Bulletin d'information ECA-N avril 2025

Ordinateur quantique et Bitcoin : menace ou opportunité ?

L'ONU a déclaré 2025 Année internationale de la science et des technologies quantiques, reflétant les efforts mondiaux déployés par les gouvernements et l'industrie pour développer des processeurs quantiques évolutifs et réaliser des avancées révolutionnaires en médecine, en chimie, IA et au-delà.
Cette newsletter d'avril vise à faire un tour d'horizon de ce domaine fascinant, et à mettre en avant le lien entre l'informatique quantique et le bitcoin.

***"Dans l'univers, tout est énergie, tout est vibration, de l'infiniment petit à l'infiniment grand."* - Albert Einstein**

Auteur : Olivier Rousselle

Table des matières

Physique quantique et ordinateur quantique

Histoire de la physique quantique

La physique quantique est la branche de la science qui étudie le comportement de la matière à très petite échelle (atomes, particules subatomiques,...). Un tournant majeur en physique a été pris au début du XXe siècle lorsque le physicien français Louis de Broglie a proposé que toute particule de matière est aussi une onde, caractérisée par une énergie E , masse m et fréquence ν :

$$E = mc^2 = h\nu$$

Cette idée révolutionnaire a jeté les bases de la mécanique quantique. Tout notre monde physique - lumière, matière - ne serait donc fondamentalement qu'énergie et vibration, comme l'a indiqué Einstein.

En 1926, Erwin Schrödinger a formulé une équation fondamentale de la physique quantique:

$$i\hbar \frac{\partial}{\partial t} |\psi\rangle = \hat{H} |\psi\rangle$$

avec $\hbar$ constante de Planck, $\frac{\partial}{\partial t}$ dérivée temporelle, $\hat{H}$ opérateur hamiltonien (énergie). Cette équation décrit l'évolution dans le temps de la fonction d'onde ψ associée à une particule.

Parmi les phénomènes clés de la physique quantique, on trouve :

- Superposition : une particule peut exister dans plusieurs états quantiques à la fois.
- Effet de l'observateur : en physique quantique, le simple fait d'observer un système peut en changer le comportement.
- Intrication quantique : deux particules peuvent devenir liées de telle sorte que l'état de l'une affecte instantanément l'état de l'autre, même à des kilomètres de distance. Einstein appelait cela un "effet fantomatique à distance". Voir illustration ci-dessous.

Illustration de l'intrication entre deux particules quantiques

Technologies et ordinateurs quantiques

Les propriétés quantiques de la matière ont profondément transformé notre monde, elles sont à l'origine de nombreuses technologies modernes :

- Les lasers, utilisés pour les lecteurs de CD/DVD, imprimantes, chirurgie de précision, télécommunications par fibre optique ;
- Les transistors, fondés sur les propriétés quantiques des semi-conducteurs, sont essentiels pour les ordinateurs, satellites et véhicules ;
- L'IRM (Imagerie par Résonance Magnétique), pour l'imagerie médicale ;
- L'horloge atomique, qui permet de mesurer le temps avec une précision extrême, ce qui est cruciale pour le GPS et la synchronisation des réseaux de communication.

Aujourd'hui, nous vivons une seconde révolution quantique avec l'émergence des ordinateurs quantiques. Contrairement aux ordinateurs classiques, qui traitent des bits valant 0 ou 1, les ordinateurs quantiques utilisent des qubits qui peuvent être dans une superposition de 0 et 1.
Les processus sont effectués en parallèle grâce à la superposition des états quantiques.

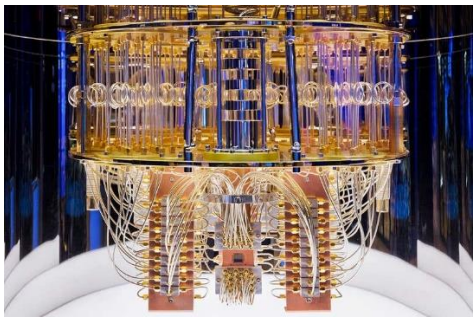


Photo du cœur d'un ordinateur quantique

Tableau de comparaison entre un ordinateur classique et un ordinateur quantique :

	Ordinateur classique	Ordinateur quantique
Unité d'information	Bit (0 ou 1)	Qubit (superposition de 0 et de 1)
Température	Température ambiante	Proche du zéro absolu (-272°C)
Matériel / hardware	Processeur CMOS Intel, AMD,...	Supraconducteurs, ions piégés, photons ou spins atomiques
Vitesse de calcul	Rapide pour tâches classiques, inefficace pour certains problèmes complexes	Potentiellement exponentielle pour certains problèmes spécifiques (ex. factorisation)
Taux d'erreur	Quasi nul	0.1% (nécessite des algos de correction d'erreur)
Prix actuel (milieu de gamme)	~ 1000 €	> 1 million €

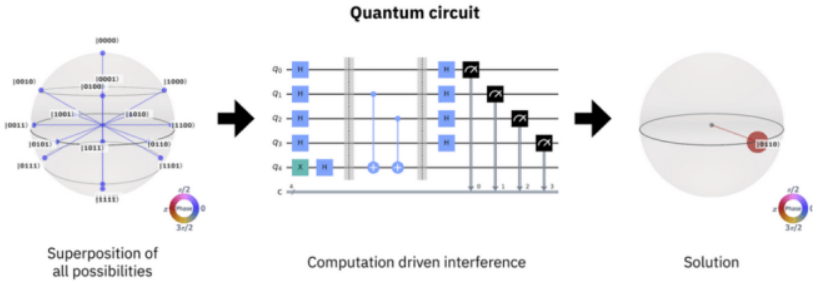
Comme indiqué précédemment, l'état d'un bit quantique ψ ne se limite pas à 0 ou 1. Il est dans un état de superposition :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

avec (α, β) les amplitudes de probabilité associées aux états 0 et 1.

Quand deux qubits sont intriqués, leur état global ne peut pas être décrit comme la simple somme de leurs états individuels. Cela permet aux ordinateurs quantiques de représenter et manipuler simultanément un nombre exponentiel d'états.

Les tâches réalisées par un ordinateur quantique sont codées dans un algorithme quantique et circuits quantiques. Les circuits quantiques sont des routines de calcul consistant en des opérations quantiques cohérentes sur des données quantiques. Ils permettent à un ordinateur quantique d'utiliser des informations classiques et de produire une solution classique, en utilisant des principes quantiques tels que les interférences quantiques, la superposition ou l'intrication pour effectuer le calcul.



Source : qiskit

Cela leur permet de résoudre certains problèmes complexes bien plus rapidement, comme le décryptage de données chiffrées… ce qui amène des enjeux cruciaux en matière de sécurité numérique.

Qu'est-ce que la cryptographie et quel est son lien avec le bitcoin ?

La cryptographie est l'art de protéger l'information en la rendant illisible pour ceux qui ne sont pas autorisés à y accéder. Chaque fois que vous envoyez un message sécurisé ou effectuez un achat en ligne, vous utilisez de la cryptographie.

Son but principal est de garantir trois choses :

- La confidentialité : seules les bonnes personnes peuvent lire le message.
- L'intégrité : le message n'a pas été modifié.
- L'authenticité : l'expéditeur est bien celui qu'il prétend être.

Il existe deux grands types de cryptographie :

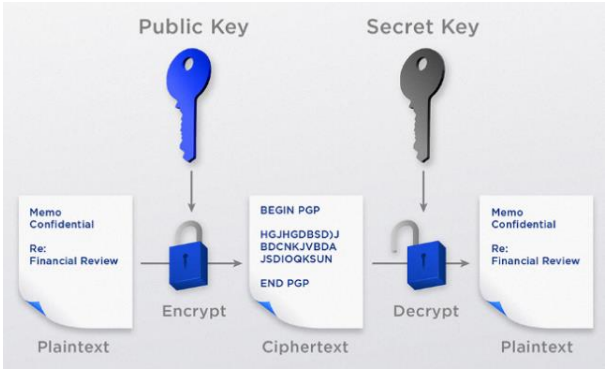
- Symétrique : un même mot de passe ou "clé" est utilisé pour chiffrer et déchiffrer les messages. Cela fonctionne bien pour les communications entre deux parties qui se font confiance.
- Asymétrique : chaque personne possède une paire de clés : une clé publique (qu'on peut partager) et une clé privée (qui reste secrète). On chiffre un message avec la clé

publique, mais seul le détenteur de la clé privée peut le lire. Cette méthode est largement utilisée dans le monde numérique moderne, y compris dans les cryptomonnaies.

Bitcoin repose sur deux usages clés de la cryptographie : cryptographie asymétrique (avec clés privée/publique) et le hachage cryptographique.
En effet, chaque utilisateur de Bitcoin possède :

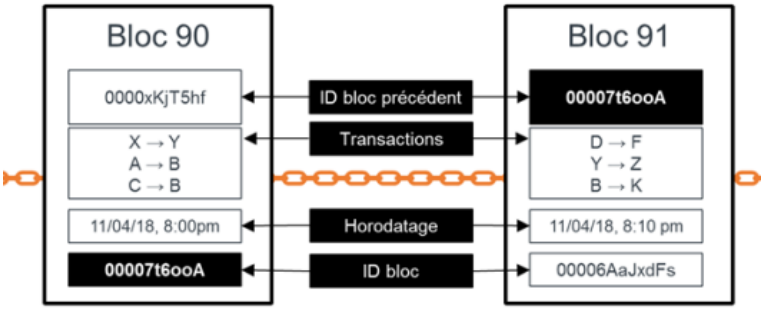
- Une clé privée : c'est comme la signature secrète. Elle permet de prouver qu'on est bien le propriétaire des bitcoins.
- Une clé publique : elle est visible par tous. C'est elle qui sert d'adresse Bitcoin, un peu comme un RIB.

Quand vous envoyez des bitcoins, vous signez la transaction avec votre clé privée. Le réseau peut ensuite vérifier cette signature grâce à votre clé publique. La sécurité du système dépend du fait qu'il est aujourd'hui pratiquement impossible, avec les ordinateurs classiques, de retrouver une clé privée à partir de sa clé publique.



Chiffrement asymétrique. Source : crypto.com

Bitcoin utilise aussi une fonction mathématique appelée fonction de hachage (SHA-256). Elle prend un message et le transforme en une suite de chiffres, appelée "empreinte". Une petite modification dans le message donne une empreinte totalement différente. Le hachage est utilisé dans l'intégrité des blocs (chaque bloc contient le hachage du précédent), la preuve de travail (les mineurs cherchent un hachage avec certaines caractéristiques), et la création des adresses Bitcoin. C'est grâce au hachage qu'on parle de "chaîne de blocs" ou blockchain : chaque bloc est lié au précédent de manière infalsifiable.

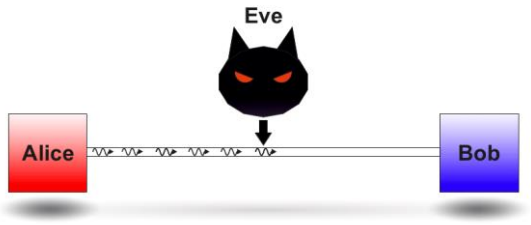


Chaine de blocs – bitcoin. Source : Blockchain France

La cryptographie quantique

La cryptographie quantique est une nouvelle branche de la cryptographie qui utilise les lois de la physique quantique pour sécuriser l'information. Plutôt que de s'appuyer sur des calculs mathématiques complexes et des clés longues, elle exploite des propriétés quantiques comme la superposition ou l'intrication pour garantir une sécurité inviolable par principe physique.

L'exemple le plus célèbre est la distribution quantique de clés (QKD - Quantum Key Distribution). Elle permet à deux personnes d'échanger une clé secrète en s'assurant qu'aucun espion ne l'a interceptée, car toute tentative d'écoute perturberait le système et serait immédiatement détectée.
On utilise des photons (des particules de lumière) pour envoyer les bits (0 ou 1). En physique quantique, le fait d'observer les photons modifie leur état. Si Alice envoie des photons à Bob pour créer une clé secrète, et qu'un espion (nommé Eve) essaie de les intercepter, alors Eve perturbera les photons et Alice & Bob le détecteront immédiatement. C'est ce qu'on appelle le principe d'intrusion détectable. Il garantit que personne ne peut intercepter la clé sans se faire remarquer.



Distribution quantique de clés entre Alice et Bob via l'envoi de photons

Même si la cryptographie quantique est prometteuse, elle est loin d'être parfaite :

- Coût élevé : les équipements optiques sont encore chers.
- Distance limitée : les photons se perdent sur de longues distances.
- Pas une solution magique : elle protège la clé, pas tout le système. Les attaques peuvent venir d'ailleurs (bugs, humains…).

La cryptographie quantique est-elle une menace pour Bitcoin ?

La sécurité du système Bitcoin dépend du fait qu'il est aujourd'hui pratiquement impossible, avec les ordinateurs classiques, de retrouver une clé privée à partir de sa clé publique.
Mais avec l'ordinateur quantique, tout change. Les algorithmes quantiques tirent leur puissance de la superposition et de l'intrication pour explorer plusieurs états en parallèle et les manipuler de manière coordonnée. Certains algorithmes quantiques peuvent casser des protections cryptographiques que nos ordinateurs classiques mettent des milliards d'années à casser.

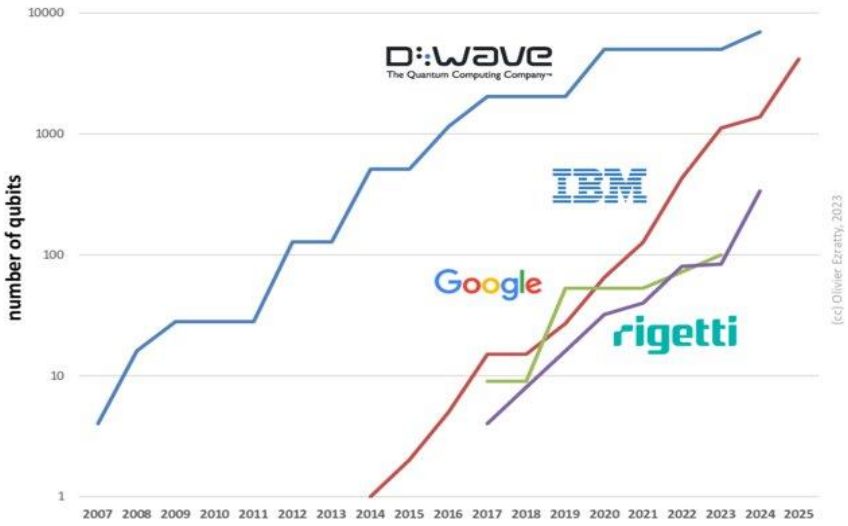
L'algorithme le plus célèbre est l'algorithme de Shor, il permet de factoriser très rapidement de grands nombres premiers. Il permet de retrouver une clé privée à partir d'une clé publique. Si quelqu'un connaît votre clé publique, un ordinateur quantique suffisamment puissant pourrait retrouver votre clé privée… et voler vos bitcoins.
L'algorithme quantique de recherche de Grover, algorithme d'exploration des bases de données, pourrait également être utilisé pour retrouver des clés privées de portefeuilles Bitcoin.

Menace quantique	Impact potentiel	Niveau de risque estimé
Algorithme de Shor	Obtention de la clé privée à partir de la clé publique	Haut
Algorithme de Grover	Recherche de clé accélérée	Moyen

Source : cryptsy.com

Le risque lié à l'utilisation des ordinateurs quantiques dans le minage de Bitcoin surgirait si un seul acteur parvenait à contrôler cette technologie. Dans ce cas, il pourrait exploiter la rapidité du calcul quantique pour trouver les nonces des blocs plus rapidement que les autres mineurs, s'accaparant ainsi une part significative du hashrate. Tant que cette technologie reste entre les mains d'un seul acteur, un risque de centralisation persiste. Toutefois, dès qu'elle se démocratisera, le hashrate se redistribuera naturellement grâce aux lois du marché libre du minage.

Mais ne nous alarmons pas. Les ordinateurs quantiques actuels sont très loin d'avoir la puissance nécessaire pour casser les clés privées Bitcoin. Selon les estimations, compromettre le chiffrement du Bitcoin nécessiterait un ordinateur quantique doté d'environ 13 millions de qubits pour parvenir à un déchiffrement en 24 heures. Les meilleurs systèmes quantiques actuels comptent environ une centaine de qubits, et font en moyenne une erreur toutes les 1000 opérations.



Evolution du nombre de qubits depuis 2007, pour les ordinateurs quantiques de D-Wave, Google, IBM et Rigetti.

Algorithmes post-quantiques

L'informatique quantique représente une menace potentielle future pour Bitcoin car elle remet en cause certains fondements de sa sécurité. Cependant, cette menace est anticipée par la communauté scientifique et technique. Les développeurs de Bitcoin suivent de près les progrès en cryptographie post-quantique.
Plusieurs solutions sont à l'étude, notamment :

- Utiliser de nouveaux algorithmes de signature résistants aux ordinateurs quantiques.
- Mettre à jour le protocole Bitcoin par un "soft fork" pour introduire ces nouvelles méthodes sans changer radicalement le système.

L'intégration de l'informatique quantique peut aussi avoir un effet bénéfique dans le minage, en augmentant de façon significative le hashrate de Bitcoin. En effet, le traitement quantique en parallèle permettrait une validation des blocs plus rapide.
La distribution quantique de clés pourrait permettre aux portefeuilles Bitcoin de se synchroniser de façon ultra-sécurisée, sans risque d'interception. Les échanges entre utilisateurs pourraient devenir encore plus confidentiels. Plus généralement, l'arrivée des ordinateurs quantiques va pousser tous les systèmes numériques à renforcer leur sécurité. Cela pourrait inciter Bitcoin à évoluer plus rapidement vers une architecture plus résiliente, le rendant plus robuste à long terme.

Le Q-Day correspond au jour où l'informatique quantique deviendra suffisamment puissante pour briser la cryptographie moderne. Le CEO de Tether, Paolo Ardoino, a indiqué dans un post sur X qu'à partir de la date du Q-Day, toutes les personnes ayant accès à leur portefeuille bitcoin devront transférer leurs bitcoins vers de nouvelles adresses résistantes aux attaques quantiques. Tous les bitcoins présents dans les portefeuilles perdus, y compris ceux de Satoshi Nakamoto, seront piratés et remis en circulation.

Ainsi, la cryptographie quantique représente à la fois une menace et une opportunité : elle remet en cause nos systèmes actuels, mais propose aussi de nouvelles solutions de sécurité, parfois radicalement plus sûres.

Les experts offrent des points de vue divergents sur la manière dont l'informatique quantique pourrait transformer le paysage du Bitcoin. Leurs prédictions vont d'un optimisme prudent à des changements révolutionnaires. Les experts en informatique quantique suggèrent un calendrier pour une perturbation potentielle (source : cryptsy):

- À court terme (2 à 5 ans) : premières évaluations des menaces quantiques ;
- Moyen terme (5-10 ans) : émergence d'une vulnérabilité potentielle ;
- À long terme (10 à 15 ans) : transformation complète de la technologie blockchain.

Et les autres blockchains ?

Les autres blockchains (Ethereum, Solana, Avalanche,…) reposent également sur les algorithmes de cryptographie pour les signatures et le hachage (bien que les protocoles et détails des algorithmes soient différents). Ainsi, toutes les menaces/opportunités évoquées précédemment s'appliquent aux autres blockchains.
Comme nous l'avons vu, l'informatique quantique offre des opportunités uniques pour améliorer ces systèmes blockchains : accélérer les processus de vérification des transactions, améliorer les mécanismes de sécurité cryptographique, réduire la complexité des calculs,…
Actuellement, des outils de pointe aident les blockchains et plateformes de cryptomonnaies à évaluer leur résistance quantique. Ces outils analysent les points faibles des systèmes de chiffrement existants et permettent des améliorations proactives de la sécurité pour une meilleure protection.

Certains projets crypto commencent à explorer des alternatives post-quantiques. Par exemple, le projet Quantum Resistant Ledger est une blockchain conçue pour résister aux ordinateurs quantiques. Elle utilise des signatures XMSS (basées sur des arbres de hachage) pour résister aux attaques par l'algorithme de Shor. Plus d'informations ici : https://www.theqrl.org/.
Des cadres de blockchain hybrides peut également être développés, ils offriraient une transition intermédiaire entre les méthodes classiques et les méthodes résistantes aux technologies quantiques.
Les développeurs de la blockchain Ethereum sont actuellement en phase de recherche sur des mises à niveau visant une résistance quantique complète des protocoles de base ; leur mise en œuvre pourrait prendre plusieurs années.
Pour en savoir plus sur l'ensemble des techniques quantiques développées actuellement pour sécuriser davantage l'écosystème blockchain, voir cet article.

L'informatique quantique recèle également un potentiel d'innovation dans la DeFi (finance décentralisée). Par exemple, les capacités de calcul quantiques améliorées pourraient conduire à des protocoles de consensus innovants, plus efficaces et plus sécurisés dans les réseaux décentralisés.

La cryptographie quantique pourrait ainsi inspirer une nouvelle génération de blockchains, avec des transactions instantanément sécurisées sans risque de vol de clé, et une communication 100 % confidentielle entre nœuds (même face à des espions équipés d'ordinateurs quantiques).
Elle pourrait offrir un nouveau standard de sécurité pour les cryptos du futur.

« L'informatique quantique représente la prochaine frontière de l'innovation en matière de cryptomonnaies » – Rapport sur l'innovation technologique 2023

Pour aller plus loin

Dans cette newsletter, nous ne sommes pas rentrés dans les détails techniques de l'informatique quantique. Si vous souhaitez aller plus loin, nous vous invitons à consulter les liens suivants.

--> Si vous souhaitez suivre des cours poussés en informatique quantique, réalisés par le CERN (module de 7 cours):
https://home.cern/news/announcement/computing/online-introductory-lectures-quantum-computing-6-november

--> Si vous souhaitez faire votre premier programme quantique, codé en Q# (langage quantique de Microsoft) et exécutable sur votre ordinateur classique :
https://learn.microsoft.com/fr-fr/training/modules/qsharp-create-first-quantum-development-kit/

--> Si vous souhaitez en savoir plus sur les fondements de la physique quantique :
https://fondationlouisdebroglie.org/MEMOS/Olivier_Rousselle_ENS-AFLB.pdf