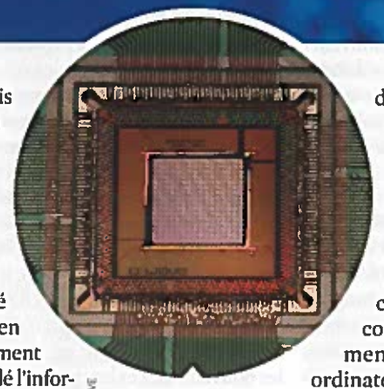
Les promesses de l'ordinateur quantique

La société D-Wave affirme avoir conçu une machine à la puissance de calcul inégalable. L'exploit a-t-il vraiment eu lieu ? De nombreux spécialistes en doutent. Mais le coup d'accélérateur donné à la recherche est si fort que l'arrivée de l'ordinateur quantique paraît imminente. Enquête au Canada.

Par Azar Khalatbari



D-WAVE

Les processeurs quantiques (ici celui de D-Wave) devraient effectuer en 10 minutes des calculs que les ordinateurs classiques réaliseraient en cinq fois l'âge de l'Univers (2^{300} secondes).

LA SOCIÉTÉ CANADIENNE D-WAVE SYSTEMS, située à Burnaby, près de Vancouver, détient l'un des secrets les mieux gardés du moment. Elle affirme avoir réussi à fabriquer l'ordinateur dont rêvent tous les informaticiens, capables de résoudre des problèmes jusque-là hors de portée. Pour 15 millions de dollars, elle propose ainsi à la vente depuis plusieurs mois une volumineuse... boîte noire ! De nouvelles versions ont même fait leur apparition au cœur de l'été : après les modèles à 84, 128 puis 512 qubits *(lire le lexique)*, la société a annoncé en juin l'arrivée du 1000 qubits ! Une performance considérée jusqu'alors comme quasi inatteignable : un ordinateur classique formé par tous les atomes de l'Univers n'atteindrait pas la puissance de 300 qubits. Séduits, de nombreux clients se sont d'ores et déjà empressés d'acquérir l'une ou l'autre des versions. Le groupe d'armement américain Lockheed Martin a ainsi été l'un des premiers en 2011, puis ce fut le tour de la Nasa et de Google qui ont craqué en 2013 pour la D-Wave II (512 qubits), suivis du géant de la vente en ligne Amazon. La NSA, l'Agence nationale de la sécurité américaine, n'a pas été en reste. Elle possède également la sienne, comme l'a révélé l'informaticien Edward Snowden.

Pour comprendre l'intérêt d'une telle machine, il faut remonter aux géniales intuitions du physicien américain Richard Feynman qui, en 1982, eut l'idée d'utiliser les propriétés quantiques de la matière pour simuler les objets physiques de la manière la plus efficace possible. Rappellons qu'à l'état subatomique, la matière a des propriétés déroutantes : il y a d'abord l'état d'« intrication » *(lire le lexique)* où deux particules, pour peu qu'elles aient interagi dans le passé, se trouvent corrélées au point de ne former qu'un seul objet, même si elles sont distantes de plusieurs millions de kilomètres. Puis la « superposition », où une particule peut être dans deux états à la fois (zéro et un, excité et au repos, haut et bas...). Ainsi sont les qubits, capables de prendre deux configurations simultanément, là où les bits de nos ordinateurs classiques ne peuvent prendre qu'une valeur *(voir schéma)*. Et cette étrange possibilité leur confère une incroyable rapidité : *« Avec des bits classiques, on ne peut faire qu'un calcul à la fois, c'est très différent avec les qubits. Avec 300 qubits, on peut faire 2^{300} calculs en même temps ! »*, précise Alexandre Blais, de l'université de Sherbrooke (Canada). Soit un nombre gigantesque à 91 chiffres ! Ce qui revient à dire que pour le même calcul complexe, là où un ordinateur classique mettrait 2^{300} secondes — un temps égal à plus de cinq fois l'âge de l'Univers — son cousin quantique y passerait 600 secondes soit 10 minutes. Époustouflant ! Que pourrait-on résoudre grâce à de telles performances ? L'exemple souvent annoncé est celui de la « factorisation », indispensable à la cryptographie, mais l'ordinateur quantique serait également très précieux pour une autre classe de problèmes allant de la recherche d'un abonné à partir de son numéro de téléphone (annuaire inversé) à l'optimisation instantanée d'un ensemble de satellites face à une éruption solaire, la gestion des données pour faire circuler des voitures autonomes ou le pilotage de l'électronique de bord d'un avion de chasse devant optimiser ses frappes en situation de combat... La liste est longue, sans oublier la gestion d'un réseau complexe d'autobus dans une mégalopole.

« Il s'agit à chaque fois de trouver la configuration pour laquelle l'énergie à dépenser est minimale », explique David Poulin, membre de l'Institut transdisciplinaire d'information quantique (Intriq) québécois. Ainsi, de très nombreux paramètres entrent en jeu pour gérer les 64 lignes de bus circulant à Paris : les embouteillages, la fréquence de chaque ligne, le nombre de passagers à embarquer ou débarquer, l'emploi du temps de chaque conducteur, etc. L'optimisation de ce problème à un grand nombre de variables reviendrait ainsi à minimiser le coût de l'exploitation. ▶

JUSUN / GETTY IMAGES

QUBIT État quantique qui correspond à la plus petite unité de stockage de l'information. Les ordinateurs actuels — qui n'exploitent pas les propriétés quantiques de la matière — se contentent de bits, et codent les informations en série de 0 et 1.

INTRICATION Caractère de deux particules qui forment à jamais un seul système car dans le passé, elles ont interagi. De ce fait, il suffit de mesurer les caractéristiques de l'une pour en déduire celles de l'autre.

SUPERPOSITION QUANTIQUE Dans le monde subatomique, les particules peuvent être à la fois dans deux états quantiques différents : « excité » et « au repos », noir et blanc, un et zéro.

CODAGE DE L'INFORMATION

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).

INTRICATION

Du quantique à l'échelle macroscopique

Dans un monde où domineront les qubits, il faudra maîtriser dans nos appareils macroscopiques tous les aspects de l'information quantique qui se manifestent habituellement uniquement à l'échelle subatomique. C'est pourquoi Bertrand Reulet, qui dirige l'Institut transdisciplinaire d'information quantique (Intriq) au Canada, traque le moindre soupçon de comportement quantique au cœur même de la matière macroscopique. Avec ses collaborateurs, il est ainsi parvenu à mettre en évidence pour la première fois une intrication entre deux photons au sein d'une « jonction tunnel », un mauvais contact entre deux métaux ordinaires, refroidie à une dizaine de millikelvins (-273 °C environ). « *Preuve qu'il nous reste encore beaucoup à comprendre sur les lois de la physique quantique* », rappelle-t-il. En attendant que ce dispositif puisse un jour transmettre des qubits, il peut déjà servir à produire des nombres parfaitement aléatoires, indispensables pour le codage et très difficile à obtenir. La trouvaille fait d'ores et déjà l'objet d'un brevet.

La question hante donc tous les esprits : D-Wave a-t-elle réellement réussi l'exploit de créer l'ordinateur capable de telles performances ? Pour l'heure, « *la plupart des spécialistes doutent* », tempère Alexandre Blais, qui mène aujourd'hui ses recherches à l'Intriq.


D-WAVE / LARRY GOLDSTEIN

Les ordinateurs dit quantiques commercialisés par la société D-Wave nécessitent une température de -273 °C pour fonctionner.

Des tests indépendants pourraient lever le doute

Un doute partagé par son collègue David Poulin qui, comme l'ensemble des experts mondiaux, souhaiterait que des tests indépendants puissent être effectués. Mais D-Wave a toujours refusé de divulguer les détails de ses calculs. « *Un test a bien été entrepris par le physicien Matthias Troyer, de l'École polytechnique fédérale de Zurich (Suisse) pour comparer le temps de calcul entre un ordinateur classique et celui de D-Wave. Il n'a détecté aucune accélération quantique ! Mais les responsables de l'entreprise ont rétorqué que le type de problème avait été mal choisi* », raconte David Poulin. Quoi qu'il en soit, réellement quantique ou non, l'ordinateur de D-Wave a d'ores et déjà réussi une autre performance : donner la fièvre aux spécialistes, les lançant dans une course effrénée aux enjeux commerciaux considérables. « *Nous préférons désormais déposer des brevets plutôt que publier des articles comme c'est de règle dans le domaine académique* », affirme ainsi Michel Pioro-Ladrière, qui développe des processeurs quantiques au sein d'Intriq. « *Dans les congrès de spécialistes, il y a beaucoup d'entrepreneurs,* confirme David Poulin. *Rien qu'au Canada, Mike Lazaridis l'ex-patron de Blackberry a mis 500 millions de dollars de sa poche pour les recherches dans ce domaine.* »

Le Canada est en effet en très bonne position dans cette course, talonnée par les États-Unis et la Chine, loin devant la France. Le pays affiche la volonté politique de relever le défi avec, entre autres, Intriq et IQC (Institute for Quantum Computing) à Waterloo, dans la province de l'Ontario. Si IQC a bénéficié des largesses de Mike Lazaridis, la recherche académique n'est pas en reste : fin juillet le gouvernement fédéral a investi 33,5 millions de dollars dans les travaux menés à l'université de Sherbrooke. Car bien des obstacles sont à franchir pour mettre au point un ordinateur dont les propriétés seraient indiscutablement quantiques.

Toute la difficulté consiste en effet, non seulement à obtenir un qubit, mais à maintenir son caractère quantique le plus longtemps possible. En théorie, la recette est simple : il faut trouver un support macroscopique — c'est-à-dire manipulable — qui obéisse aux lois de la mécanique quantique qui ne s'applique habituellement qu'à l'infiniment petit, le monde subatomique *(lire l'encadré ci-contre)*. Sans quoi, impossible de garantir le principe de superposition, la spécificité du qubit ! Dans le jargon, c'est la « décohérence », entraînée par exemple par la moindre augmentation de température.

Aluminium et silicium pour accélérer la conductivité

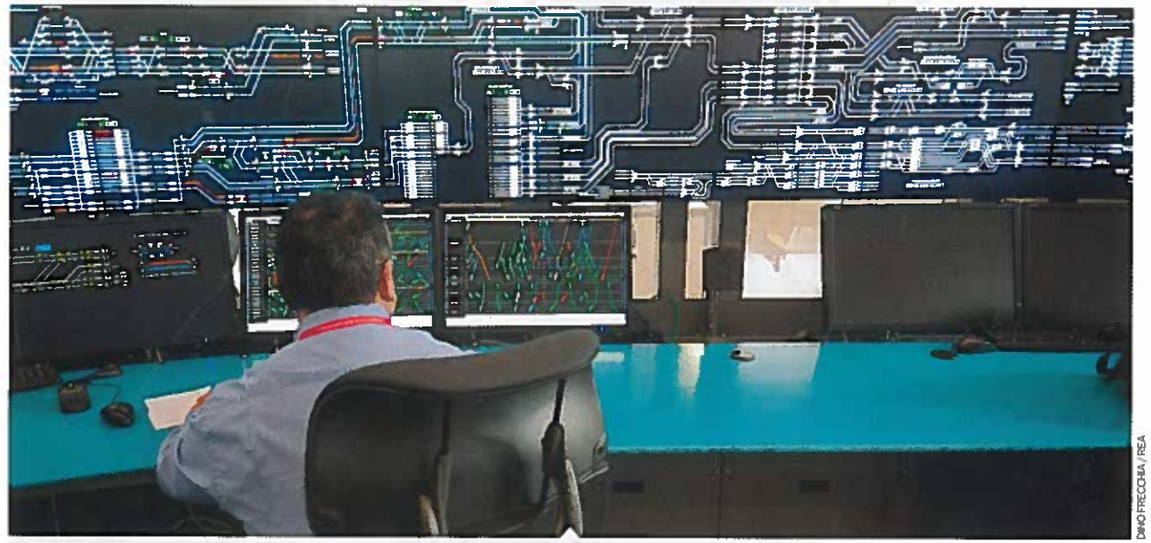
C'est pourquoi le calculateur de D-Wave se présente avant tout comme un réfrigérateur fonctionnant à quelques millikelvins (-273 °C environ). « *Le but est d'obtenir un temps de cohérence — c'est-à-dire le temps où cet état de superposition est maintenu — plus important que le temps de calcul* », rappelle Michel Pioro-Ladrière. Or, à cette température, tous les matériaux ne se valent pas. L'équipe canadienne poursuit donc deux pistes : l'aluminium et le silicium. « *L'aluminium que nous utilisons est extrêmement pur. Il est déposé sur un substrat en saphir, le tout étant refroidi à quelques millikelvins*», explique Alexandre Blais. Or, à ces températures, l'aluminium devient supraconducteur, c'est-à-dire qu'il n'oppose aucune résistance au passage du courant, un comportement que seule la mécanique quantique peut expliquer. « *Alors l'objet lui-même se comporte comme un seul atome que nous appelons "transmon" dans lequel circulent des paires d'électrons qui adoptent un comportement quantique* », poursuit le chercheur.

POUR EN SAVOIR PLUS

À regarder pour comprendre :
▸ **sciav.fr/826quantique**

APPLICATIONS

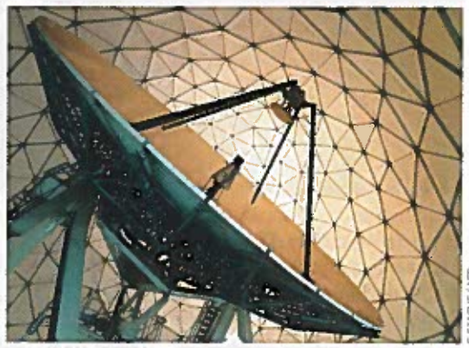
Réseaux, essaims, « big data » : gérer des systèmes complexes


DENIS FRECCHIA / REA

L'optimisation du réseau de transports en commun dans une mégalopole (ici, le centre opérationnel du Transilien à Paris) doit prendre en compte de nombreuses variables (trafic, montée et descente des passagers...) et nécessite une très grande capacité de calcul.


MIKE BLAKE / REUTERS

L'évolution d'un essaim de drones, qui exige de coordonner en permanence le mouvement de tous ses éléments, implique de disposer d'une informatique puissante.


C. STACHE / AFP

L'exploitation des « big data », comme celles produites par l'interception des télécommunications (ici, une antenne de la NSA, l'agence de renseignement américaine), réclame des ordinateurs toujours plus performants.

Pour l'heure, l'aluminium frôle un temps de cohérence d'une milliseconde, mais au vu des sommes investies dans le secteur, les chercheurs espèrent bien l'allonger. Michel Pioro-Ladrière a opté, lui, pour le silicium (Si). « *C'est un matériau largement utilisé dans les transistors. Une fois notre processeur quantique mis au point, les étapes de la fabrication iront très vite* », assure-t-il. Pour ce faire, il exploite le spin des électrons, le petit aimant doté de propriété quantique qui existe dans chaque électron. Or le spin des électrons se comporte dans le silicium tout comme si lesdits électrons se trouvent dans le vide.

Là, le temps de cohérence excède la dizaine de millisecondes tandis qu'une opération peut en principe ne durer qu'une nanoseconde, soit 10 000 000 de fois moins. Il reste donc encore à rassembler un grand nombre de qubits... Car là où D-Wave annonce un millier, les différents laboratoires de recherche à travers le monde n'affichent toujours qu'un score de 14 qubits.

De l'avis de tous les experts, une chose est sûre : cette accélération de la recherche a pour conséquence... de rendre l'invention du vrai ordinateur quantique imminente. Pour preuve ? Des sociétés spécialisées concoctent déjà des algorithmes adaptés à la machine tant attendue. « *Il existe déjà une bibliothèque baptisée "quantum zoo" qui propose une cinquantaine d'algorithmes* quantiques* », explique David Poulin, qui y contribue. ■

* http://math.nist.gov/quantum/zoo/