CREOGN
CENTRE DE RECHERCHE

Note flash du CREOGN

Une question d'actualité : une référence synthétique

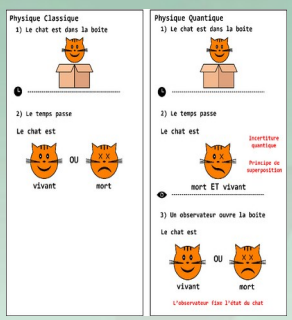
N° 4 - Décembre 2022

Alexandre GRASSET

L'informatique quantique

La physique quantique est la science de l'infiniment petit qui vise à expliquer les dynamiques régissant la matière au niveau atomique et subatomique. L'informatique quantique permet d'exploiter ces propriétés uniques afin de démultiplier les puissances de calcul et de stockage d'un appareil en conservant la logique binaire existante. La nature inhérente à ce nouveau paradigme le rend particulièrement adapté à la résolution de certains problèmes tels que la simulation de molécules complexes ou la factorisation de nombres importants.

Ce dernier point entraîne de profonds bouleversements pour la cryptographie, élément clé de la sécurité des systèmes d'information mais aussi de la viabilité des technologies blockchain (cryptomonnaies, NFT, etc.). L'informatique quantique a donc été logiquement identifiée comme un levier stratégique dans la compétition internationale et le développement de nouvelles technologies gourmandes en puissance de calcul telles que l'intelligence artificielle ou le big data.



En page 3
Schéma du chat de Schrödinger

Points clés/à retenir :

• Le qubit est l'unité élémentaire de stockage de l'information quantique ; similaire au bit classique, il peut avoir une valeur binaire de 0 ou 1. Néanmoins, le qubit applique deux principes quantiques particuliers, la superposition et l'intrication, pour aboutir à un gain remarquable en performances ;
• La superposition permet à un qubit d'être dans un état « incertain » de 0 ou 1 qui ne sera déterminé définitivement qu'une fois mesuré par le système (cf. exemple du chat de Schrödinger). Cela signifie que 4 qubits en superposition peuvent avoir 16 valeurs différentes contre seulement 1 avec 4 bits traditionnels. Plus on ajoute de qubits, plus le nombre de valeurs est exponentiel et donc plus la plage (capacité) de calcul disponible augmente par rapport aux processeurs classiques ;
• L'intrication est un phénomène de « jumelage » entre qubits permettant de déterminer l'état d'un qubit intriqué en mesurant simplement son « jumeau ». Ce phénomène ouvre la porte à des manipulations et à des prédictions déductives accélérant les vitesses de calcul ;
• Le nombre de qubits d'un processeur quantique permet de déterminer sa puissance. Le seuil minimum envisagé pour obtenir des applications concrètes est de 1 000 à 5 000 qubits. Actuellement le processeur le plus puissant est « l'Osprey » d'IBM avec 433 qubits ;
• La puissance d'un ordinateur quantique permettrait théoriquement de « briser » un chiffrement avancé (RSA avec une clé de 2 048 bits) en une centaine de secondes alors qu'il faudrait 1 milliard d'années à un supercalculateur. Des organismes technologiques (le *National Institute of Standards and Technology* – NIST – aux États-Unis) travaillent donc déjà à l'élaboration de standards de cybersécurité dits « post-quantiques » pour les systèmes classiques afin de les rendre capables de résister à de telles attaques ;

• La cryptographie quantique est un domaine annexe de l'informatique quantique qui vise à créer des paradigmes de chiffrement robustes en utilisant les propriétés quantiques de la lumière (polarisation de photons). Cette technique a été mise en œuvre avec succès pour la première fois par le satellite chinois « Micius » en 2016 afin d'établir une communication sécurisée théoriquement (presque) impossible à espionner avec sa base de contrôle terrestre.

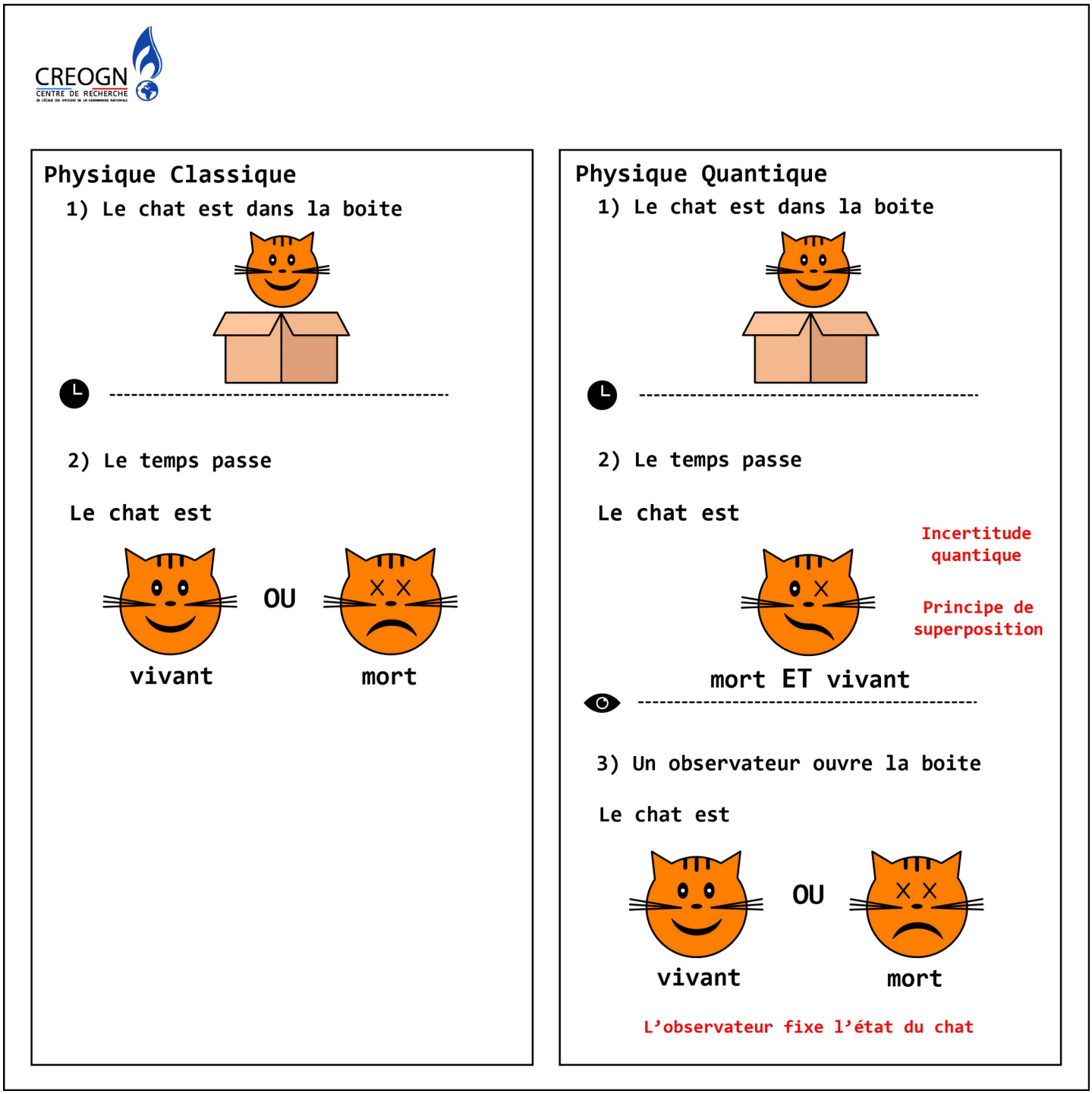
Avantages/gains :

• Possibilité de résoudre des calculs et des problèmes hors d'atteinte pour des systèmes traditionnels (notion de « suprématie quantique ») ;
• Permet de dépasser les limites physiques atteintes par la miniaturisation des processeurs, obstacle à l'augmentation des puissances de calcul énoncée par la loi de Moore ;
• Accélération conséquente des opérations de déchiffrement de données utilisant des algorithmes « vulnérables » ne répondant pas aux standards post-quantiques ;
• La puissance de calcul en parallèle permettrait de grandement faciliter l'implémentation d'algorithmes d'apprentissage machine pour de l'intelligence artificielle (IA), ouvrant la possibilité pour cette technologie d'atteindre son plein potentiel ;
• Intégration théorique possible dans des systèmes informatiques « hybrides » ayant une architecture traditionnelle pour la gestion et le stockage de données et une architecture quantique pour les tâches de calcul. C'est le chemin de développement le plus probable pour la démocratisation de la technologie.

Inconvénients/difficultés :

• Les systèmes quantiques ne se substituent pas à l'informatique classique. Les spécificités de la physique quantique la rendent propice à la résolution de problèmes mathématiques complexes mais elle reste difficile à généraliser pour des cas d'usage quotidiens ;
• La nature probabilistique du quantique est une lame à double tranchant qui génère aussi des marges d'erreur difficiles à corriger à l'heure actuelle, faussant ainsi certains résultats ;
• Ce phénomène est amplifié par la fragilité des systèmes quantiques due au principe de « décohérence » (interférences liées à l'environnement direct) qui implique des conditions de mise en œuvre très particulières pour pouvoir les utiliser correctement ;
• La vulnérabilité théorique des algorithmes actuels signifie qu'il existe un risque qu'un attaquant intercepte des données dès aujourd'hui pour pouvoir les décrypter dans le « futur », une fois qu'un ordinateur quantique viable sera disponible (déchiffrement rétrospectif) ;
• Cette technologie est toujours au stade expérimental, signifiant qu'il subsiste encore des interrogations et des besoins de financement conséquents afin de déterminer le dispositif technique le plus à même de créer une architecture quantique optimale stable et tolérante aux erreurs.

Schéma du chat de Schrödinger



La célèbre expérience de pensée du chat de Schrödinger permet d'illustrer le principe contre-intuitif de superposition d'état mais aussi de ce que les physiciens ont longtemps appelé « le problème de la mesure ». On imagine qu'un chat est placé dans une boîte fermée équipée d'un mécanisme pouvant provoquer la rupture d'une fiole de poison, tuant ainsi l'animal. Le déclenchement du système est basé sur un processus atomique ayant une chance sur deux d'aboutir au bout d'un certain temps. La physique quantique admet que tant que la boîte n'est pas ouverte, il est impossible de pouvoir déterminer l'état du chat. Pour s'assurer de son sort il est donc nécessaire de regarder à l'intérieur de la boîte, ce qui, dans le monde quantique, revient à effectuer une mesure. C'est l'acte de la mesure lui-même qui force la « fixation » d'un état définitif en vertu de sa transition de la physique quantique vers la physique classique.