Conclusion générale

Le développement de l'informatique quantique constitue à la fois une opportunité et un défi pour le secteur financier suisse. Capables d'effectuer des calculs et des simulations complexes avec à la fois davantage d'efficacité et davantage de précision, les ordinateurs quantiques ouvrent de nouvelles perspectives d'utilisation, par exemple en matière de gestion des risques et d'optimisation des portefeuilles. Mais, en parallèle, il faut améliorer les protocoles de sécurité actuels en y intégrant une cryptographie post-quantique. Les contraintes technologiques en résultant ne doivent pas être sous-estimées, de sorte que les établissements financiers devraient se préparer à ces changements en posant dès aujourd'hui les jalons pertinents pour leur transition quantique.

Afin de tracer la voie vers un avenir post-quantique, il est indispensable que les banques investissent dans leur préparation quantique *(quantum readiness)*. En développant leurs propres compétences de manière ciblée et en collaborant avec des organisations spécialisées, elles s'assureront durablement des avantages compétitifs tout en minimisant les risques liés à l'informatique quantique. Ces investissements ne sont pas seulement la marque d'un état d'esprit innovant, ils sont aussi une étape importante vers une place financière suisse durablement plus résiliente.

«La quantum readiness n'est pas seulement la marque d'un état d'esprit innovant, elle est aussi une étape importante vers une place financière suisse durablement plus résiliente.»

Les recommandations formulées dans le présent rapport proposent une première approche pour se familiariser avec le sujet et organiser une transition quantique réussie. Les opportunités, mais aussi les risques inhérents à l'informatique quantique devront être analysés plus en détail dès que cette technologie se sera davantage diffusée dans le secteur financier et dans d'autres secteurs. Pour l'heure, il faut nourrir et cultiver le dialogue entre le secteur financier et les autorités, afin de suivre en permanence les évolutions dans ce domaine et d'identifier en amont les éventuelles mesures à prendre. Quoi qu'il en soit, la collaboration de la branche avec des organismes de recherche et des entreprises de premier plan incite à l'optimisme et laisse à penser que la Suisse est en bonne voie pour jouer un rôle de leader en matière de technologie quantique.

Glossaire

Algorithme: Suite finie d'instructions permettant de résoudre un problème spécifique ou d'accomplir une tâche. En informatique quantique, il existe des algorithmes particuliers, comme l'algorithme de Shor ou l'algorithme de Grover, qui utilisent la mécanique quantique pour effectuer certains calculs plus rapidement que des algorithmes classiques.

Algorithme de Grover: Algorithme quantique qui, par rapport à des algorithmes classiques, permet une accélération quadratique de la vitesse de recherche dans une banque de données non classée. Il est susceptible d'affecter la sécurité des procédés de cryptographie symétrique.

Algorithme de Shor: Algorithme quantique capable de factoriser des grands nombres en nombres premiers à une vitesse exponentiellement accélérée par rapport à des algorithmes classiques. Il est susceptible d'affecter la sécurité des procédés de cryptographie asymétrique comme le RSA.

Correction d'erreurs: Méthodes complexes permettant des calculs stables, dans la mesure où les ordinateurs quantiques sont sujets aux erreurs.

Crypto-agilité: Capacité de réagir rapidement à de nouvelles menaces cryptographiques en basculant les systèmes vers de nouvelles normes et de nouveaux algorithmes.

Cryptographie post-quantique: Nouvelle génération d'algorithmes cryptographiques capables de résister aux attaques d'ordinateurs quantiques. Le NIST a déjà standardisé trois de ces algorithmes.

Décohérence: Dégradation progressive du comportement quantique d'un qubit sous l'effet des interactions avec son environnement, ce qui conduit à des pertes d'informations. La décohérence est un des plus grands défis des systèmes quantiques.

Intrication: Fait, pour deux qubits, d'être liés entre eux de telle sorte que tout changement d'état de l'un influe aussitôt sur l'état de l'autre, indépendamment de la distance qui les sépare.

Noisy intermediate-scale quantum (NISQ): Type d'ordinateur quantique actuellement disponible, mais d'une puissance limitée. Ces systèmes restent sujets aux erreurs et ont un faible nombre de qubits, mais ils sont déjà capables de résoudre des problèmes spécifiques plus rapidement que des ordinateurs conventionnels.

One-time pad (OTP) ou masque jetable: Procédé cryptographique qui, s'il est correctement mis en œuvre, est théoriquement impossible à casser. Il utilise une clé aléatoire de la même longueur que le message à transmettre. Cette clé est utilisée une fois seulement, puis jetée, ce qui protège le procédé contre toutes les attaques cryptographiques – à condition que la clé soit secrète et complètement aléatoire. Sa transmission de l'émetteur au destinataire du message par un moyen sûr constitue une difficulté pratique.

Portes quantiques: Eléments de base d'un ordinateur quantique. Les portes quantiques manipulent des qubits pour effectuer des calculs et rendent possibles des états parallèles grâce à des phénomènes quantiques comme la superposition et l'intrication. Alors que les portes logiques classiques ne travaillent qu'avec les valeurs 0 et 1, les portes quantiques peuvent réaliser plus efficacement des opérations plus complexes.

Quantum key distribution (QKD) ou échange quantique de clé: Procédé qui utilise les lois de la mécanique quantique pour partager une clé de communication sûre entre deux parties. Il est à l'épreuve des attaques classiques et quantiques.

Quantum random access memory (qRAM) ou mémoire vive quantique: Elément de mémoire qui permet de traiter en parallèle de grandes quantités de données dans un ordinateur quantique. C'est une solution potentielle à la limitation actuelle des flux de données (classiques) dans les ordinateurs quantiques.

Qubit: Plus petite unité d'information quantique. Alors que les bits classiques ont toujours pour valeur soit 0, soit 1, les qubits, par superposition, peuvent exister simultanément dans les deux états.

Superposition: Phénomène de mécanique quantique par lequel un qubit peut exister simultanément dans plusieurs états classiques (0 et 1). La superposition permet aux ordinateurs quantiques de traiter en parallèle d'énormes quantités de données.

Rédaction

Andrea Luca Aerni, Policy Advisor Digital Finance, ASB
Richard Hess, Head of Digital Finance, ASB
Panagiotis Psomas, Intern Digital Finance, ASB

Experts

QuantumBasel

Damir Bogdan, CEO, QuantumBasel
Frederik F. Flöther, Chief Quantum Officer, QuantumBasel

Etablissements membres de l'ASB

Marco Foglia, Information Security Officer, Raiffeisen Suisse
Christian Hostettler, Lead Technology Architect, PostFinance
Cedric Membrez, Head Applied Research, Group Emerging Technology, UBS

A propos de l'Association suisse des banquiers (ASB)

L'Association suisse des banquiers (ASB) est l'association faîtière de la place financière suisse et défend les intérêts de quelque 270 établissements membres. Depuis 1912, elle prône des conditions-cadres optimales, propices à une place bancaire compétitive et innovante. Elle encourage le dialogue avec les milieux politiques et les autorités, contribue à la réflexion sur des sujets majeurs comme la finance durable et les monnaies numériques, soutient la formation initiale et continue au sein de la branche. En tant que centre de compétences, elle s'engage en faveur d'un développement durable du secteur bancaire.

swissbanking.ch

A propos de QuantumBasel

QuantumBasel est une entreprise privée qui, sur le campus d'innovation uptownBasel et en partenariat avec des start-up, des groupes et des universités, s'appuie sur la technologie quantique et l'IA pour promouvoir des innovations durables. Grâce à un écosystème technologique mondial alliant recherche et expertise, QuantumBasel accélère le passage de l'informatique quantique du laboratoire aux applications industrielles. Fin 2024, le premier ordinateur quantique commercial de Suisse entrera en service sur le campus.

quantumbasel.com

Association suisse des banquiers
Aeschenplatz 7
Case postale 4182
CH-4002 Bâle
office@sba.ch
www.swissbanking.ch