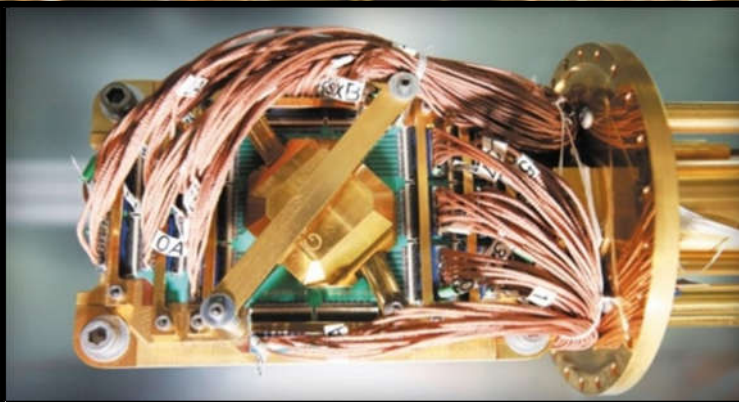
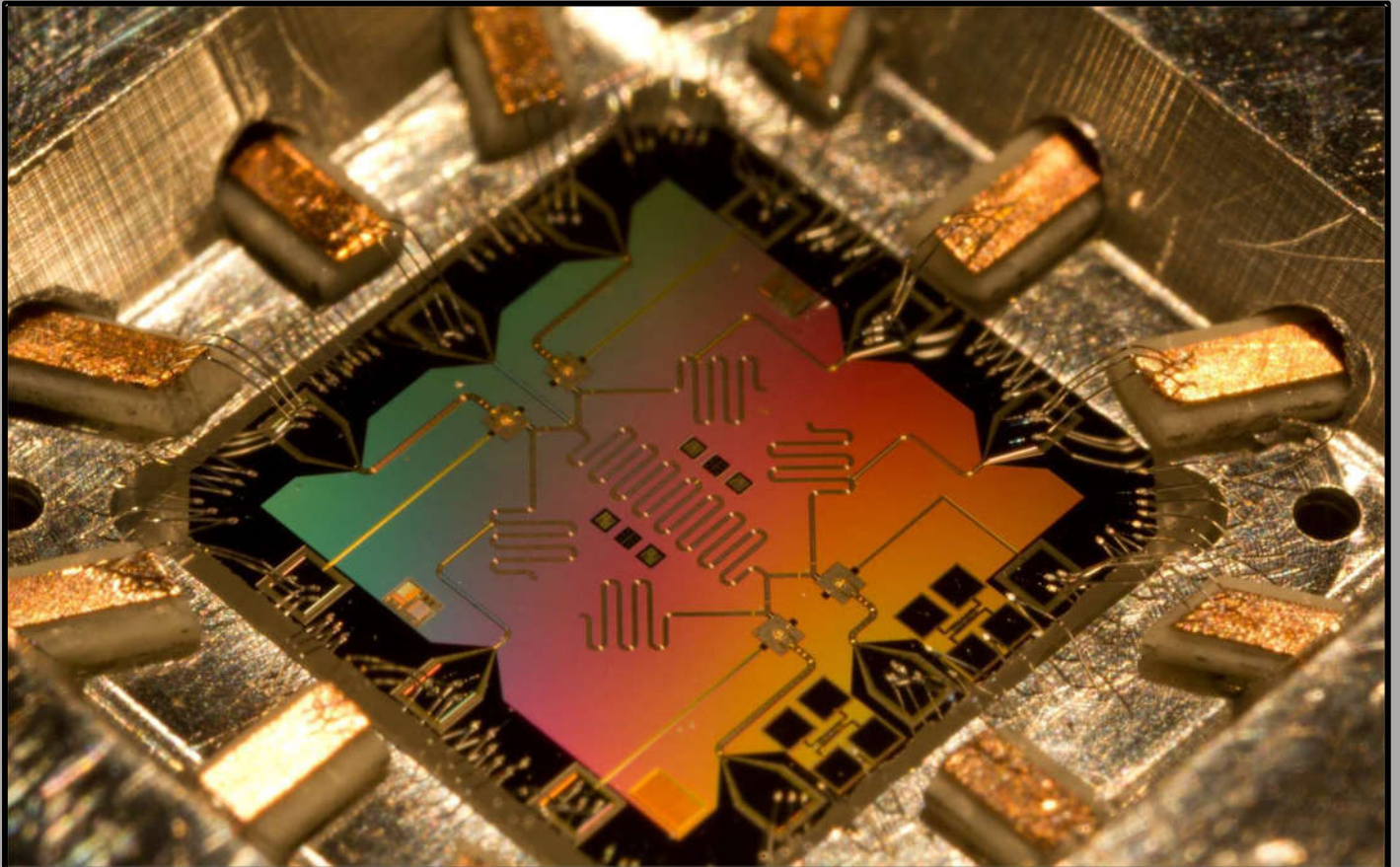


# L'ordinateur quantique



# Sommaire

- I. [Présentation général](#)
- II. [Un peu de physique quantique](#)
  - a. [La superposition](#)
  - b. [L'intrication quantique](#)
- III. [Comment fonctionne nos ordinateurs classiques](#)
- IV. [Le Qubit](#)
- V. [Utilisation](#)
- VI. [Puissance](#)
- VII. [Les possibilités](#)
- VIII. [Historique de l'ordinateur quantique jusqu'à aujourd'hui](#)
- IX. [L'avenir de l'ordinateur quantique](#)
- X. [conclusion](#)

# I. Présentation général

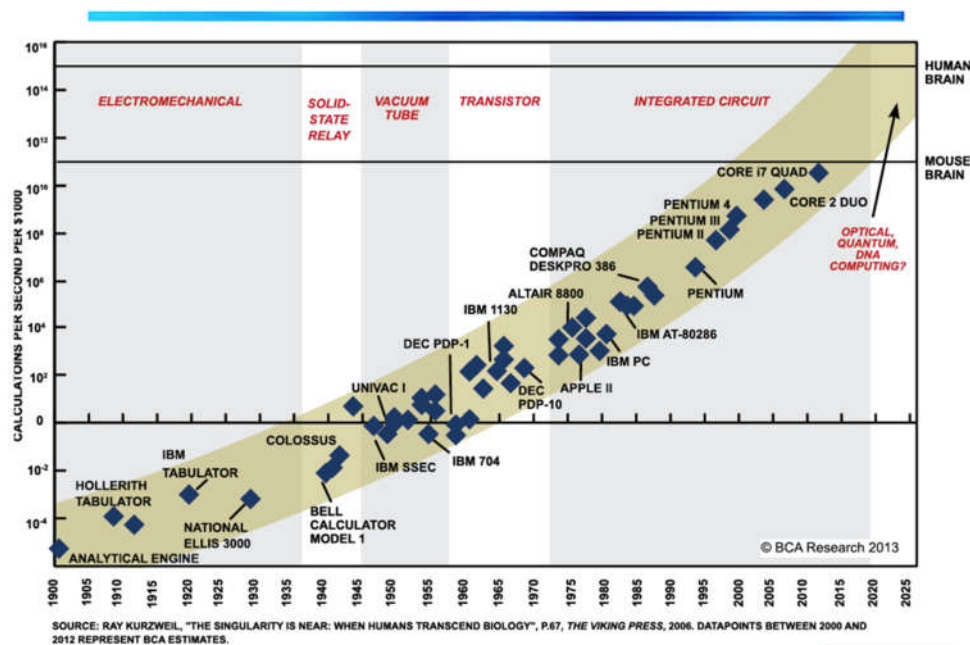
On entend de plus en plus parler de l'ordinateur quantique dans les médias, mais sans vraiment comprendre de quoi il s'agit.

Selon la loi de Moore, En 2020, les transistors seront de la taille d'un atome. On parle alors de processeurs ou d'ordinateurs quantiques.

"La loi de Moore concerne l'évolution de la puissance des ordinateurs. Selon cette loi le nombre de transistors, c'est-à-dire l'élément principal qui compose les processeurs des ordinateurs, double tous les deux ans. Et parallèlement double également la puissance des appareils. Moore fixa ensuite le cycle non plus sur deux ans mais dix-huit mois. Donc, selon Moore tous les 18 mois il y a doublement du nombre de transistors, rendant les ordinateurs rapidement obsolètes."

Et Moore avait raison. Sa loi s'est vérifiée jusqu'à aujourd'hui.

## Loi de Moore



<http://www.extremetech.com/wp-content/uploads/2015/04/MooresLaw2.png>

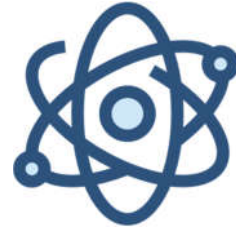


Maintenant passons à ce qui nous intéresse, l'ordinateur quantique :

Un calculateur quantique (anglais: quantum computer parfois traduit "ordinateur quantique", ou "système informatique quantique"), utilise les propriétés quantiques de la matière, telle que la superposition et l'intrication afin d'effectuer des opérations sur des données.

À la différence d'un ordinateur classique basé sur des transistors qui travaille sur des données binaires (codées sur des bits, valant 0 ou 1), le calculateur quantique travail sur des qubits dont l'état quantique peut posséder plusieurs valeurs en même temps.

Donc Pour résumer, un ordinateur quantique est un ordinateur qui utilise des particules subatomique au lieu de transistors. Grace aux propriétés de ces particules, on peut avoir une puissance de calcul beaucoup plus grande et donc surpasser tout ce qui existe déjà, mais ce n'est pas si simple...



## II. Un peu de physique quantique

La physique quantique est l'appellation générale d'un ensemble de théories physiques nées au XXe siècle qui décrivent le comportement des atomes et des particules.

### a. La superposition

Au début du XXe siècle, les physiciens se sont rendu compte du fait que la matière se comportait bizarrement dans l'infiniment petit. Par exemple, une particule de l'infiniment petit peut se trouver dans un état indéterminé avant toute mesure.

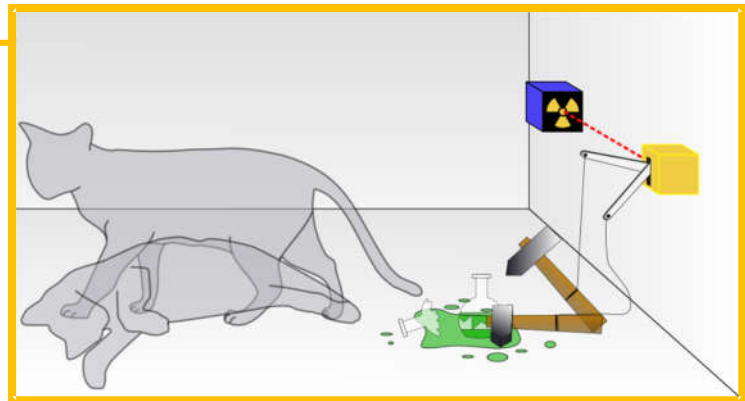
On peut faire une analogie avec l'expérience de pensée du "Chat de Schrödinger" imaginée en 1935 par le physicien Erwin Schrödinger.

On met dans une boîte un chat et une fiole de poison. On rajoute un mécanisme situé dans la boîte qui peut casser la fiole de poison à tout moment.

Si la fiole se casse, le chat meurt.

Donc du temps que la boîte est fermée, on ne sait pas si le chat est mort ou vivant, on peut donc en déduire que le chat est mort et vivant en même temps. Et on ne sera s'il est vivant ou mort qu'à partir du moment où ouvrira la boîte.

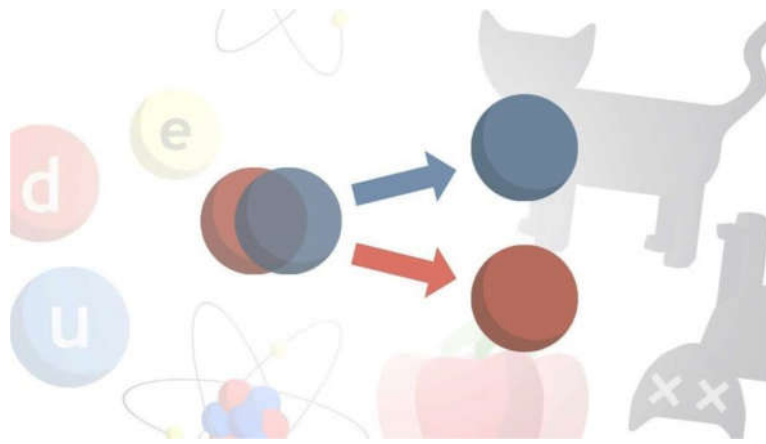
*"Je n'ai aucun moyen de savoir si le mécanisme s'est déclenché. Si mon chat était un objet quantique, je dirais qu'il est à la fois mort et vivant car selon la théorie de la superposition quantique, c'est tout à fait possible."* Erwin Schrödinger



Voilà ce qui explique grossièrement un des principes de la physique quantique.

Pour le remettre dans le contexte de l'infiniment petit des particules.

Les scientifiques ont pris un électron et se sont rendu compte qu'aussi incroyable que cela paraisse, il possédait à la fois deux vitesses, et est à deux endroits différents à la fois. Voire même plus de deux endroits !



Et lorsqu'on le mesure, l'électron reste fixé sur 1 seul état, comme pour le chat de Schrödinger lorsqu'on ouvre la boîte.

Pour désigner le fait qu'en mécanique quantique, les objets peuvent être dans plusieurs états à la fois, on parle du principe de superposition.

## b. L'intrication quantique

L'intrication est une autre propriété étonnante de la physique quantique. On peut lier deux objets quantiques a priori indépendants : par exemple, on peut les forcer à être dans des états opposés au moment d'une mesure.

Pour illustrer ça naïvement, imaginez 2 ampoules, chacune dans deux maisons différentes. En les intriquant, il deviendrait possible de connaître l'état d'une ampoule (allumée ou éteinte) en observant simplement la seconde, car les deux seraient liées, intriquées.

Revenons à la physique. Certaines particules microscopiques ont une propriété appelée le spin. Il n'est pas nécessaire de savoir de quoi il s'agit exactement. Si besoin, pensez à cela : vous êtes caractérisée, entre autre, par la couleur de vos cheveux. Cette couleur peut valoir "brun", "roux", "blond". Bref, c'est l'une de vos caractéristiques. Et bien une particule, elle, est caractérisée par son "spin", peu importe ce que c'est.

Tout ce que vous devez savoir, c'est que si une particule a un spin, il ne peut valoir que soit up, soit down. Imaginons maintenant l'expérience suivante :



1. On prend une particule sans spin



2. Elle se désintègre en deux particules quantiques qui peuvent avoir un spin : grâce à la superposition, lors d'une mesure, on pourra trouver pour chacune d'entre elles un spin up ou spin down avec une certaine probabilité



3. On sépare les deux particules de plusieurs kilomètres



4. On mesure le spin de la première, et immédiatement après, celui de la deuxième



On trouve un spin up pour la première

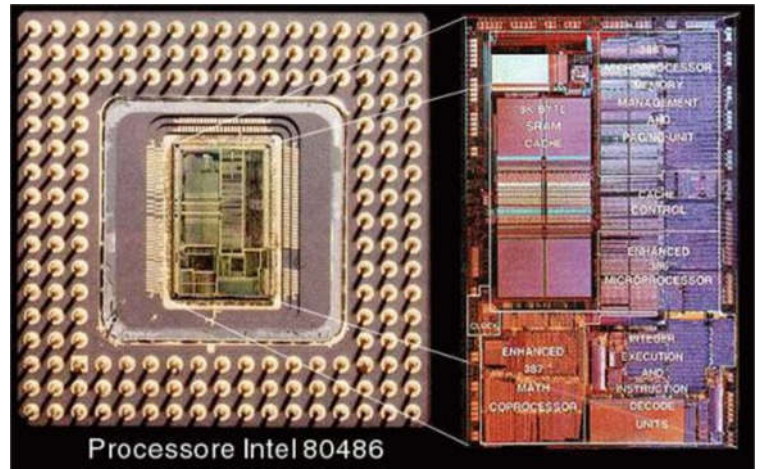
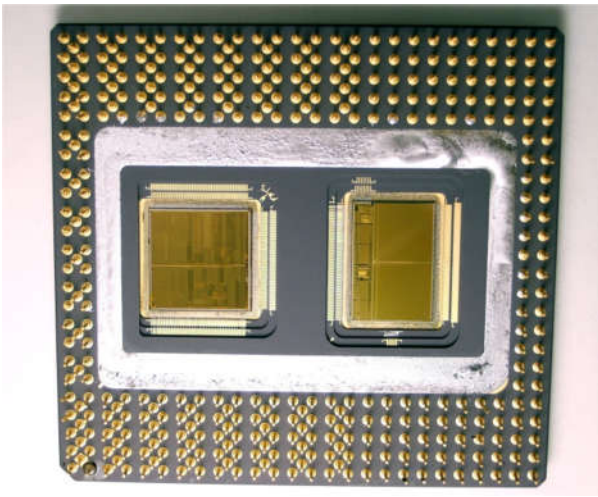


La mesure du spin de la deuxième particule donne down

### III. Comment fonctionne nos ordinateurs classiques

Avant d'aborder les principes de fonctionnement d'un ordinateur quantique, il serait intéressant de faire un petit rappel concernant la manière de calculer d'un ordinateur classique.

Globalement, il faut retenir que votre ordi traite l'information grâce à une série de circuits électriques qui s'allument et s'éteignent à la commande. Les statuts « allumer » et « éteint » sont respectivement représentés par des « 1 » et des « 0 » contenus dans une case, c'est ce qu'on appelle un bit. Le cerveau de votre machine est donc principalement constitué de milliards de cases contenant des 0 et des 1. Après traitement, cette information (la suite de 0 et de 1), est transformée en image, vidéo ou son et c'est tout.



Avant de parler d'un ordinateur quantique On va prendre un instant pour expliquer comment fonctionne un ordinateur classique, d'un point de vue fondamental.

Dans ces circuits un ordinateur traite ces informations sous forme binaire, des 0 et des 1. Électriquement c'est assez facile de se représenter comment cela fonctionne si le courant passe c'est un 1 et si le courant ne passe pas c'est un 0. À notre niveau quand on fait faire quelque chose à un ordinateur il utilise des algorithmes qui prennent des données en entrée et en fournissent en sortie. Et comme au niveau des circuits, ces données sont sous forme binaire, et bien un algorithme ça se réduit finalement à une suite d'instructions permettant de traiter et de manipuler des bits.

Ce qui traite l'information sous forme binaire s'appelle les portes logiques. Elles agissent directement sur les bits. Et physiquement ces portes logiques sont des transistors.

Un microprocesseur c'est essentiellement un gros paquet de transistors câblés entre eux qui permettent de réaliser des portes logiques et de manipuler les informations sous forme binaire.

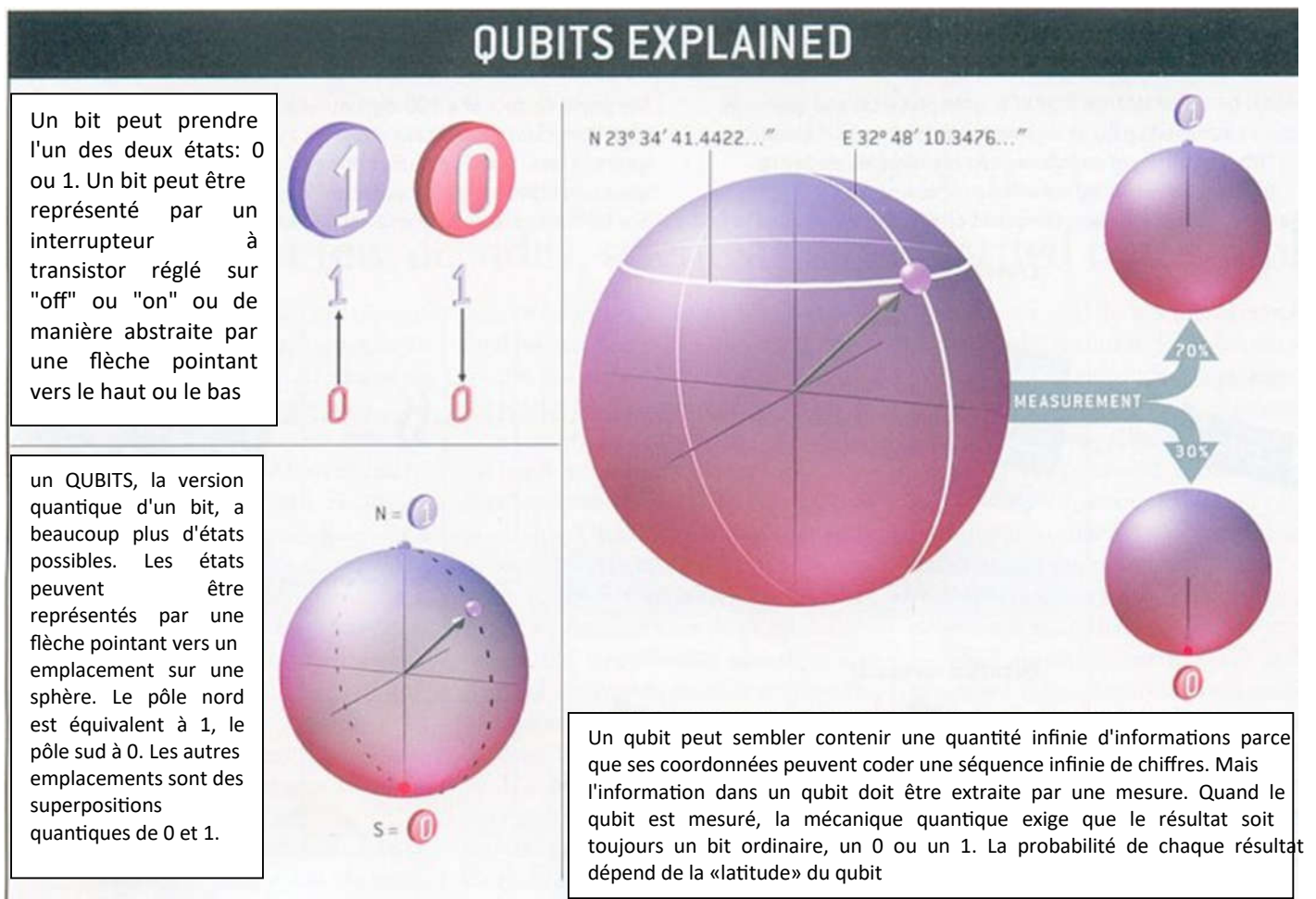
## IV. Le Qubit

L'ordinateur quantique traite comme son homologue classique de l'information. La différence majeure entre ces deux types d'ordinateurs est la manière de représenter cette information.

L'ordinateur classique représente l'information sous forme de bits (pour binary digit) qui peuvent avoir pour valeur 0 ou 1.

L'ordinateur quantique représente l'information à l'aide de qubits (pour quantum binary digit) qui ont un état qui est une superposition de deux états, 0 et 1.

Cela est possible du fait du principe de la superposition quantique ([Chat de Schrödinger](#))



Le fait d'avoir cet état de superposition entre le 0 et le 1 permet au qubit, quand il est accompagné d'un autre qubit d'avoir quatre états, et quand on rajoute deux autres qubits, on aura 16 états. La loi générale sera alors "2" à la puissance "n" avec "n" qui est le nombre de qubit dans le processeur.

Je vous laisse imaginer la quantité d'information qu'on pourrait traiter avec plusieurs qubits dans le processeur. Il existe plusieurs façons physiques de représenter un qubit, on peut le représenter par les spins d'électron, par les niveaux d'énergie dans un atome ou par la polarisation d'un photon.

## V. Utilisation

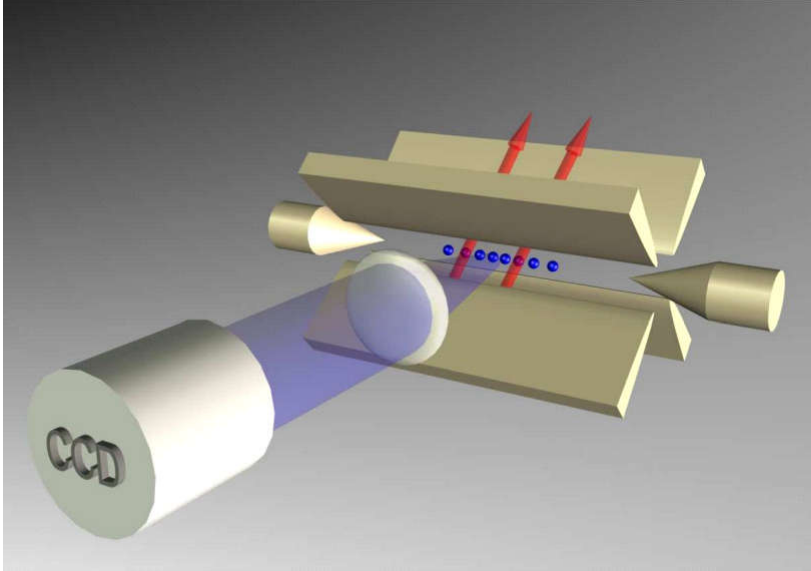
Pour implémenter des qubits utilisable pour le calcul, il faut être capable de réaliser un système macroscopique ayant des propriétés quantiques pendant un temps suffisamment long.



On utilise actuellement entre autres les procédés suivants :

Les circuits supraconducteurs avec jonction Josephson : technologie mise en œuvre par IBM depuis la fin des années 70 permettant d'envisager des circuits ayant une bonne résistance à la décohérence (perte de cohérence d'un objet possédant plusieurs états superposés).

Les ions piégés, sont constitués de particules chargées piégé par des champs magnétiques dans les espaces clos et ils sont contrôlés par laser. Ils permettent de mettre en œuvre le plus grand nombre de qubits.

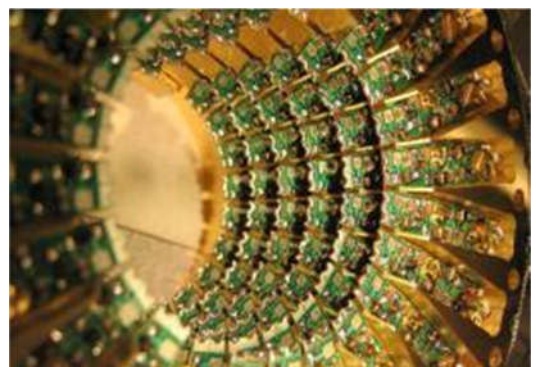


Des ions sont piégés dans un potentiel électromagnétique

- basse température
- transitions excitables par laser

Il existe un très grand nombre d'autre implémentation de qubits. Mais ce qu'il faut retenir, c'est que tout son délicate à mettre en œuvre et souvent à de très basse température ( $-273^{\circ}$ ) afin d'éviter les perturbations extérieures, au vu de la taille des installations nécessaires et de la complexité de mise en œuvre (installation cryogénique), on comprend que l'ordinateur quantique est confiné dans des centres de calcul.

Réfrigérants à l'hélium liquide nécessaire au refroidissement des composants



Filtre permettant de ne pas affecter le fonctionnement du processeur par champs magnétiques

D'autre part du fait de la taille réduite des données en entrée et en sortie, typiquement quelques bits, on peut envisager des accès par le web.

Par conséquent, on peut s'attendre à un usage grand public de l'informatique quantique dans un futur proche, du moins sous la forme d'appareil possédé par des particuliers.

## VI. Puissance

Votre ordinateur ne peut pas résoudre tous vos problèmes !

On a aussi l'impression que les ordinateurs peuvent résoudre tous les problèmes du monde parce qu'ils sont puissants et efficaces. Et c'est faux !

Les chercheurs rencontrent souvent des problèmes que leurs ordinateurs ne peuvent pas résoudre. Alors, ils cherchent des moyens de rendre leurs ordinateurs plus puissants. Pour rendre un ordinateur plus puissant, il faut :

- Augmenter sa mémoire (pour stocker + d'informations).
- Augmenter le nombre de transistors dont il dispose (pour traiter + d'informations).

Malheureusement, il arrive un moment où rajouter de la mémoire et du processeur ne suffit même plus à rendre l'ordi satisfaisant.

Mais même les meilleurs supercalculateurs (des ordinateurs géants, utilisés par les chercheurs) peuvent être surmenés par certains problèmes résolument trop compliqués – comme celui du [voyageur de commerce](#). Ces ordinateurs classiques ne sont pas faits pour résoudre ces problèmes complexes. Ils ne “pensent” tout simplement pas de la bonne manière.

### Qubits : deux valeurs à la fois



Les ordinateurs que nous utilisons actuellement codent les informations en séries de bits (0 ou 1). Un ordinateur quantique utilise des qubits, qui peuvent prendre deux valeurs à la fois (0 et 1) selon le principe de « superposition » que permettent les propriétés quantiques de la matière. Au sein du qubit, la part du 1 peut varier entre 0 % et 100 % (de gauche à droite de la première série), et de la même manière la part du zéro (de gauche à droite de la deuxième série).

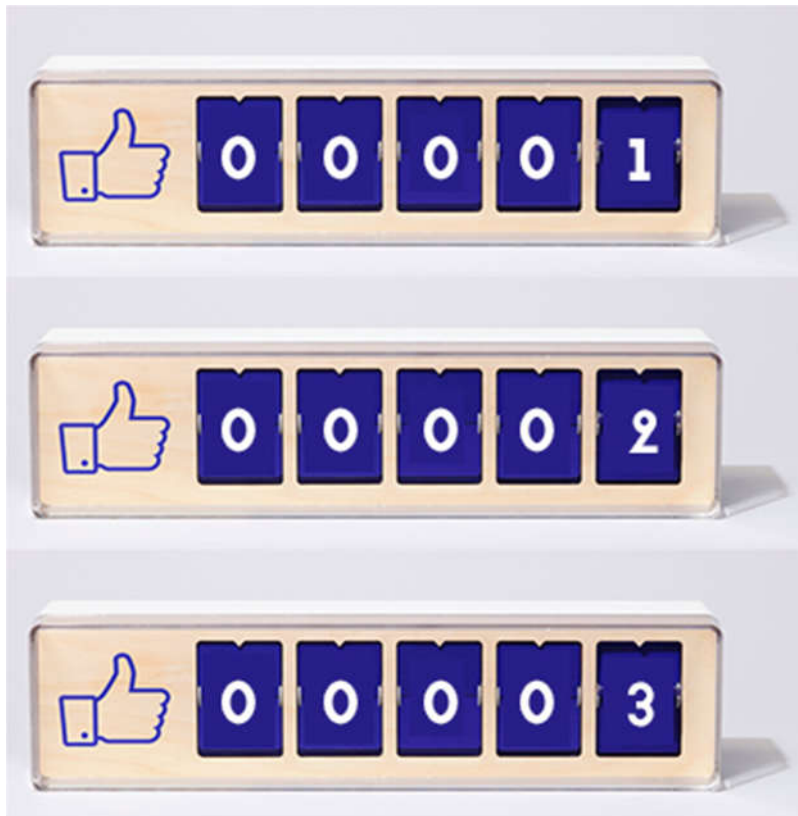
La base de tout : le qubit (à prononcer “kubite”)

Au lieu d'utiliser des bits qui ne peuvent prendre comme valeur que 0 ou 1, l'ordinateur quantique utilise des bits quantiques, ou qubits, qui ne prennent pas comme valeur 0 ou 1, mais une superposition de 0 et de 1.

Imaginez un défi un peu bête : utilisez le compteur ci-dessous pour m'afficher tous les nombres qui existent entre 0 et 99999 :



Vous n'aurez pas d'autres choix que de passer par toutes les combinaisons pour réussir ce défi :



...



C'est exactement comme ça que fonctionne un ordinateur classique pour compter. Il doit traiter chaque information, chaque "nombre" dans notre exemple, une à une.

Un ordinateur quantique va raisonner autrement. Voilà comment un ordinateur quantique réagirait si je le mettais au défi :



Le principe, c'est celui de la superposition quantique qu'on a vu plus haut. Une case du compteur, autrement dit 1 bit, ne représente plus qu'une seule valeur comme on en a l'habitude, mais une superposition de plusieurs valeurs – 9 dans notre exemple.

Que cet exemple du compteur ne vous trompe pas : en informatique quantique, un ordinateur continue à travailler avec des 0 et des 1. L'ordinateur quantique ne superpose non pas 9 valeurs comme le fait le compteur ci-dessus, mais seulement 2 valeurs (0 et 1).

Ça reste un exploit. Concrètement, cela veut dire qu'un ordinateur quantique peut calculer beaucoup plus rapidement qu'un ordinateur classique, puisqu'il peut traiter tous ses états possibles en même temps (pour reprendre l'analogie du compteur : il a compté en 1 fois au lieu de compter 99999 fois).

Un ordinateur quantique à 4 qbits va calculer 16 fois plus rapidement qu'un ordinateur classique à 4 bits, et ainsi de suite. On double la puissance d'un ordinateur quantique à chaque fois qu'on lui ajoute un qbit ! Ce qui n'est pas le cas pour un ordinateur classique.



Pour montrer un exemple de mise en œuvre d'un algorithme quantique, nous pouvons utiliser l'outil qu'IBM met à disposition en ligne à l'adresse :



<https://quantumexperience.ng.bluemix.net/qx/experience>



## VII. Les possibilités



### Cryptographie :

Ainsi la cryptanalyse serait bien plus rapide que par un ordinateur classique, car augmentant de façon linéaire (en  $N$ ) avec la taille  $N$  de la clé, et non de façon exponentielle (en  $2^N$ , par exemple) comme avec des méthodes de force brute, séquentielles ou même massivement parallélisées. En effet, pour casser un chiffrement basé sur l'utilisation des nombres premiers, les ordinateurs actuels, même parallélisés, devront résoudre ce problème dans un temps de calcul qui augmentera exponentiellement avec la longueur de la clef. Ce caractère exponentiel disparaît totalement dès lors que l'on passera de la base binaire (système actuel avec les bits) à une base de taille quasi infinie grâce au qubit.

Les grandes capacités de factorisation permettraient ainsi à un calculateur quantique de casser de nombreux systèmes cryptographiques actuellement utilisés, en particulier la plupart des méthodes de chiffrement asymétriques. Ces algorithmes sont utilisés pour protéger des pages Web, des messages électroniques, et beaucoup d'autres types de données. Parvenir à casser ces protections serait un avantage majeur pour l'organisation ou le pays qui y parviendrait, et une réédition de l'exploit réalisé pour Enigma.

La seule façon de rendre sûr un algorithme est d'augmenter la taille de la clé en fonction de l'évolution des technologies qui permettent de casser des clés toujours de plus en plus longues, ralentissant en même temps le codage des messages sur les réseaux utilisateurs.



### Cryptographie quantique :

Si les transmissions quantiques se généralisaient dans l'avenir, elles pourraient assurer une confidentialité totale. On ne peut en effet pas réaliser une copie exacte de l'état intriqué d'un qubit cette règle est connue sous le nom de théorème de non-clonage. Si un nœud intermédiaire essaie de copier une requête quantique, il la perturbera nécessairement. L'émetteur de la requête pourra détecter l'existence éventuelle de cette perturbation. Cette question pose toutefois aussi celle de la faisabilité de répéteurs.



### Intelligence artificielle :

À l'heure actuelle, l'Intelligence Artificielle puise sa force dans les capacités de calcul des processeurs traditionnels. Plus les capacités de calcul sont élevées, plus le traitement d'information est efficace.

Les ordinateurs quantiques peuvent être utiles dans un cadre beaucoup plus large, allant de l'optimisation à l'intelligence artificielle et l'apprentissage automatique (machine Learning), cela veut dire que bientôt les machines seront assez puissantes pour apprendre par elles-mêmes à une vitesse que l'humain ne peut toujours pas anticiper, ce qui peut amener de grandes améliorations mais ce qui peut surtout faire peur, ce qui amènerait les films de science-fiction comme "Terminator" à de simples films d'anticipation.



#### Voiture autonome :

Les véhicules deviennent autonomes. L'environnement de la route est très instable car il est impossible de prévoir certains événements (la traversée d'un piéton par exemple). Le fait de réguler toute une flotte est donc impossible avec nos technologies actuelles car le temps que le système calcule les nouvelles actions à réaliser serait trop important.

Avec le principe de superpositions d'états, l'Intelligence Artificielle aura déjà prévu tous les cas possibles et n'aura plus qu'à choisir l'action à réaliser au moment voulu. Et avec la puissance de calcul infinie, l'Intelligence Artificielle serait capable de gérer de manière totalement autonome toute une flotte de véhicules dans une mégapole.



#### Simulation de physique quantique et de physique des particules :

Des circuits quantiques sont déjà utilisés pour des simulations de mécanique quantique et de physique des particules, fonction pour laquelle Richard Feynman les avait imaginés au départ. Ils y sont très utiles, car les calculs quantiques deviennent complexes dès qu'on sort de quelques cas triviaux.



#### Prévisions financières :

Les calculateurs quantiques sont envisagés pour étudier la nature stochastique des marchés financiers et construire de nouveaux modèles de prévisions. Ces nouveaux outils permettraient d'évaluer la distribution de résultats dans un très grand nombre de scénarios générés au hasard.

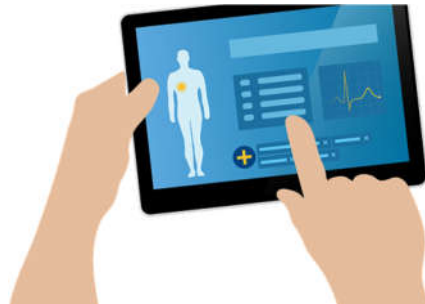


#### Prévisions météorologiques :

Prévoir le temps qu'il fera demain est aujourd'hui assez simple et totalement réalisable. Mais lorsque l'on essaye de prévoir le temps qu'il fera dans 10 jours, la tâche semble impossible. En effet, pouvoir prévoir comment vont évoluer les perturbations, les anticyclones etc. nécessite de prévoir tous les aléas et la puissance de calcul dont nous disposons (malgré le fait qu'elle

continue de doubler tous les deux ans) ne nous permet toujours pas d'anticiper tous ces phénomènes.

Maintenant, imaginez un système qui serait capable de calculer en continu toutes les modifications environnementales. Alors la prévision du climat sera d'une prévision infallible..



### Médecine :

Avec sa capacité de calcul extraordinaire, l'ordinateur quantique permet de résoudre des problèmes d'une très grande complexité. Notamment les problèmes d'optimisation. Dans le domaine de la santé, l'ordinateur quantique permettra ainsi de « rendre plus facile l'analyse de l'information génétique, ou de répertorier le patrimoine génétique des individus », Directeur des services aux professionnels de l'entreprise D-Wave

Si la composition chimique des protéines est plutôt connue, leur structure l'est moins en raison du nombre extrêmement élevé de possibilités. Une meilleure compréhension du repliement des protéines permettra donc de mieux comprendre la vie, d'élaborer de nouvelles thérapies et de nouveaux médicaments.

De la même manière que précédemment, un ordinateur quantique est capable en théorie de tester simultanément un grand nombre de possibilités de repliement, identifier les plus prometteuses et les tester beaucoup plus rapidement que n'importe quel ordinateur « normal ».

La radiothérapie utilise des logiciels sophistiqués pour établir le meilleur traitement possible. Le logiciel utilisé ne fonctionne pas de manière optimale car il existe trop de variables à prendre en compte. Et ni ces logiciels ni les ordinateurs ordinaires n'ont la capacité de tester toutes les solutions possibles.

C'est là qu'intervient l'ordinateur quantique. Il cherche le meilleur traitement possible avec un nombre très important de paramètres. Il permet donc d'atteindre un résultat plus précis, mais surtout, en théorie, beaucoup plus rapidement.

## VIII. Historique de l'ordinateur quantique jusqu'à aujourd'hui

**1970** : Richard Feynman commence à parler d'informatique quantique.

**1982** : L'hypothèse de réaliser un ordinateur quantique est soulevé pour la première fois par Richard Feynman. Son projet ne retient pas alors l'attention car il ne propose pas d'application concrète.

**1985** : David Deutsch d'Oxford démontra théoriquement qu'il était possible de réaliser une machine de Turing à l'aide des concepts de mécanique quantiques.

**1994** : Peter Shor développe un algorithme permettant la factorisation d'un nombre donné en temps polynomial (au lieu d'exponentiel). A partir de cette date, tout s'est accéléré, et de gros moyens financiers ont été débloqués afin de permettre à des équipes de chercheurs dans le monde entier de travailler sur la mise au point d'un ordinateur quantique.

**1996** : Lov Grover, de Bell Labs, publie un algorithme quantique de recherche d'un élément dans un ensemble de  $n$  objets.

**1998** : Premier ordinateur quantique à 2 qubits.

**1999** : Ordinateur quantique à 3 qubits.

**2000** : Ordinateur quantique à 5 qubits.

**2001** : Isaac Chuang et son équipe parviennent à factoriser le nombre 15 grâce à un ordinateur de 7 qubits.

---

Conscients de ce potentiel, les géants du numérique investissent le terrain. C'est le cas de Google, IBM, Intel ou Microsoft.

---

IBM travaille sur les ordinateurs quantiques depuis plus 35 ans.



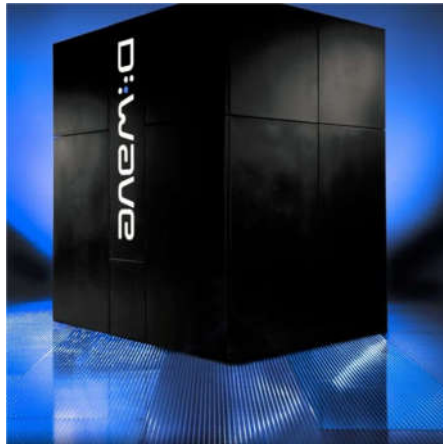
En mai 2016, IBM a dévoilé un ordinateur quantique à 5 qubits, accessible au grand public par internet.

En mars 2017, IBM a ouvert une division commerciale, IBM Q, pour développer et vendre du calcul quantique par le cloud.



En mai 2017, IBM a annoncé 2 nouveaux prototypes de processeur quantique, à 16 et 17 qubits. IBM espère à terme développer un processeur quantique à 50 qubits.

---



D-wave est une entreprise canadienne Pioneer en informatique quantique.

En 2017 Elle réalise un premier ordinateur quantique de démonstration à 16 qubits.

En 2011, elle vend un ordinateur quantique à 128 qubits, le d-wave one, pour 10 million dollar à Lockheed Martin.

En 2013, elle vend une machine à 512 qubits, le d-wave two, à un laboratoire d'intelligence artificielle quantique mis en place par la NASA, Google et des universités américaines.

En 2015, elle passe la barrière du millier de qubits avec son ordinateur quantique d-wave 2x.

En 2017, elle vend une machine à 2000 qubits, le d-wave 2000Q, à une entreprise de sécurité informatique, "temporal defense systems".

Les machines d-wave sont cependant critiquées car elle utilise un procédé appelé Quantum annealing qui est pour certains une impasse pour le calcul quantique. Cette technologie ne permet de résoudre que des problèmes d'optimisation.

---



Google est un client, mais aussi développeur sa propre technologie de calcul quantique. Cette technologie est un hybride entre celle d'IBM et celle de d-wave.

En juin 2017, Google a testé une machine à 20 qubits, basée sur sa propre technologie.

D'ici la fin 2017, Google espère tester une machine à 49 qubits

Dans quelques années les ordinateurs seront plus puissants que tout ordinateur classique pour réaliser certaines tâches.

Microsoft, Intel, Ali Baba et atos

Microsoft travaille sur les ordinateurs quantiques avec une initiative appelée "station Q", basée essentiellement sur une technologie appelée "topological quantum computing".

En décembre 2016, Intel a révélé qu'il travaille sur la réalisation de puces quantiques sur silicium.

En juillet 2016, Ali Baba, le géant du commerce en ligne chinois, s'est associé avec l'Académie des Sciences chinoises pour mettre sur pied un laboratoire de calcul quantique, le "Alibaba quantum computing laboratory".

En juillet 2017, Atos annonce son "Atos learning machine", un ordinateur classique capable de simuler 40 qubits. Il permet aux chercheurs et développeurs de travailler sur des algorithmes quantiques.

## IX. L'avenir de l'ordinateur quantique

Nous avons vu que l'accélération que l'on peut attendre d'un ordinateur quantique à  $n$  qubits est de  $2^n$ . Pour un ordinateur à 50 qubits, cela donne une accélération d'un facteur d'un million de milliards environ.

Avec une telle accélération, des problèmes qui étaient impossible à résoudre sont maintenant apportés. Cette limite de 50 qubits et s'appelle suprématie quantique, c'est la limite à partir de laquelle un ordinateur quantique devient plus puissant que tout ordinateur classique.

On comprend donc pourquoi les entreprises qui travaillent dans le domaine de l'informatique quantique se livrent une course effrénée pour atteindre cette limite.

### Les ordinateurs quantiques vont-ils remplacer nos ordinateurs classiques ?

Les ordinateurs quantiques sont d'une telle complexité qu'ils ne sont pas destinés au grand public. Ils seraient seulement utiles pour des applications très spécifiques, là où les ordinateurs classiques sont impuissants. Pour regarder un film ou aller sur internet, les bits classiques suffisent amplement ! Le rêve des chercheurs est de créer un ordinateur quantique universel, sur lequel on pourrait faire fonctionner n'importe quel algorithme.

La mise au point de machines est compliquée, sans même parler de langages, de systèmes d'exploitation. La dizaine d'ordinateurs quantiques actuellement existants sont encore expérimentaux. Chercheurs et constructeurs s'attellent à tester des particules quantiques (quantum) suffisamment stables dans le temps et ne nécessitant pas de fonctionner à des températures négatives extrêmes. Étonnamment, les ordinateurs quantiques opérationnels actuellement sont donc des ordinateurs classiques sur lesquels sont simulés des circuits quantiques, notamment en utilisant la puissance de calcul des GPU (Graphics Processing Unit) de cartes graphiques.

On aura de plus en plus besoin de traiter un nombre grandissant de variables, mais il est probable qu'informatique séquentielle et informatique quantique cohabiteront

## X. conclusion

L'avenir des ordinateurs quantiques semblent alors très promettant, quoi que encore incertain, étant donné les nombreuses contraintes que présente leur construction. La concurrence entre les grandes firmes informatiques pour mettre au point un algorithme de détection/correction des erreurs, et, plus important, une manière plus accessible de créer le qubit, continue d'embraser cette lueur d'espoir de voir un jour l'apparition d'un premier calculateur quantique, qui permettra des prouesses non seulement en informatique ou en cryptographie, mais aussi en recherche et simulation des effets quantiques.

---

### Sources :

<https://youtu.be/85XpYLWxg5k>

<https://youtu.be/mgflJso5bMg>

<https://youtu.be/lUeQ0nkQw4s>

<https://youtu.be/O15hYimr1a0>

<https://youtu.be/8qcn4edJuaq>

<https://www.institut-pandore.com/>

[https://fr.wikipedia.org/wiki/Calculateur\\_quantique](https://fr.wikipedia.org/wiki/Calculateur_quantique)

<https://www.teresacree.org/actualites/1643/actualite-ce-que-voit-l-intelligence-artificielle-revele-par-google-grace-a-ses-reseaux-neuronaux-quantiques-123298>

[https://www.rtf.be/info/medias/detail\\_informatique-quantique-ces-ordinateurs-qui-vont-changer-le-monde?id=9757472](https://www.rtf.be/info/medias/detail_informatique-quantique-ces-ordinateurs-qui-vont-changer-le-monde?id=9757472)

<https://iq.intel.fr/un-ordinateur-quantique-quest-ce-que-cest/>

<https://iatranshumanisme.com/2018/01/27/informatique-quantique-va-changer-monde/>

<http://dept-info.labri.fr/~ges/ENSEIGNEMENT/CALCULQ/ENSEIRB2012.pdf>

<http://automatesintelligent.blog.lemonde.fr/2007/03/05/un-ordinateur-quantique-commercialise-des-2008/>

...