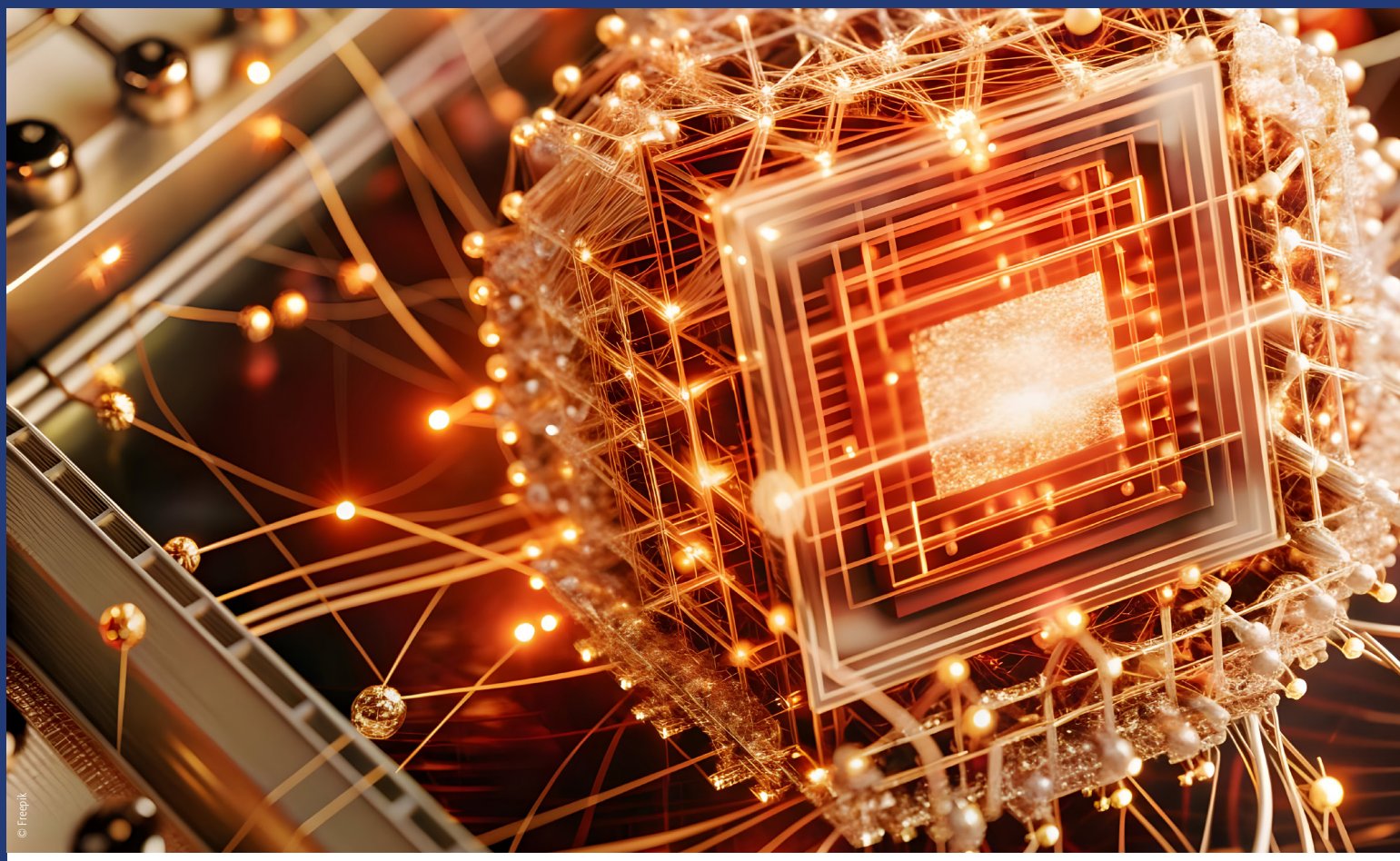

Introduction

Les bits classiques deviennent quantiques. Pourquoi faire ?

Oubliez les bits 0 et 1 : l'ère du bit quantique (le qubit) a sonné. 100 ans après la première révolution quantique, la seconde déverrouille des capacités de calcul inédites, pour certains problèmes complexes. Calculs super-polynomiaux, communications inviolables, détections de signaux plus précises : bienvenue dans le monde fascinant de l'Information quantique !

Fabrice Dupuy
Auteur de l'ouvrage 'Internet Quantique'

Introduction

Information quantique ? Quésaco, aurait-on envie de demander ? L'information quantique (parfois abrégée en QIS pour *Quantum Information Science*) est un domaine interdisciplinaire qui exploite les principes de la théorie quantique pour effectuer des tâches de traitement, de stockage et de transmission d'éléments quantiques d'information ou qubits.

Qubit ? KES ? Explication !

Au lieu d'utiliser des éléments d'information binaires, c'est-à-dire des bits classiques qui peuvent être soit des 0 soit des 1, l'information quantique utilise des éléments binaires quantiques ou qubits, qui seront eux dans l'un des états quantiques de base |0> ou |1>, ou dans une superposition des deux !

Avoir un bit classique d'information (noté c pour classique) sur un système ou un objet, c'est connaître l'état, soit 0, soit 1, dans lequel ce dernier se trouve. La pièce de monnaie est retombée sur *pile* (le bit c prend la valeur 1) ou sur *face* (c = 0); un chat normal est *vivant* (c = 1) ou *mort*

(c = 0). Tout Internet est basé sur ce principe d'encodage des mots, des chiffres, des échantillons de voix ou de vidéo en bits classiques pour leur transport entre expéditeurs et destinataires. Sur les réseaux, ne circulent que des 0 et des 1…

Dans le cadre de cette nouvelle science, avoir un bit quantique d'information (noté q comme quantum bit ou qubit) à propos du même objet, c'est modéliser le fait que l'objet puisse être dans une superposition d'états, jusqu'à ce que l'on effectue la mesure d'une propriété observable de cet objet. Avant la mesure (par exemple l'observation de la pièce retombée sur une surface plate), l'état quantique de la pièce est une superposition complexe des états |pile> = |1> et |face> = |0>. Avant l'ouverture de la boîte imaginée par Erwin Schrödinger, son chat est dans une superposition d'états |mort> = |0> et |vivant> = |1>. Toute l'information sur l'état du système quantique est contenue dans sa fonction d'onde : |Ψ>pièce ou |Ψ>chat.

A quoi ça sert, puisque de toute façon, à notre échelle, la pièce est retombée soit sur son côté pile, soit sur son côté face, et le chat de Schrödinger dans sa boîte est soit vivant, soit mort, mais pas dans une superposition de mort-vivant ?

La science de l'information quantique (QIS) devrait permettre de dépasser les limites des ordinateurs classiques dans la simulation des systèmes quantiques, par exemple. Dans une conférence marquante en 1981 intitulée «*Simulating Physics with Computers*», Richard Feynman soulignait ces limitations intrinsèques ; il fit valoir que la complexité du calcul nécessaire pour simuler un système quantique croît exponentiellement avec la taille du système, rendant la simulation classique impossible pour des systèmes même modestes. L'idée lui vint de la simulation quantique : construire un ordinateur qui fonctionne lui-même selon les principes de la physique quantique. Un tel simulateur quantique serait intrinsèquement capable de manipuler les états quantiques et d'imiter le comportement des systèmes quantiques avec une efficacité bien supérieure à celle des ordinateurs classiques.

Par exemple, l'ordinateur quantique pourra simuler le comportement des électrons dans les matériaux pour comprendre les mécanismes de la supraconductivité à haute température, ce qui pourrait révolutionner le transport d'énergie sans perte ; il pourra nous aider à comprendre les processus d'absorption de la lumière et de transport d'énergie dans les matériaux pour développer des cellules solaires plus performantes. La simulation quantique concernera aussi les interactions entre des molécules d'un médicament potentiel et des cibles biologiques (comme des protéines) afin de prédire leur efficacité et leurs effets secondaires, accélérant ainsi le processus de découverte de médicaments.

A l'échelle des atomes, des molécules, notre univers est probablement un gigantesque processeur d'informations quantiques. Dans ce cadre, l'information quantique peut être considérée comme le concept physique qui capture le mieux la nature de l'univers, à savoir ses changements, les traitements qui y ont lieu, les relations ou corrélations entre ses sous-systèmes. L'information quantique fournira une bien meilleure vision relationnelle des entités, des systèmes, des phénomènes et des événements (du moins à l'échelle de l'infiniment petit).

Un large éventail de domaines applicatifs

Ainsi la science de l'information quantique (QIS) englobe un large éventail de domaines de recherche et de développement, notamment :

• **le calcul quantique (Quantum Computing) ou l'informatique quantique** consistant à développer des ordinateurs quantiques capables de résoudre certains problèmes beaucoup plus rapidement que les ordinateurs classiques, en exploitant la superposition et l'intrication ; les applications potentielles incluent la découverte de médicaments, la science des matériaux, l'optimisation complexe et l'intelligence artificielle ;

• **les communications quantiques (Quantum Communications)** ou l'utilisation des propriétés quantiques pour transmettre des informations de manière sécurisée ; la **cryptographie quantique** promet des systèmes de communication théoriquement inviolables ; la **téléportation quantique** permet de transférer l'état quantique d'un qubit à un autre ;

• **la détection quantique (Quantum Sensing)** ou le développement de capteurs ultra-sensibles basés sur les principes quantiques pour des mesures de haute précision dans des domaines tels que la physique, la biologie et la médecine ;

• **la simulation quantique (Quantum Simulation)** utilisant des systèmes quantiques contrôlables pour simuler d'autres systèmes quantiques complexes, ce qui est bien plus difficile avec les ordinateurs classiques ; l'apport est crucial pour la recherche en chimie, en science des matériaux et en physique fondamentale.

> **" Les ordinateurs quantiques à petite échelle (de 50 à 1 000 qubits), déjà disponibles dans des 'clouds' permettent de réaliser des expériences et de tester des algorithmes, mais ils restent bruyants et ne surpassent pas encore les machines classiques dans les applications réelles."**

Au sein de cette science, le calcul quantique (ou l'informatique quantique) consistera donc à coder l'information quantique en qubits sur lesquels les ordinateurs quantiques pourront effectuer des opérations de calcul : par exemple l'algorithme quantique conçu par Peter Shor en 1994, qui factorise un entier naturel N (non premier) de façon polynomiale et non plus sub-exponentielle. Quant à la cryptographie quantique, elle consistera à encoder les n bits d'une clé secrète en qubits et à les distribuer de façon plus sécurisée. Enfin, les capteurs quantiques seront des appareils utilisant les principes de la physique quantique pour mesurer des grandeurs physiques (durée, valeur d'un champ magnétique, masse, etc.) avec une précision bien supérieure à celle des capteurs classiques ; ces capteurs exploiteront des phénomènes comme la superposition et l'intrication quantique pour améliorer la sensibilité et la précision des mesures. On les utilisera notamment en médecine, en navigation, en géophysique et en détection de matières.

Pour bien préciser les choses : si la physique quantique consistait à obtenir de l'information sur les états et le comportement de tel ou tel système physique, tel ou tel objet d'une expérimentation, la science de l'information quantique consiste à faire porter de l'information quantique et sa surprenante logique algorithmique sur de tels systèmes physiques (des capteurs, des ordinateurs quantiques). L'objectif étant de simuler l'infiniment petit (les électrons d'un matériau supraconducteur, les molécules d'un nouveau médicament, les liquides de spin quantique, les condensats de Bose-Einstein) ou de bénéficier d'une algorithmie non classique.

Dans ce dossier

Les technologies quantiques suscitent donc un intérêt considérable, mais parfois encore excessif. Entre promesses audacieuses et réel progrès technologique, il est important d'essayer d'y voir clair. Ce qui est réel aujourd'hui, en octobre 2025, ce sont les ordinateurs quantiques à petite échelle (de 50 à 1 000 qubits), déjà disponibles dans des 'clouds' ; ils permettent de réaliser des expériences et de tester des algorithmes, mais ils restent bruyants et ne surpassent pas encore les machines classiques dans les applications réelles. L'article suivant questionnera ce que pourrait être une suprématie quantique.

Ce qui est réel aussi est la distribution quantique de clés (QKD), avec des projets pilotes dans les réseaux de télécommunications et via les satellites, utilisant l'intrication de photons pour échanger des clés de chiffrement avec une sécurité basée sur la physique. **Yannick Gautier** et **Sylvain Chenard** aborderont la cybersécurité et l'apport du quantique dans l'article 'Du risque quantique à l'atout défensif : le réseau au cœur de la cybersécurité'.

Ce qui est réel concerne les capteurs quantiques déjà en laboratoire et en phase de tests industriels préliminaires. Ils permettront des imageries par résonance magnétique ultra-précises, détecteront les structures souterraines par gravimétrie et prendront en charge la navigation sans GPS, grâce à des interféromètres atomiques. Dans ce qui suit, **Myriam Nouvel** poursuit avec un point d'avancement sur le développement des capteurs quantiques, 'lorsque la technologie est au service de notre quotidien'.

Dans une synthèse du rapport de l'académie des technologies, **Olivier Ezratty** présente 'les défis de la création d'ordinateurs tolérants aux fautes', avec leurs millions de qubits et leurs codes de correction d'erreurs.

Enfin, vu l'hétérogénéité matérielle (hardware) des ordinateurs quantiques, **Frédéric Barbaresco**, **Félicien Schopfer** et **Emmanuelle Vergnaud** présentent l'objectif d'un projet visant l'obtention d'un classement mondial des performances des calculateurs quantiques agnostiques aux technologies matérielles : le projet BACQ (Benchmarks Applicatifs des Calculateurs Quantiques) du programme national du Laboratoire national d'essais (LNE).

Bonne lecture, bonne découverte ! ■

Les articles