

QU'EST-CE QUE L'INFORMATIQUE QUANTIQUE ?

L'informatique quantique¹ repose sur les principes de la mécanique quantique, une théorie physique vieille de plus de 100 ans qui décrit le comportement des très petites particules (atomiques et subatomiques). Contrairement aux objets classiques qui existent à un endroit et à un moment donnés, les particules quantiques sont mieux comprises comme existant dans de multiples états possibles (voir ci-dessous). Ces propriétés défient notre logique habituelle de cause à effet, mais elles sont déjà bien établies et utilisées dans des technologies courantes telles que les lasers, l'imagerie par résonance magnétique (IRM), les semi-conducteurs, la recherche biologique ou encore les smartphones².

Les ordinateurs traditionnels utilisent des bits valant 0 ou 1, tandis que les ordinateurs quantiques fonctionnent avec des qubits (quantum bits) qui peuvent exister dans plusieurs états à la fois. Cela permet aux qubits de traiter beaucoup plus d'informations, de réaliser de nombreux calculs simultanément, et de résoudre des problèmes beaucoup plus rapidement que les machines traditionnelles. Une autre propriété remarquable des qubits est l'intrication quantique (entanglement en anglais), un phénomène dans lequel deux qubits deviennent interconnectés de telle sorte que l'état de l'un révèle instantanément des informations sur l'autre, quelle que soit la distance qui les sépare³.

Les aspects physiques et technologiques de l'informatique quantique présentent des défis majeurs. Les qubits sont fragiles et très sensibles aux perturbations environnementales. Ils tombent facilement dans un état que les physiciens appellent la décohérence, ou subissent d'autres types d'erreurs.⁴ Surmonter ces défis physiques est à la fois coûteux et technologiquement complexe, car cela nécessite de protéger les qubits contre les interférences à l'aide de techniques comme le refroidissement extrême ou le blindage magnétique, encore en développement.⁵ La complexité de la programmation quantique et l'absence de normes universelles signifient également que la production de logiciels est coûteuse, limitée à un nombre restreint d'entreprises, et souvent adaptée à un seul appareil. À ce jour, la plupart des applications de l'informatique quantique restent théoriques, et aucune n'est encore prête à être déployée à grande échelle sur le marché, bien que certaines avancées importantes réalisées au cours de la dernière année suggèrent que l'informatique quantique pourrait arriver plus tôt que prévu.

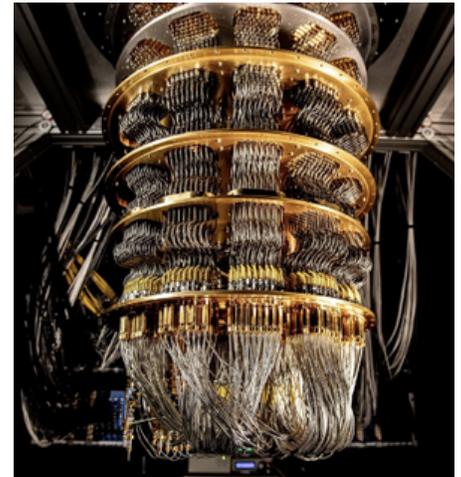


Figure 1 Le système d'informatique quantique de Google

PERCÉES ET DÉVELOPPEMENTS RÉCENTS

En 2019, un groupe de recherche chez Google Quantum AI a démontré que son processeur quantique pouvait réaliser en 200 secondes une tâche informatique qui aurait pris plus de 10 000 ans à un ordinateur classique.⁶ Depuis, d'importantes avancées ont permis de réduire les interférences et d'améliorer la connexion des qubits au sein de machines plus puissantes, notamment : (a) la puce quantique « Willow » de Google annoncée en décembre 2024, capable de réduire considérablement le bruit et le taux d'erreur ; (b) le lancement en février 2025 de processeurs quantiques distribués de l'Université d'Oxford, permettant une puissance de traitement bien plus élevée ; (c) un processeur quantique supraconducteur de 62 qubits, produit par l'Université des sciences et technologies de Chine (USTC) en 2021.⁷

Les investissements dans l'informatique quantique ont explosé ces dernières années, alors que les gouvernements et les grandes entreprises technologiques se livrent une course pour être les premiers à commercialiser des applications pratiques.⁸ Les États-Unis, la Chine, l'Union européenne, l'Allemagne, le Royaume-Uni, le Japon, l'Inde et bien d'autres pays ont considérablement renforcé leurs investissements dans des stratégies nationales quantiques.⁹ À ce jour, plus de 50 milliards de dollars ont été investis dans la recherche et le développement en informatique quantique.¹⁰ Au cours des prochaines années, certaines des applications pratiques les plus importantes de l'informatique quantique pourraient inclure les domaines suivants :

Sécurité et cryptographie: Les ordinateurs quantiques pourraient devenir capables de casser les systèmes de sécurité classiques en quelques secondes, ce qui nécessiterait le développement de communications quantiques sécurisées. Cette perspective a suscité d'importants investissements nationaux et l'élaboration de nouveaux protocoles de sécurité pour anticiper ces applications potentiellement transformatrices de l'informatique quantique.¹¹

Santé et médecine: La conception de médicaments repose sur la simulation du comportement des molécules, impliquant souvent des milliards d'interactions et de résultats potentiels à tester. Les premières recherches suggèrent que la convergence entre le traitement quantique et les outils d'intelligence artificielle (IA) pourrait

permettre d'aborder certaines des simulations les plus complexes, notamment la modélisation du repliement des protéines.¹² D'autres applications médicales incluent le diagnostic de maladies, la simulation des effets de l'édition génétique, et la modélisation de pandémies à l'échelle mondiale.¹³

Climat et énergie:

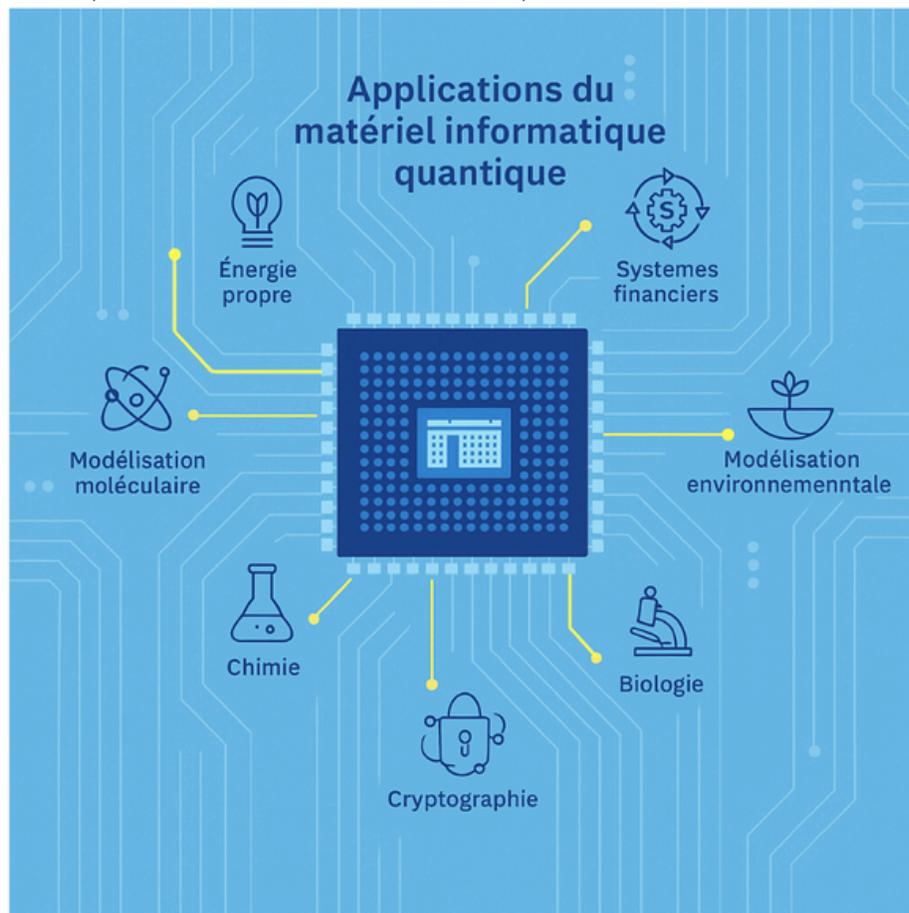
La modélisation des scénarios climatiques futurs et le développement des énergies renouvelables pourraient directement bénéficier de l'énorme potentiel de l'informatique quantique. Dans certains scénarios, les approches pilotées par l'informatique quantique pourraient permettre une augmentation spectaculaire de la production d'énergie propre, des solutions énergétiques hautement optimisées, une modélisation climatique plus précise, et une consommation d'énergie bien inférieure à celle des ordinateurs classiques.¹⁴

Finance et commerce: Les systèmes financiers complexes sont difficiles à modéliser avec les méthodes informatiques traditionnelles, mais l'informatique quantique pourrait permettre une modélisation bien plus précise et fiable dans un avenir relativement proche.¹⁵ Cela

modélisation des marchés financiers, ainsi que l'optimisation des routes commerciales et des structures d'échange à l'échelle mondiale.

Conclusion:

Le potentiel de l'informatique quantique pour prédire et modéliser plus précisément les tendances et dynamiques mondiales complexes pourrait permettre des investissements plus efficaces dans le développement durable, avec des implications majeures pour notre capacité collective à atteindre la neutralité carbone (net zero) et faire face



aux crises inter-connectées du changement climatique, de la pollution et de la perte de biodiversité. D'autres domaines tels que le transport, la production industrielle, la recherche biologique ou encore les neurotechnologies pourraient devenir fortement dépendants de l'informatique quantique dès que des systèmes pratiques et évolutifs seront disponibles.¹⁶ L'Open Quantum Institute (OQI), lancé au sein du GESDA en 2023 et actuellement incubé au CERN pour sa phase pilote (2024–2026), a précisé sa mission de promouvoir un accès mondial, équitable et inclusif à l'informatique quantique, et à travers cela, d'explorer les applications susceptibles de bénéficier à l'humanité.

CONSÉRATIONS POUR L'ONU

L'Assemblée générale des Nations Unies a proclamé 2025 comme Année internationale des sciences et technologies quantiques, avec l'UNESCO jouant un rôle de coordination pour le système des onusien.¹⁷ Cela constitue une incitation à se concentrer sur le potentiel des technologies quantiques à accélérer les progrès en matière de développement durable, tout en évaluant attentivement les risques associés aux avancées rapides qui se profilent. Parmi les questions et domaines de risques les plus importants à considérer pour le système des Nations Unies, on peut citer :

Une « course à l'armement » quantique: Les gouvernements s'efforcent de préparer leurs systèmes de sécurité nationale à d'éventuelles perturbations liées à l'informatique quantique, même si les avancées majeures en cryptographie ne devraient pas voir le jour avant au moins dix ans.¹⁸ À l'instar de la course à la domination dans le domaine de l'IA, la course quantique pourrait rapidement s'intensifier si un gouvernement ou une entreprise revendiquait une avancée technologique leur permettant de briser les systèmes de sécurité d'autres pays. Au sein de l'ONU, l'Union internationale des télécommunications (UIT) élabore des normes pour soutenir l'adoption sécurisée et interopérable de ces technologies, ce qui sera crucial à mesure que cette course s'intensifie. L'ONU pourrait s'appuyer sur ces travaux en promouvant des mécanismes de vérification des capacités quantiques, et en développant des principes et normes généraux pour leur développement et déploiement en toute sécurité.



Droits de l'homme: Avec sa capacité à briser facilement les systèmes de cryptage traditionnels, l'informatique quantique pourrait potentiellement être utilisée pour violer la vie privée, manipuler des communautés, ou restreindre la liberté d'expression. L'année dernière, l'UNESCO a organisé une série de discussions sur les implications sociales, éthiques et liées aux droits humains de l'informatique quantique.¹⁹ Il sera essentiel à l'avenir de mieux comprendre ces implications et de définir le rôle que l'ONU peut jouer pour adapter ses approches face à ces nouveaux risques émergents.

Enjeux sociaux et économiques :

Aujourd'hui, les investissements dans l'informatique quantique sont concentrés dans un petit nombre de pays, avec un engagement croissant du secteur privé. Comme pour l'intelligence artificielle, cela pourrait conduire à des scénarios d'inégalités mondiales, où les bénéfices de l'informatique quantique (dans les domaines de la finance, de la santé ou du développement) seraient inégalement répartis, accentuant la fracture numérique déjà existante dans le cadre de l'Année internationale des sciences et technologies quantiques, l'UNESCO coordonne des stratégies visant à réduire la fracture quantique, avec un accent particulier sur les disparités entre le Nord et le Sud global. Dans ce contexte, le rôle de l'ONU dans l'établissement de normes, de standards et de réglementations internationales pourrait devenir particulièrement crucial, à mesure que l'informatique quantique devient une réalité au cours de la prochaine décennie.

Aujourd'hui, aucune application pratique de l'informatique quantique n'existe encore, mais les importants investissements mondiaux dans cette technologie montrent que de nombreux gouvernements et autres acteurs perçoivent son potentiel de transformation dans plusieurs secteurs clés. Savoir comment positionner l'ONU dans ce moment de transformation qui émerge représente une excellente opportunité pour le UN Futures Lab récemment établi par le Secrétaire général, pour les fonctions de prospective du Conseil scientifique consultatif, pour les partenaires scientifiques de l'ONU tels que le GESDA, l'Open Quantum Institute, et le ou la future Envoyée spéciale des Nations Unies pour les générations futures. En s'appuyant sur l'Année internationale des sciences et technologies quantiques, l'ONU pourrait attirer l'attention sur les nombreuses applications transformatrices que l'informatique quantique pourrait offrir.

RÉFÉRENCES

1 Cette note reflète les points de vue des scientifiques indépendants du Conseil scientifique consultatif. Elle a bénéficié de l'examen d'experts de l'UIT, de l'UNESCO, de UNU et de la GESDA. Elle ne reflète pas nécessairement la position de l'ONU ni celle des institutions partenaires. La mention d'une entreprise ou d'un produit commercial dans ce document n'implique en aucun cas une approbation de la part de l'ONU ou des auteurs. L'utilisation des informations contenues dans ce document à des fins publicitaires ou promotionnelles n'est pas autorisée. Les noms et symboles de marques sont utilisés à des fins éditoriales, sans intention de porter atteinte aux lois sur les marques ou le droit d'auteur. Nous regrettons toute erreur ou omission qui aurait pu être commise involontairement.

2 Voir, par exemple, Taylor, Michael A., et Warwick P. Bowen. « Quantum metrology and its application in biology. » *Physics Reports* 615 (2016) : 1-59; Gill, Sukhpal Singh, et al. « Quantum Computing: Vision and Challenges. » *arXiv preprint arXiv:2403.02240* (2024); Gmachi, Claire, et al. « Recent progress in quantum cascade lasers and applications. » *Reports on Progress in Physics* 64.11 (2001) : 1533; Yukawa, Hiroshi, et al. « Quantum life science: biological nano quantum sensors, quantum technology-based hyperpolarized MRI/NMR, quantum biology, and quantum biotechnology. » *Chemical Society Reviews* (2025); McDermott, Robert, et al. « Microtesla MRI with a superconducting quantum interference device. » *Proceedings of the National Academy of Sciences* 101.21 (2004) : 7857-7861; Wang, Aijuan, et al. « HQNet: A hybrid quantum network for multi-class MRI brain classification via quantum computing. » *Expert Systems with Applications* 261 (2025) : 125537.

3 Pour en savoir plus sur les applications potentielles de l'informatique quantique, voir Azhari, Rama, et Agita Nisa Salsabila. « Analyzing the Impact of Quantum Computing on Current Encryption Techniques. » *IAIC Transactions on Sustainable Digital Innovation (ITSDI)* 5.2 (2024) : 148-157; Vadisetty, Rahul, et Anand Polamarasetti. « Quantum Computing For Cryptographic Security With Artificial Intelligence. » 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA). IEEE, 2024.

4 Voir également Bacon, Dave Morris. *Decoherence, control, and symmetry in quantum computers*. University of California, Berkeley, 2001; Martinez, Josu Etxezarreta. « Decoherence and quantum error correction for quantum computing and communications. » *arXiv preprint arXiv:2202.08600* (2022); Abad, Tahereh, et al. « Impact of decoherence on the fidelity of quantum gates leaving the computational subspace. » *arXiv preprint arXiv:2302.13885* (2023); Park, Kimin, et al. « Slowing quantum decoherence of oscillators by hybrid processing. » *npj Quantum Information* 8.1 (2022) : 67; Gill, Sukhpal Singh, et al. « Quantum Computing: Vision and Challenges. » *arXiv preprint arXiv:2403.02240* (2024).

5 Voir enfin Gill, Sukhpal Singh, et al. « Quantum computing: A taxonomy, systematic review and future directions. » *Software: Practice and Experience* 52.1 (2022) : 66-114.

6 Arute, Frank, et al. « Quantum supremacy using a programmable superconducting processor. » *Nature* 574.7779 (2019) : 505-510.

7 Voir, Jerbi, S., Gyurik, C., Marshall, S.C. et al. « Shadows of quantum machine learning. » *Nature Communications* 15, 5676 (2024). <https://doi.org/10.1038/s41467-024-49877-8>; Wang, Yunfei, et Junyu Liu. « A comprehensive review of Quantum Machine Learning: from NISQ to Fault Tolerance. » *Reports on Progress in Physics* (2024); Melnikov, Alexey, et al. « Quantum machine learning: from physics to software engineering. » *Advances in Physics: X* 8.1 (2023) : 2165452.

8 Pour une liste des entreprises du secteur privé impliquées dans le quantique, voir : <https://technologymagazine.com/top10/top-10-quantum-computing-companies>.

9 Pour une cartographie utile des investissements, voir : <https://www.gureca.com/quantum-initiatives-worldwide/>.

10 Voir : <https://radar.gesda.global/opportunities/open-quantum-institute-incubation-phase> ; <https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/>

11 S. Mitra, B. Jana, S. Bhattacharya, P. Pal et J. Poray, « Quantum cryptography: Overview, security issues and future challenges, » 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, Inde, 2017, pp. 1-7, doi: 10.1109/OPTRONIX.2017.8350006; Portmann, Christopher, et Renato Renner. « Security in quantum cryptography. » *Reviews of Modern Physics* 94.2 (2022) : 025008; Sonko, Sedat, et al. « Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. » *Computer Science & IT Research Journal* 5.2 (2024) : 390-414.

12 Blunt, Nick S., et al. « Perspective on the Current State-of-the-Art of Quantum Computing for Drug Discovery Applications. » *Journal of Chemical Theory and Computation*, vol. 18, no. 12, 2022, p. 7001-7023; Robert, Anton, et al. « Resource-efficient quantum algorithm for protein folding. » *npj Quantum Information* 7.1 (2021) : 38; Casares, Pablo Antonio Moreno, Roberto Campos, et Miguel Angel Martin-Delgado. « QFold: quantum walks and deep learning to solve protein folding. » *Quantum Science and Technology* 7.2 (2022) : 025013; Casares, Pablo Antonio Moreno, Roberto Campos, et Miguel Angel Martin-Delgado. « QFold: quantum walks and deep learning to solve protein folding. » *Quantum Science and Technology* 7.2 (2022) : 025013.

13 Voir, Ur Rasool, Raihan, et al. « Quantum computing for healthcare: A review. » *Future Internet* 15.3 (2023):94; Kumar, Avinash, et al. « Quantum computing for health care: a review on implementation trends and recent advances. » *Multimedia Technologies in the Internet of Things Environment, Volume 3* (2022):23-40; Flöther, Frederik F. « The state of quantum computing applications in health and medicine. » *Research Directions: Quantum Technologies 1* (2023):e10; Jayanthi, Prisilla, Bharatendra K. Rai, et Iyyanki Muralikrishna. « The potential of quantum computing in healthcare. » *Technology Road Mapping for Quantum Computing and Engineering*. IGI Global, 2022. p. 81-101; Aggarwal, Lakshita, Shelly Sachdeva, et Puneet Goswami. « Quantum healthcare computing using precision based granular approach. » *Applied Soft Computing* 144 (2023):110458.

14 Voir, Berger, Casey, et al. « Quantum technologies for climate change: Preliminary assessment. » arXiv preprint arXiv:2107.05362 (2021); Ajagekar, Akshay, et Fengqi You. « Quantum computing and quantum artificial intelligence for renewable and sustainable energy: A emerging prospect towards climate neutrality. » *Renewable and Sustainable Energy Reviews* 165 (2022):112493; Ho, Kin Tung Michael, et al. « Quantum computing for climate resilience and sustainability challenges. » *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*. Vol. 2. IEEE, 2024; Ashwani, Siddhant, et al. « Quantum Computing for Climate Change: A Comprehensive Review of Current Applications, Challenges, and Future Directions. » *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2024.

15 Orús, Román, Samuel Mugel et Enrique Lizaso. « Quantum computing for finance: Overview and prospects. » *Reviews in Physics* 4 (2019):100028.

16 Pour plus de littérature sur ces sujets, voir Herman, Dylan, et al. « Quantum computing for finance. » *Nature Reviews Physics* 5.8 (2023):450-465; De Leon, Nathalie P., et al. « Materials challenges and opportunities for quantum computing hardware. » *Science* 372.6539 (2021):eabb2823; Ollitrault, Pauline J., Alexander Miessen et Ivano Tavernelli. « Molecular quantum dynamics: A quantum computing perspective. » *Accounts of Chemical Research* 54.23 (2021):4229-4238; Preskill, John. « Quantum computing 40 years later. » *Feynman Lectures on Computation*. CRC Press, 2023. p. 193-244; Caleffi, Marcello, et al. « Distributed quantum computing: a survey. » *Computer Networks* 254 (2024):110672; Kim, Youngseok, et al. « Evidence for the utility of quantum computing before fault tolerance. » *Nature* 618.7965 (2023):500-505; Gill, Sukhpal Singh, et al. « Quantum computing: A taxonomy, systematic review and future directions. » *Software: Practice and Experience* 52.1 (2022):66-114; LaPierre, Ray. *Introduction to quantum computing*. Springer Nature, 2021; Ur Rasool, Raihan, et al. « Quantum computing for healthcare: A review. » *Future Internet* 15.3 (2023):94; Nimbe, Peter, Benjamin Asubam Weyori et Adebayo Felix Adekoya. « Models in quantum computing: a systematic review. » *Quantum Information Processing* 20.2 (2021):80; Peral-García, David, Juan Cruz-Benito et Francisco José García-Peñalvo. « Systematic literature review: Quantum machine learning and its applications. » *Computer Science Review* 51 (2024):100619; Arute, Frank, et al. « Quantum supremacy using a programmable superconducting processor. » *Nature* 574.7779 (2019):505-510.

17 Assemblée générale des Nations Unies. Année internationale de la science et de la technologie quantiques, 2025. Résolution adoptée par l'Assemblée générale A/RES/78/287 (Nations Unies, 2024).

18 Par exemple, en 2021, les États-Unis ont mis en place une stratégie exigeant que toutes les agences fédérales adoptent la cryptographie post-quantique (PQC) d'ici 2030. La Commission européenne, Singapour, l'Australie et d'autres pays ont mis en place des dispositifs de suivi des capacités quantiques, des recommandations et des feuilles de route pour moderniser la cryptographie et les communications.

19 <https://unesdoc.unesco.org/ark:/48223/pf0000388955>.