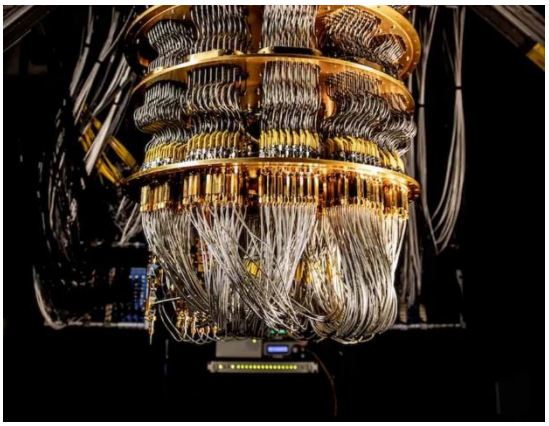
Baptiste Picard

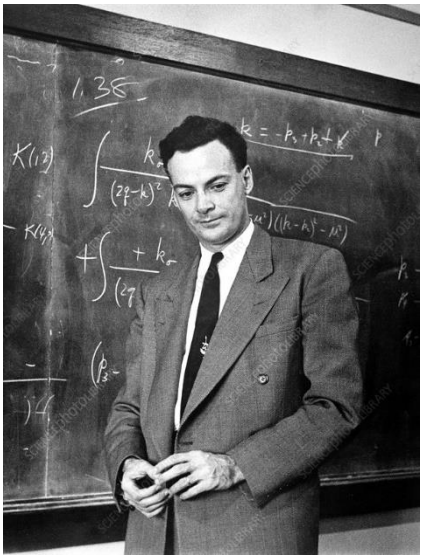
Ordinateur quantique :
Les Secrets de la Technologie de Demain

Introduction et histoire :

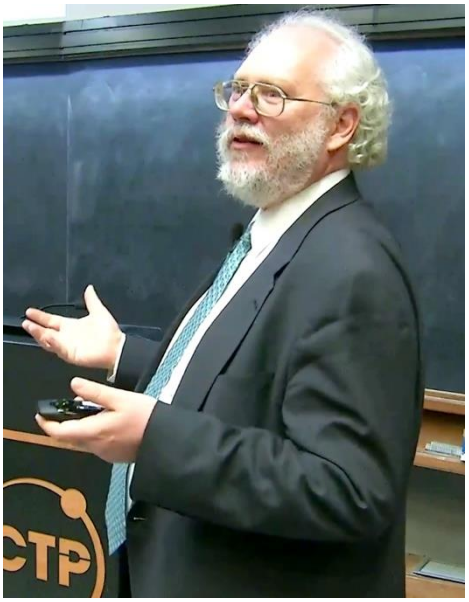
L'histoire de l'ordinateur quantique remonte aux années 1980, lorsqu'un certain nombre de chercheurs ont commencé à explorer la possibilité d'utiliser les principes de la mécanique quantique pour révolutionner l'informatique. L'idée maîtresse est de tirer parti des phénomènes quantiques tels que la superposition et l'intrication pour effectuer des calculs beaucoup plus rapidement que ce qui est possible avec les ordinateurs classiques.



L'un des pionniers dans ce domaine est le physicien Richard Feynman, qui, en 1981, a suggéré que les ordinateurs basés sur la physique quantique pourraient être capables de simuler des systèmes quantiques beaucoup plus efficacement que les ordinateurs classiques. Peu après, en 1985, le chercheur britannique David Deutsch a formalisé l'idée d'un ordinateur quantique en publiant un modèle théorique de calcul quantique, connu sous le nom de « machine de Turing quantique ».



Le développement de l'ordinateur quantique a connu des avancées majeures dans les années 1990, lorsque Peter Shor, un mathématicien américain, a proposé en 1994 un algorithme quantique capable de factoriser des grands nombres entiers de manière exponentiellement plus rapide qu'un algorithme classique. Cet algorithme de Shor a mis en lumière l'impact potentiel de l'informatique quantique, en particulier dans le domaine de la cryptographie.



Depuis lors, de nombreuses entreprises technologiques et instituts de recherche se sont lancés dans la course au développement d'un ordinateur quantique fonctionnel à grande échelle. En 2019, Google a annoncé avoir atteint la « suprématie quantique » avec son processeur quantique Sycamore, réalisant un calcul en 200 secondes que le plus puissant superordinateur classique mettrait des milliers d'années à résoudre.

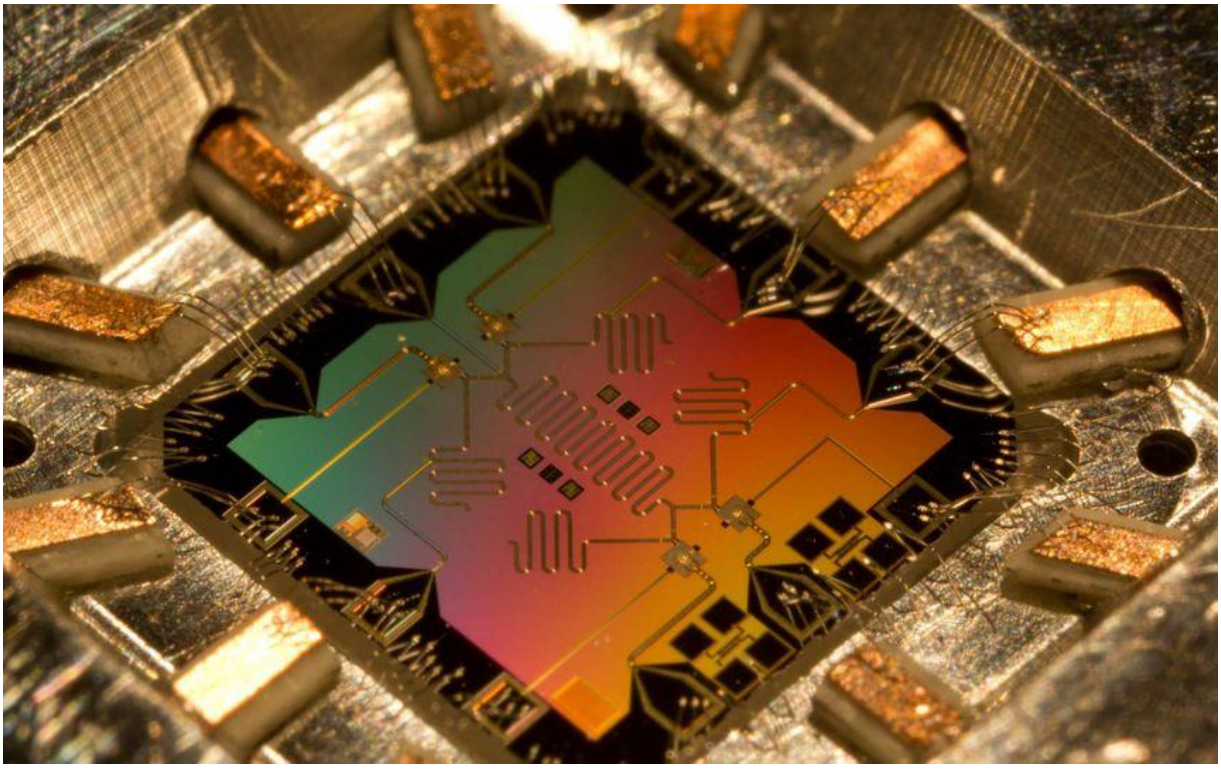
Etude de marché :

Offreurs :

Les principaux acteurs dans le domaine de l'informatique quantique incluent à la fois des entreprises technologiques, des startups spécialisées et des institutions académiques. Parmi les grandes entreprises, IBM (leader du marché), Google, Microsoft et Amazon sont à la pointe du développement des technologies quantiques. IBM, par exemple, propose son service de cloud quantique IBM Quantum Experience, qui permet aux utilisateurs d'accéder à un ordinateur quantique en ligne. Google, avec son programme Google Quantum AI, continue de travailler sur la mise au point de processeurs quantiques plus puissants. Des startups comme Rigetti Computing, IonQ, et D-Wave Systems se concentrent également sur le matériel et les algorithmes quantiques.

Demandeurs :

La demande en informatique quantique provient de divers secteurs. Les gouvernements et les agences de défense, en particulier, s'intéressent fortement à l'impact potentiel des ordinateurs quantiques sur la cryptographie et la sécurité nationale. Le secteur financier explore la possibilité d'utiliser les ordinateurs quantiques pour des applications telles que la modélisation de portefeuilles financiers et la gestion des risques. L'industrie pharmaceutique et chimique voit aussi un énorme potentiel dans la simulation quantique, qui pourrait accélérer la découverte de nouveaux médicaments et matériaux. Enfin, des entreprises dans le domaine de la logistique et de l'intelligence artificielle se tournent vers l'informatique quantique pour résoudre des problèmes d'optimisation complexes.



Besoins :

L'informatique quantique répond à des besoins spécifiques que l'informatique classique ne peut pas satisfaire de manière efficace. Il s'agit principalement de la résolution de problèmes liés à la simulation de systèmes quantiques (par exemple, dans la chimie et la physique des matériaux), à l'optimisation combinatoire (comme dans la gestion de flux logistiques) et au traitement rapide de grandes quantités de données. Un besoin critique est également celui de la cryptographie post-quantique, c'est-à-dire le développement de nouvelles méthodes cryptographiques capables de résister aux attaques potentielles des ordinateurs quantiques sur les systèmes de cryptage classiques.

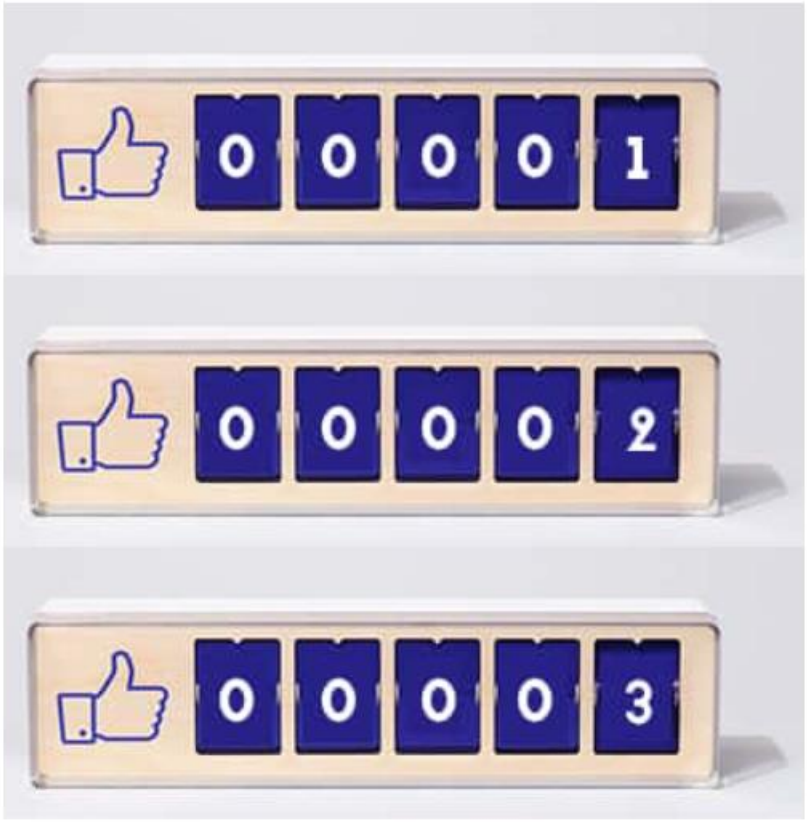
La technologie des ordinateurs quantiques connaît une croissance rapide, avec des avancées majeures dans plusieurs industries. Selon les projections, le marché global pourrait atteindre une valeur économique annuelle de 850 milliards de dollars d'ici 2040.


2,143.00
3,201.00
1,890.00
1,500.00
5,203.00
4,023.00
3,032.00
34,527.00
1,230.00
1,705.00
9,576.00
3,029.00
8,903.00
64,041.00
2,405.00
55,085.00
51,957.00
50,000.00
40,000.00
30,000.00

Technologie :

Les ordinateurs quantiques exploitent les principes de la mécanique quantique pour traiter l'information de manière radicalement différente des ordinateurs classiques.

Bits classiques : Dans un ordinateur classique, l'information est représentée par des bits, qui peuvent être soit 0 soit 1. L'ordinateur réalise 1 seule étape à la fois comme dans le schéma ci-dessous :



...

Qubits : Dans un ordinateur quantique, l'information est représentée par des qubits, qui peuvent être 0, 1 ou une superposition des deux. Cela signifie qu'un qubit peut exister simultanément dans plusieurs états. L'ordinateur quantique réalise toute ces étapes en même temps c'est ce que l'on appelle la superposition quantique.

Exemple :

5 bits = 1 état à la fois (2^5 = 32 combinaisons possibles, mais un seul état à la fois)

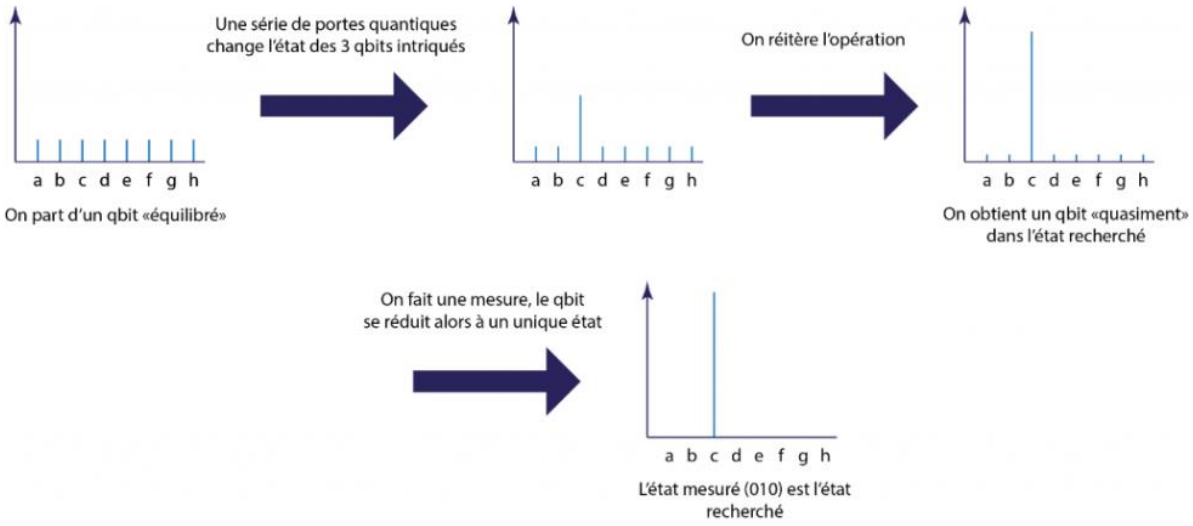
5 qubits = 32 états simultanément (grâce à la superposition, chaque qubit peut être à la fois 0 et 1, permettant 2^5 = 32 combinaisons à la fois)

Les qubits présentent une croissance exponentielle en termes de capacité d'information par rapport aux bits. En effet 10 qubits ne représentent que 1024 états simultanément tandis que 50 qubits peuvent représenter plus de 10^{15} états simultanément soit plus d'un trillion d'états.

En informatique quantique, les deux principales propriétés qui différencient les qubits des bits classiques sont la superposition et l'intrication.

La superposition permet à un qubit d'explorer plusieurs possibilités en même temps. Par exemple, si vous avez 2 qubits, vous pouvez avoir jusqu'à 2^2 = 4 états différents (00, 01, 10, 11) simultanément.

L'intrication est une propriété qui permet de lier plusieurs qubits de manière telle que l'état de l'un affecte instantanément l'état de l'autre, même s'ils sont séparés par de grandes distances. Lorsque deux qubits sont intriqués, la mesure de l'un détermine immédiatement l'état de l'autre. Cela crée une corrélation forte entre les qubits et permet des calculs quantiques très complexes, car la manipulation d'un qubit peut indirectement influencer les autres qubits intriqués.


Une série de portes quantiques
change l'état des 3 qbits intriqués
On réitère l'opération
a b c d e f g h
On part d'un qbit «équilibré»
On obtient un qbit «quasiment»
dans l'état recherché
On fait une mesure, le qbit
se réduit alors à un unique état
L'état mesuré (010) est l'état
recherché