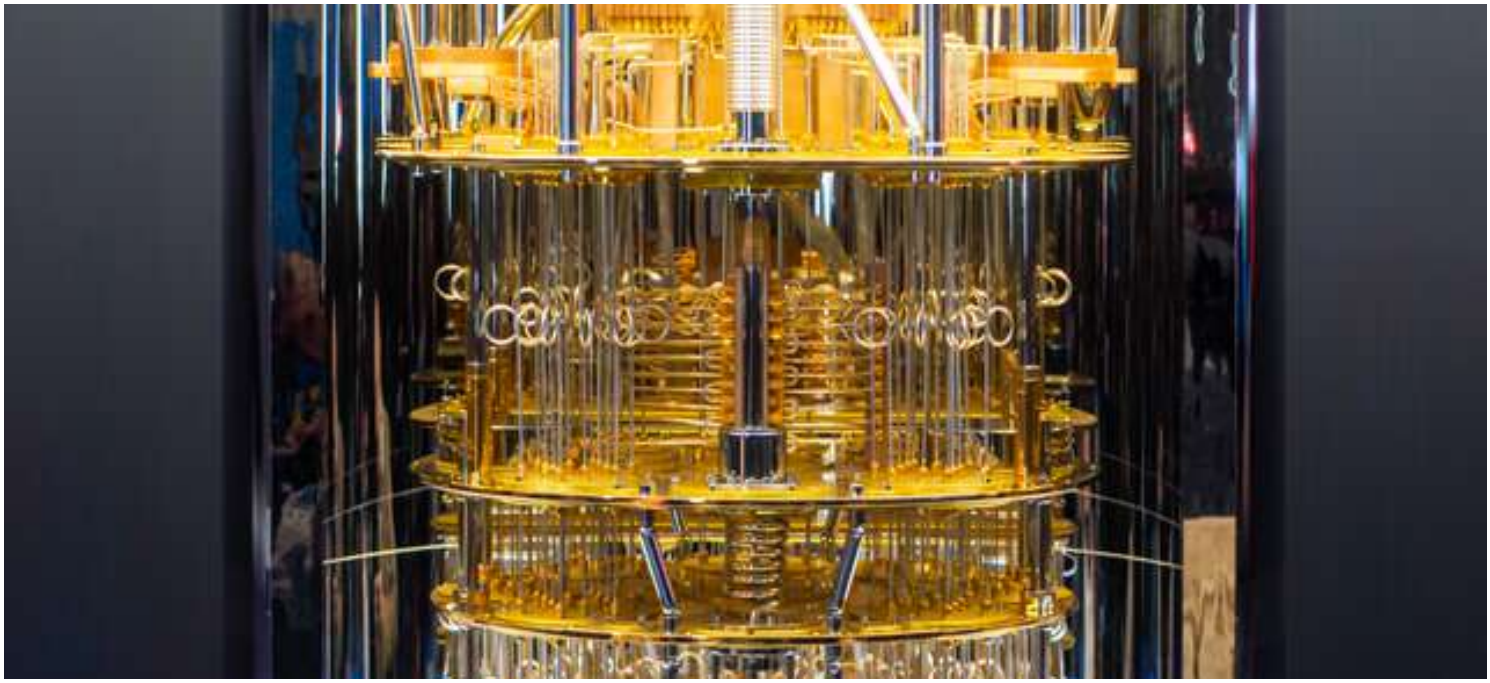


Qu'est-ce qui distingue l'informatique quantique de l'informatique classique ?

Une vidéo est présente à cet emplacement dans la version web de l'article publié sur Futura; elle a été retirée de ce document PDF pour des raisons techniques.

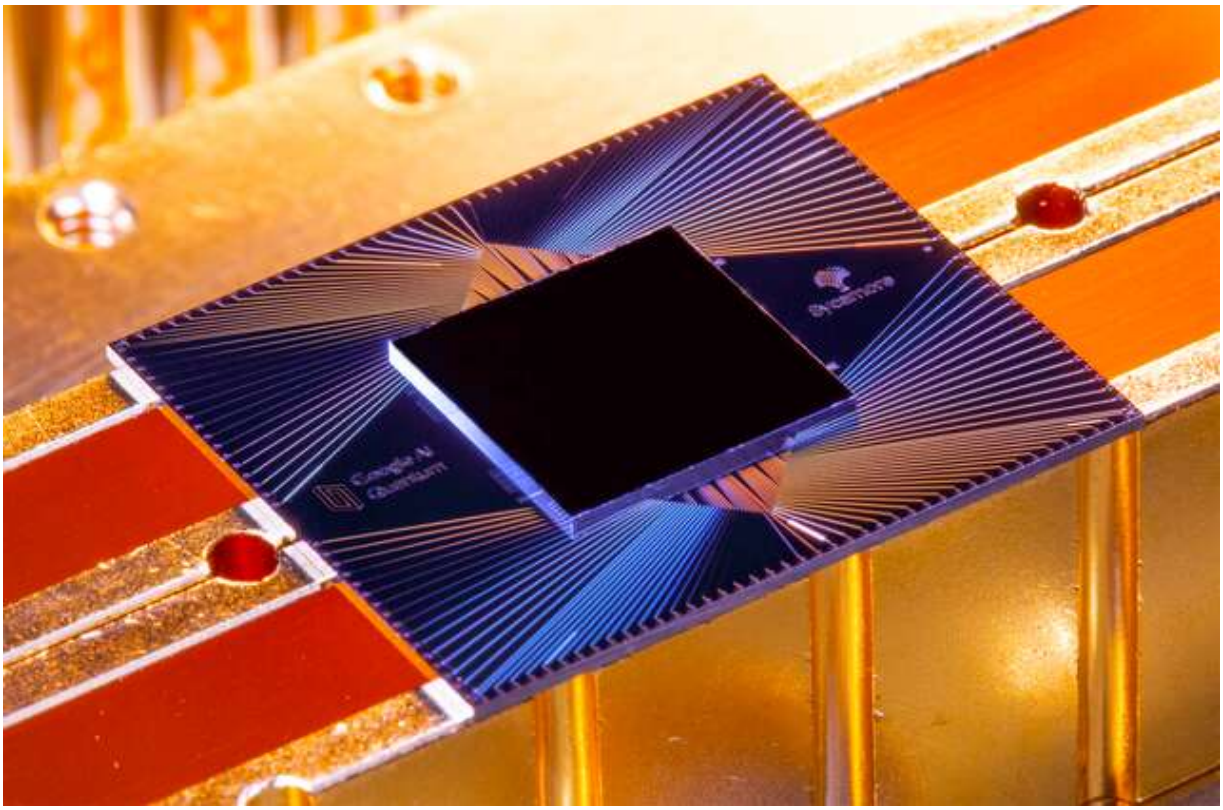
PAR DANIEL ICHBIAH
JOURNALISTE

LE 18 JANVIER 2023

Au royaume lilliputien des quanta, la matière adopte des propriétés qui dépassent notre entendement usuel. L'une d'elles mène à l'élaboration d'une informatique d'un nouveau genre, à même de surpasser les super ordinateurs actuels pour certains types de calculs. Pourtant, cela n'est pas si simple : les processeurs quantiques sont difficiles à mettre au point à grande échelle et ils nécessitent la conception d'algorithmes inédits...

En octobre 2019, **Google** a annoncé avoir atteint **la « suprématie quantique »**... Qu'est ce que cette « suprématie quantique » ? Une situation décrite en 2012 par John Preskill, un **physicien** américain du *California Institute of Technology* (Caltech). Preskill a posé qu'elle serait atteinte le jour où un ordinateur **quantique** saurait résoudre un problème bien plus rapidement qu'un ordinateur classique. Google a donc clamé avoir atteint cette situation avec son processeur Sycamore et donc avoir marqué une étape de l'histoire de l'informatique. Quand bien même, comme nous le verrons plus loin, **cette affirmation a été remise en question**, cet événement a contribué à mettre en **lumière** les potentiels de cette informatique d'un goût nouveau.

Qu'est-ce au juste que l'informatique quantique et en quoi diffère-t-elle du modèle habituel ?



LE PROCESSEUR QUANTIQUE SYCAMORE DE GOOGLE. GOOGLE A AFFIRMÉ AVOIR ATTEINT LA « SUPRÉMATIQUE QUANTIQUE » EN OCTOBRE 2019 – SOIT LE MOMENT OÙ UN ORDINATEUR CLASSIQUE SURPASSERAIT LE PLUS PUISSANT DES ORDINATEURS CLASSIQUES. CETTE AFFIRMATION A ÉTÉ CONTESTÉE DEPUIS. © ERIK LUCERO, GOOGLE QUANTUM HARDWARE

La révolution quantique

Le siècle dernier a été celui de l'électronique. En 1897, le premier dispositif électronique, le tube à vide a été inventé, puis il a été remplacé par le transistor inventé en 1947, lui-même reconverti peu à peu en **circuit intégré** -- en 1959. À partir de là, il n'a fallu que 13 ans pour que le

premier microprocesseur soit mis en vente. Toutes ces révolutions technologiques ont été permises par la **physique quantique** élaborée au début du XX^{e} siècle.

Or, le XX^{e} siècle a vu advenir une seconde révolution quantique, qui exploite de nouvelles propriétés notamment la capacité à contrôler individuellement des **atomes**, des **électrons** et des **photons**. Ces nouvelles capacités sont en mesure de révolutionner la technologie des **ordinateurs**.

Les étranges propriétés des quanta

La découverte des propriétés des quanta a stupéfait plus d'un Homme de science car, à cette échelle, un atome se comporte tantôt comme une particule, tantôt comme une onde. Il en résulte des comportements totalement étrangers à notre façon de concevoir la **matière**.

La première est la superposition d'états. Par la nature même des quanta, un bit quantique ou **qubit**, dans la mesure où il peut se comporter comme une onde, peut superposer plusieurs valeurs. Cela semble dépasser notre entendement commun et pourtant telle est la réalité.

Une autre propriété stupéfiante est « l'**intrication quantique** », un phénomène par lequel une particule dispose d'une sorte de jumelle. Elles forment un tout indivisible, même à distance. Cette propriété est combinée à la superposition des états pour accélérer les calculs en permettant une nouvelle forme de parallélisation, mais aussi le développement de **capteurs** aux performances jamais égalées.

Des bits et des qubits

Un ordinateur classique tel que nous le connaissons travaille sur des informations **binaires**, soit des 0 et des 1. L'unité de calcul, le bit peut être égal à 0 ou bien à 1, un peu comme une ampoule peut être allumée ou éteinte.

Or, grâce au phénomène de superposition, le qubit peut embrasser plusieurs valeurs simultanément ! Ainsi, donc, il peut être :

- égal à 0 ;
- dans le même temps, égal à 1 ;
- pour chacune de ces deux valeurs, nous avons une probabilité d'occurrence. Par exemple : 78 % pour le 0 et 22 % pour le 1. Ou bien 34 % pour le 0 et 66 % pour le 1. Si la probabilité est de 100 % pour le 0 ou pour le 1, on parle d'« état propre ».

Prenons l'exemple d'un **nombre binaire** de 3 bits. En informatique habituelle, nous avons 8 combinaisons possibles (2^3) :

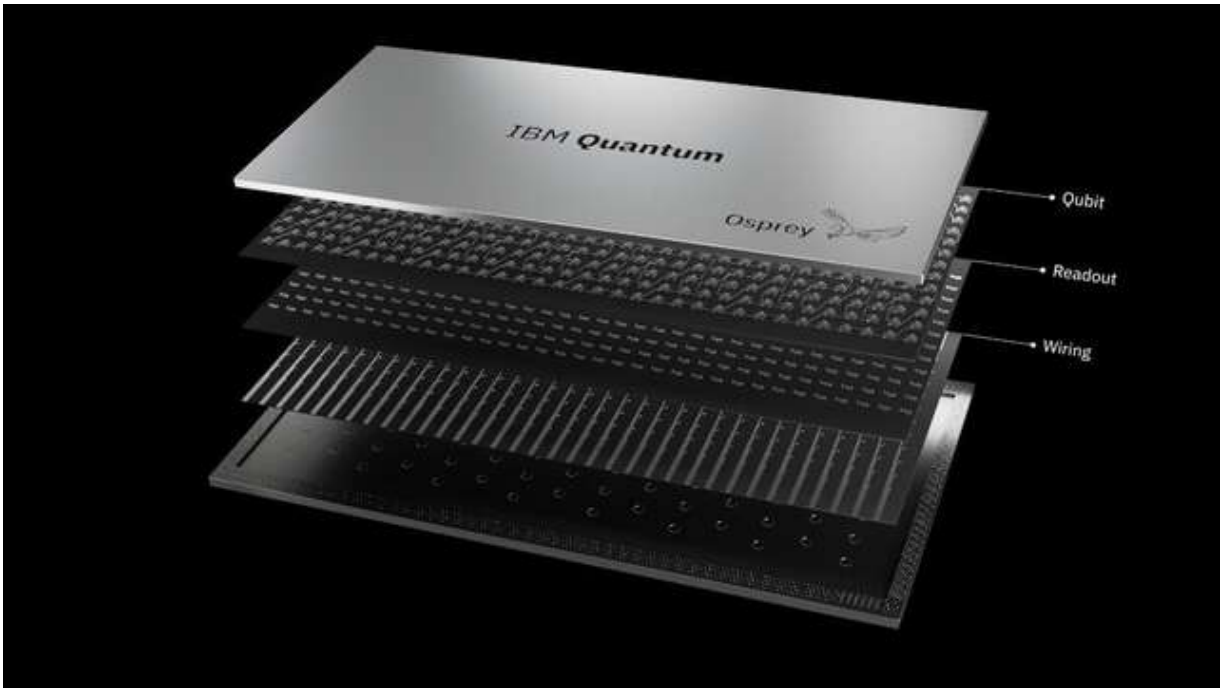
000	001	010	011
100	101	110	111

Avec 3 qubits d'un processeur quantique, nous avons ces 8 états en parallèle. Et donc, l'**ordinateur quantique** pourrait théoriquement calculer 2^3 fois plus vite qu'un ordinateur classique -- soit huit fois.

De fait, la puissance de calcul d'un ordinateur quantique est à même de doubler chaque fois que l'on ajoute un qubit alors que dans les ordinateurs classiques, la puissance est proportionnelle au nombre de circuits intégrés placés dans les processeurs.

Il en résulte que les processeurs quantiques ont le potentiel de résoudre certains problèmes plusieurs millions de fois plus rapidement que les **supercalculateurs** d'aujourd'hui Et de rendre possibles des calculs impossibles en pratique sur les supercalculateurs. Comme obtenir en quelques jours un résultat qui prendrait mille ans de calcul normalement.

Est-ce à dire qu'ils vont remplacer tous les ordinateurs actuels ? Eh bien non, ce n'est pas si simple...



LE PROCESSEUR OSPREY D'IBM EST SUPPOSÉ POUVOIR ALIGNER PAS MOINS DE 400 QBITS EN PARALLÈLE ET DEVRAIT SERVIR À LA CONSTRUCTION D'UN SUPER ORDINATEUR QUANTIQUE. © IBM

Qui bâtit des ordinateurs quantiques ?

En 2011, la société canadienne **D-Wave a fait sensation** en lançant le premier ordinateur quantique commercialisé (le D-Wave One à l'époque) exploitant des qubits **supraconducteurs**. Pour mémoire, la **supraconductivité** désigne la propriété d'un **matériau** qui, refroidi à très basse température acquiert la capacité de conduire un **courant électrique**, sans **résistance**, et sans perte d'**énergie**. Depuis, des sociétés telles que **IBM**, et Google ont également monté des structures exploitant des qubits supraconducteurs et donc des circuits électroniques dont le courant électrique joue le rôle d'un quanta unique. On appelle cela des atomes artificiels. Bien d'autres entreprises sont impliquées dans cette course à la performance et nous les citons plus loin.

De son côté, l'Union européenne a investi 1 milliard d'euro dans le cadre du Quantum Flagship, qui implique 5 000 chercheurs et devrait aboutir en une dizaine d'années à la création de plusieurs ordinateurs quantiques européens.

Ce programme a été complété par des programmes encore plus ambitieux à travers l'**entreprise commune EuroHPC** qui vise à équiper les centres de calculs européens par des

accélérateurs quantiques issus de l'initiative **EuroQCI**. Celle-ci vise à prototyper et déployer une infrastructure pan-européenne de communications quantiques.

Ces deux programmes portent l'investissement européen dans le quantique à l'horizon 2027 à plus de 4 milliards d'euros.

L'UNION EUROPÉENNE A LANCÉ LE PROJET QUANTUM FLAGSHIP POUR FINANCER LA RECHERCHE ET LA CRÉATION DE PLUSIEURS ORDINATEURS QUANTIQUES DE TYPES DIFFÉRENTS. UN MILLIARD D'EUROS A ÉTÉ AFFECTÉ À CE PROJET VISANT À POSITIONNER NOTRE CONTINENT DANS LA COMPÉTITION SUR LES TECHNOLOGIES QUANTIQUES. © QUANTUM FLAGSHIP

L'approche de D-Wave

Une fois qu'un problème a été élaboré dans le système, les ordinateurs quantiques de D-Wave ne peuvent déterminer une réponse qu'en abaissant le système à son état d'énergie (température) le plus bas.

Le passage vers cet état de plus basse énergie, ou « **état fondamental** », est la clé de l'opération. De fait, la raison pour laquelle un tel ordinateur est parfois appelé un optimiseur quantique est qu'il descend à cet état d'énergie fondamental « adiabatiquement » (sans rejet ni apport calorifique au sein du système). Ainsi, un ordinateur tel que ceux proposés par D-Wave opère en refroidissant ses circuits jusqu'à 20 millikelvin (soit - 272,98 °C, près du **zéro absolu**) grâce au matériau supraconducteur. Il crée alors un passage direct depuis l'état initial du système programmé (le problème) jusqu'à l'état fondamental du système (la réponse) de façon fulgurante, en tenant compte simultanément de toute une gamme de permutations différentes.

Notons que IBM et Google ont adopté d'autres approches des qubits supraconducteurs -- on parle d'ordinateurs quantiques « programmables ».

La tunellisation

En essence, un ordinateur quantique tels que ceux de D-Wave obtient les réponses aux questions par « tunnellisation » à travers un paysage énergétique jusqu'à l'état d'énergie le plus bas possible. C'est comme si vous lanciez une balle de golf directement dans un trou.

L'état du système initial est la balle de golf sur un tee, le paysage énergique les collines et les vallées du cours, et le trou l'état fondamental. Pour atteindre le trou (la réponse) avec un ordinateur classique, le système déplace la balle par-dessus les obstacles jusque dans le trou.

Avec un ordinateur quantique tel que le D-Wave Advantage, nous pourrions dire que la balle perfore un tunnel à travers les collines et dépressions pour aller directement dans le trou !

PIONNIÈRE DE L'INFORMATIQUE QUANTIQUE, LA SOCIÉTÉ D-WAVE A PRÉSENTÉ LE MODÈLE ADVANTAGE EN MAI 2022. EQUIPÉS DE 5 000 QBITS, CES SYSTÈMES RÉSIDENT À BURNABY AU CANADA, À JULICH EN ALLEMAGNE, ET MARINA DEL REY EN CALIFORNIE. IL EST POSSIBLE D'EN EXPLOITER LES POTENTIELS *VIA* UN SERVICE CLOUD D'AMAZON : AWS MARKETPLACE. © D-WAVE

Qubits photons et à base de cavité dans les diamants

La Chine a annoncé dès 2020 avoir pu exploiter une technologie plus efficace que la supraconductivité : **son ordinateur Jiuzhang 2** repose sur des qubits photons. Une même approche est adoptée par la Californienne PsiQuantum, **la Canadienne Xanadu** mais aussi la Française **Quandela**.

De leur côté, deux **starts-up** allemandes, SaxonQ et XeedQ, entendent exploiter les qubits à base de cavités dans les **diamants** et prétendent qu'elles pourraient y arriver à des températures bien moins extrêmes.

La start-up grenobloise Siquance ou l'Australienne Diraq ont pour approche d'exploiter le « **spin** » (charge électrique) dans le **silicium** avec pour avantage de reprendre le design classique des transistors utilisés dans l'informatique (ou CMOS) et donc de potentiellement s'appuyer sur des décennies de développement dans la microélectronique pour atteindre des millions de qubits.

Par ailleurs, des recherches sur les « **ions** piégés » et « atomes froids » auraient montré de meilleures performances que les approches suivies par IBM et Google
Il reste que les ordinateurs quantiques sont extrêmement difficiles à construire et qu'ils doivent souvent opérer dans des conditions complexes à obtenir et à maintenir.

Les ordinateurs classiques sont loin d'avoir dit leur dernier mot

Quand bien même les ordinateurs quantiques peuvent résoudre certains types de problèmes spécifiques avec une **vitesse** incroyablement supérieure à celle des ordinateurs classiques, que la chose soit bien claire : ils ne sont pas appelés à remplacer les ordinateurs classiques et coexisteront avec ces derniers.

Oui... Il est peu envisageable que l'on puisse demain acheter des ordinateurs quantiques dans une boutique comme on peut le faire aujourd'hui pour un **Mac** ou un PC. En premier lieu, ces ordinateurs d'un nouveau genre ne peuvent souvent opérer que dans des conditions extrêmement difficiles à obtenir et à maintenir. Il se trouve aussi que les ordinateurs quantiques ne sont pas des machines de calcul universelles. Ils ne savent pas résoudre tous les problèmes. Ils ne savent en résoudre qu'une liste très limitée, mais savent le faire de manière très efficace.

De la nécessité de corriger les erreurs

En pratique, les ordinateurs quantiques sont encore loin de livrer leurs promesses, celle d'un calcul dont la puissance augmente exponentiellement avec le nombre de qubits. La principale raison est que le taux d'erreur de ces qubits est très élevé.

À un tel niveau de miniaturisation, certaines particules sont susceptibles de se comporter de façon erronée. Eh oui ! Les qubits sont instables et dès lors que l'un d'eux est perturbé, il en résulte une erreur de calcul...

Le taux d'erreur est actuellement couramment supérieur de plus de 1 % par opération de calcul, beaucoup plus important que dans les bits classiques. Ces erreurs s'accumulant après chaque opération, les calculs deviennent rapidement faux et les résultats inexploitables.

Dans la pratique, on va demander à un ordinateur quantique de résoudre un même problème plusieurs fois. Chaque fois, nous aurons une réponse différente avec une probabilité, et celle qui a la probabilité la plus élevée sera jugée comme la meilleure réponse.

Par ailleurs, pour contourner le problème, il existe deux solutions.

- La première consiste à créer des qubits qui génèrent moins d'erreurs. Il y a là un défi de **physique quantique**, et d'informatique théorique qui occupe des milliers de physiciens et de **mathématiciens** dans le monde. Les travaux les plus prometteurs, tels ceux de Mazyar Mirrahimi et Zaki Leghtas sont issus de la rencontre d'un mathématicien et d'un physicien.
- La seconde consiste à créer des codes de correction d'erreurs qui permettent de transformer quelques qubits « moyens » en un qubit « meilleur », d'une qualité suffisante pour réaliser les calculs. Dans ce cas, le facteur de redondance est très élevé. Dans les estimations actuelles, il faudrait assembler entre 1 000 et 10 000 qubits « physiques » pour créer un qubit logique « corrigé ». Or, pour obtenir un début d'avantage quantique par rapport à un ordinateur classique, il faut disposer d'environ 100 qubits logiques. C'est pourquoi de nombreux fournisseurs tels que PsiQuantum aux USA ont dans leur roadmap un ordinateur quantique à 1 million de qubits physiques.

Ces qubits physiques devraient être bien plus fiables que les meilleurs qubits physiques actuellement disponibles. Toutefois, cela engendre des problèmes énormes de passage à l'échelle qui risquent d'occuper les physiciens et les ingénieurs sur quelques décennies.

De nouveaux types d'algorithmes

Il se trouve aussi que les ordinateurs quantiques nécessitent -- tout comme pour les ordinateurs classiques -- que l'on développe des algorithmes spécifiques à leur approche.

Ainsi, l'algorithme développé par Peter Shor de Bell Labs en 1994 est à même de factoriser un nombre, soit de trouver les **nombres premiers** qui, multipliés entre eux, aboutissent à un nombre particulier. Par exemple :

$70 = 2 \times 5 \times 7$

Si cet exemple est simple, lorsqu'on aborde des nombres très grands, un tel calcul devient extrêmement ardu et long pour les ordinateurs actuels. C'est d'ailleurs sur ce principe que reposent les systèmes de **cryptologie** actuels -- ceux utilisés par votre banque ou bien pour valider les transactions en **bitcoin**. En pratique, la factorisation d'une clé **RSA** 2 048 bits qui protège nos transactions **Internet** actuelles nécessiterait un ordinateur quantique disposant de 20 millions de qubits environ 10 à 100 fois meilleurs que les meilleurs qubits actuels. Donc nous avons encore de la marge.

L'algorithme de Grover, pour sa part, aide à analyser des tableaux de n enregistrements et peut trouver une information en √n étapes. Par exemple, si une base comporte un million d'enregistrements, il va trouver l'information requise en 1 000 étapes, là où un ordinateur classique prendrait bien plus de temps puisqu'il analyserait chacun des enregistrements, ce qui correspondrait potentiellement à un million d'étapes.

LES PROCESSEURS D-WAVE 2000Q RÉALISÉS PAR LA SOCIÉTÉ D-WAVE POUR L'ORDINATEUR QUANTIQUE LANCÉ EN 2017. COÛT : 15 MILLIONS DE DOLLARS. © D-WAVE

Google a-t-il réellement atteint la suprématie quantique ?

Nous l'avons vu plus haut, **Google** a clamé, en octobre 2019, avoir atteint la « suprématie quantique » avec son processeur Sycamore, qui a effectué un calcul avec 53 qubits. Il a fallu 200 secondes à Google pour effectuer 1 million de mesures. Google a alors affirmé que le super ordinateur Summit d'IBM aurait mis 10 000 ans à accomplir la même prouesse. Peu après, IBM a publié un article pour affirmer qu'en réalité, sous certaines conditions, Summit ne prendrait pas 10 000 ans mais 3 jours pour aboutir au même résultat. Depuis, des chercheurs français ont baissé la note à 8 heures sur un simple cluster de serveur occupant un demi-rack. Et depuis 2019, diverses équipes de chercheurs ont réussi à reproduire la performance sur des calculateurs classiques. Comme le problème résolu par Google était théorique, sans utilité particulière, Sycamore n'a pas réellement dépassé les capacités des ordinateurs classiques pour la **résolution** de problèmes concrets.

La suprématie quantique reste donc un Graal qui, au début de l'année 2023, n'est pas encore été atteint.