Opinions Libres
le blog d'Olivier Ezratty

# Comprendre l'informatique quantique – panorama des acteurs

Maintenant que nous avons fait le tour des **principes généraux d'un ordinateur quantique universel** puis de leurs **algorithmes et applications**, nous voici à l'étape d'un panorama des acteurs que sont les constructeurs d'ordinateurs quantiques. Ils sont principalement Américains ou Canadiens. Cependant, pour quasiment toutes les technologies d'ordinateurs quantiques, divers laboratoires de recherche veillent au grain pour faire avancer l'état de l'art sans qu'il soit encore récupéré par une entreprise privée. Je les évoquerai lorsque cela sera nécessaire.

**Les paramètres clés d'un ordinateur quantique**

La partie descriptive du **fonctionnement d'un ordinateur quantique** s'appuyait sur sa déclinaison la plus courante et celle qui a probablement le plus bel avenir : l'ordinateur quantique universel doté de portes quantiques construites autour de registres de qubits. Mais ce n'est pas la seule architecture d'ordinateur quantique.

Avant de décrire les différents types d'ordinateurs quantiques, faisons un détour par la définition des paramètres clés de performance d'un ordinateur quantique définis en 2000 par **David DiVicenzo**, alors chercheur chez IBM et maintenant à l'Université d'Aix la Chapelle en Allemagne, dans **The Physical Implementation of Quantum Computation**.

Alors que les qubits individuels existaient à peine, il définissait les caractéristiques techniques de base d'un tel ordinateur comme suit :

- Des **qubits bien caractérisés** : l'ordinateur quantique utilise des qubits qui exploitent des particules élémentaires pouvant avoir deux états distincts et mesurables. On en connait bien les caractéristiques physiques. L'architecture est scalable au sens où elle permet d'aligner un grand nombre de qubits en batterie. Aujourd'hui existent plusieurs types de qubits déjà évoqués avec les supraconducteurs, les ions piégés, les lacunes de carbone dans le diamant de synthèse, les photons, les fermions de Majorana ou encore les quantum dots de silicium. Dans la pratique, seuls les qubits à base de supraconducteurs sont opérationnels et à petite échelle.

- Des **qubits initialisables** : en général, à la valeur 0 appelée souvent "ground state" pour les quantum associés, correspondant, par exemple, au niveau d'énergie le plus faible d'une particule élémentaire.

- Des **temps de cohérence** largement supérieurs au temps d'activation des portes quantiques

: nous l'avions déjà évoqué dans une partie précédente. Le temps pendant lequel les qubits sont en état de cohérence (superposition d'états) et intriqués (liens entre qubits via des portes doubles) doit être supérieur à la durée d'activation des portes pour que l'on puisse exécuter un algorithme contenant un enchainement d'un grand nombre de portes quantiques. Le ratio espéré est au moins de 1000 pour 1 pour pouvoir exécuter jusqu'à quelques centaines de portes quantiques d'affilée sachant que cette quantité va intégrer les longues suites de portes quantiques utilisées par les codes de correction d'erreurs.

- Un jeu de **portes quantiques universelles** : les qubits doivent pouvoir être contrôlés physiquement avec au moins deux portes quantiques jouant le rôle de portes quantiques universelles à partir desquelles on va pouvoir reproduire toutes les portes quantiques classiques. Il faut au minimum une porte unitaire (agissant sur un seul qubit comme la porte X) et une porte à deux qubits comme la CNOT. L'architecture physique des qubits conditionne la nature des portes quantiques universelles qui agissent sur les qubits. Elles ne sont pas les mêmes d'une technologie à l'autre.

- La **capacité à mesurer l'état des qubits** à la fin des calculs : qui semble évidente. Cette mesure ne doit pas influencer l'état des autres qubits du système. Il faudrait idéalement avoir un taux d'erreur de la mesure qui soit largement inférieur à 0,1%.

DiVicenzo ajoutait deux autres critères optionnels qui servent plutôt aux communications quantiques : la possibilité de convertir des qubits statiques en qubits pouvant se déplacer, et ensuite de transporter de manière fiable un état quantique d'un qubit à l'autre et à distance. C'est utilisé dans les techniques de communication et de cryptographie quantique mais peut aussi servir à relier entre eux différentes unités élémentaires de traitement quantiques.

## paramètres d'un ordinateur quantique

| **critères de DiVincenzo** (IBM, 2000) | **valeurs courantes** |
|---|---|
| qubits bien caractérisés | supraconducteurs, ions piégés, … |
| initialiser tous les qubits | à valeur 0 (ground state) |
| temps décohérence >> activation porte quantique | 100 µs vs 10-100 ns |
| jeu de portes quantiques universelles | X, H, CNOT, SWAP, … |
| mesurer les qubits à la fin du calcul | avec erreur < 0,1% |
| **autres critères pratiques** | **valeurs courantes** |
| nombre de qubits | <=72 en UQ et 2048 en QA |
| température d'opérations | 15 mK ou température ambiante |

D'un point de vue pratique, on caractérise aussi les ordinateurs quantiques par leur nombre de qubits et par leur température de fonctionnement.

Le nombre de qubits est à évaluer à la fois dans le temps présent mais dans sa capacité à évoluer. Certaines technologies sont plus faciles à miniaturiser que d'autres. Et il faut intégrer dans cette miniaturisation à la fois les chipsets quantiques de qubits et les éléments qui les contrôlent. Aujourd'hui, les qubits à ions piégés ou en photonique scalent mal. Les qubits

supraconducteurs scalent moyennement. Et les qubits en CMOS (spins d'électrons et quantum dots) scalent le mieux.

Les ordinateurs quantiques actuellement opérationnels, à base de supraconducteurs, fonctionnent tous à très basse température autour de 15 mK (1 mK = 1 milli-kelvin, 0 kelvin = 0 absolu situé à –273,15°C), mais certains types de qubits à l'état de recherche sont censés fonctionner à température ambiante, comme ceux de l'optique linéaire à base de photons et les NV Centers(cavités dans du diamant dopé à l'azote). Le fonctionnement à très basse température est un moyen de préserver la cohérence des qubits. Mais il limite la quantité d'énergie consommable autour des qubits pour en contrôler localement l'état. Un fonctionnement à 1K ou 4K permettra de consommer plus d'énergie pour contrôler les qubits qu'un fonctionnement à 15 mK.

Ces considérations permettant de jauger les capacités d'un ordinateur quantique impliquent la création d'une nouvelle discipline : le benchmarking d'ordinateurs quantiques ! Elle nécessite évidemment des moyens intellectuels et physiques qui dépassent ceux du test de simples smartphones ou laptops !

Comme l'indique Kristel Michielsen dans **Benchmarking gate-based quantum computers**, 2017 (33 pages), les benchmarks peuvent s'appuyer lorsque le nombre de qubits est inférieur à 50 à une comparaison du rendu des algorithmes entre ordinateurs quantiques et leur simulation sur supercalculateurs.

Les ordinateurs quantiques benchmarkés auront généralement des caractéristiques dissemblables : des portes quantiques universelles différentes nécessitant l'assemblage de différentes portes quantiques par les compilateurs pour exécuter un même algorithme, et des codes de correction d'erreurs différents, adaptés au taux d'erreurs des qubits et des portes quantiques des ordinateurs comparés. Les dissemblances seront bien plus importantes qu'entre deux processeurs Intel et AMD ou deux processeurs de smartphones !

**Les grandes catégories d'ordinateurs quantiques**

Il y a ordinateur quantique et ordinateur quantique. On oppose souvent les ordinateurs quantiques adiabatiques du Canadien D-Wave aux ordinateurs quantiques universels d'IBM ou Google. Mais il faut compter en tout avec au moins quatre catégories d'ordinateurs quantiques que voici :

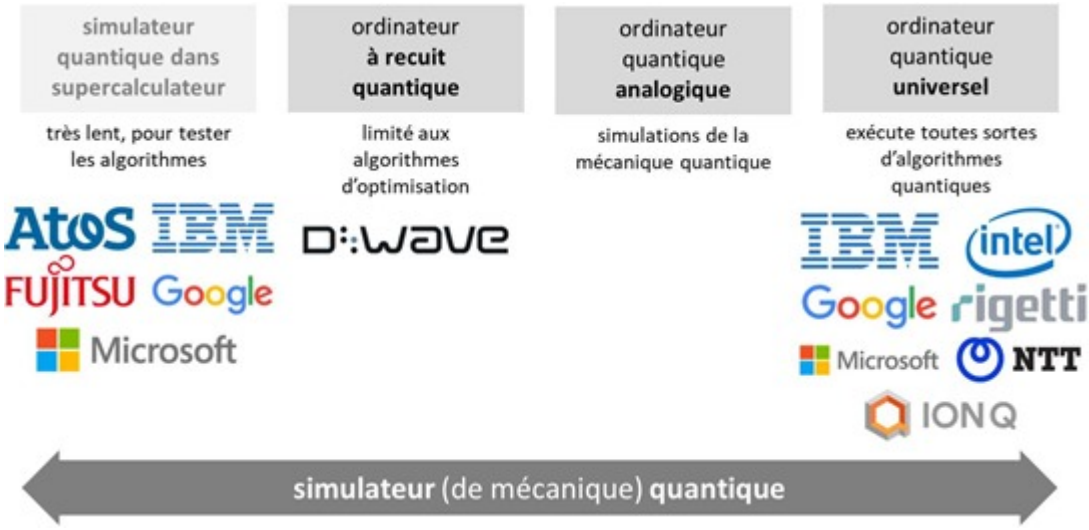
- Les **supercalculateurs classiques** qui sont utilisés pour réaliser des simulations de l'exécution d'algorithmes quantiques. Ils transforment ces algorithmes, les portes quantiques et les qubits pour exploiter les capacités de traitement d'ordinateurs traditionnels. Cela permet de tester des algorithmes quantiques sans ordinateurs quantiques. Mais c'est bien plus lent ! A ce jour, les supercalculateurs peuvent simuler jusqu'à l'équivalent d'une quarantaine à une cinquantaine de qubits. C'est ce que proposent IBM, Microsoft, Google et le Français Atos. Simuler des ordinateurs quantiques de cette manière demande beaucoup de puissance à la fois côté mémoire, pour stocker 2 puissance N états de registres quantiques à N qubits, ainsi que pour les traitements associés qui reposent sur des multiplications de matrices en nombres flottants. Des records dans ce domaine sont régulièrement battus. En 2017, la **simulation de 45 qubits** était réalisée sur un supercalculateur du Département de l'Energie US (du National Energy Research Scientific Computing Center ou NERSC)

exploitant 8192 processeurs Intel Xeon Phi, ce qui s'explique par la présence d'un centre de recherche conjoint avec Intel au NERSC. Le record était battu la même année par IBM avec la simulation de 56 qubits. Pour simuler 49 qubits, il faut rien moins qu'un Péta-Octets de mémoire vive !

- Les **ordinateurs quantiques** à recuit simulé comme ceux du Canadien D-Wave. Ils s'appuient sur des qubits de qualité moyenne et sont adaptés à l'exécution d'une partie seulement des algorithmes quantiques connus et avec un gain en puissance de calcul intéressant mais contesté par certains spécialistes. Cette technique utilise une évolution lente et contrôlée d'un ensemble de qubits reliés entre eux dans des matrices de qubits ("lattice"). On l'initialise dans un état voisin de la solution et le système converge vers la solution qui relève souvent de la recherche d'un minimum énergétique comme pour la simulation d'interactions atomiques dans des molécules ou l'optimisation de la durée d'un parcours complexe.

- Les **ordinateurs quantiques analogiques** servent de simulateurs de phénomènes quantiques sans passer par la case qubits avec ses 0 et 1. Ce sont des outils de laboratoires. Cette catégorie comprend les ordinateurs quantiques utilisant de l'optique linéaire, à savoir des photons. Il est pour l'instant difficile de les faire monter en puissance. Il n'existe pas d'offre commerciale dans le domaine, même en devenir.

- Les **ordinateurs quantiques universels** utilisent des qubits avec des portes quantiques capables d'exécuter tous les algorithmes quantiques et avec un gain de vitesse optimum par rapport aux supercalculateurs ainsi que vis à vis des ordinateurs quantiques adiabatiques. Ils sont pour l'instant limités à une cinquantaine de qubits. Le niveau de bruit quantique des qubits nuit à l'efficacité des calculs et impose de démultiplier les qubits et l'enchaînement des portes quantiques pour gérer des codes de correction d'erreurs quantiques (QEC). En attendant que ces ordinateurs quantiques montent en puissance avec des qubits de qualité, on se contente de qubits de qualité intermédiaire. Cette sous-catégorie d'ordinateurs quantiques universels est baptisée NISQ pour "Noisy Intermediate-Scale Quantum" dans par John Preskill dans **Quantum Computing in the NISQ era and beyond** en 2018. Elle décrit les ordinateurs quantiques universels existants et à venir dans un futur proche supportant 50 à quelques centaines de qubits et à même de dépasser les capacités des supercalculateurs.



Enfin, l'expression ambigüe de simulateur quantique est principalement accolée aux ordinateurs quantiques analogiques qui sont dédiés à la simulation de phénomènes quantiques. Elle est aussi applicable aux trois autres catégories d'ordinateurs quantiques qui ont aussi la capacité de simuler les effets quantiques de la matière. La simulation d'effets quantiques est comme nous l'avons vu dans la partie sur les algorithmes et les applications quantiques la catégorie d'application la plus enthousiasmante du quantique de par son impact potentiel sur l'environnement et la santé.

**Incertitude quantique**

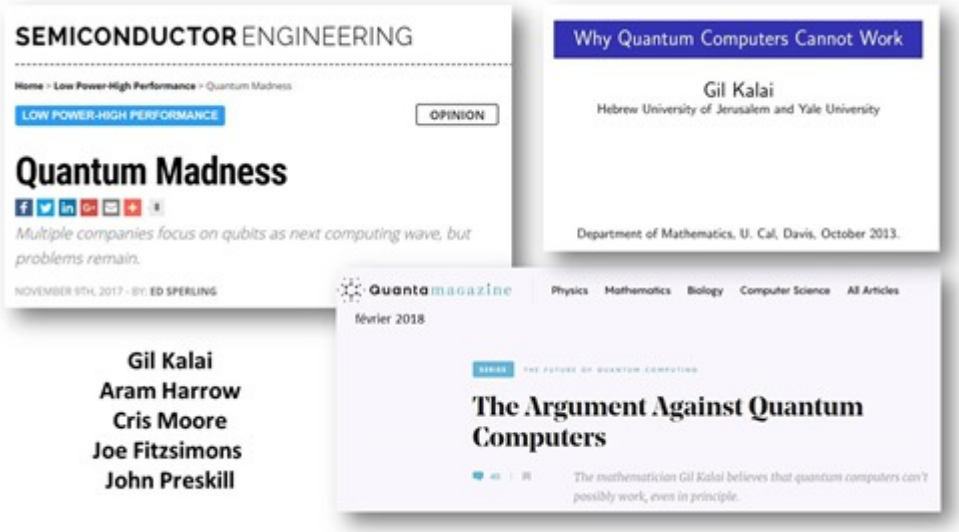
La prospective dans l'informatique quantique est art difficile. On navigue entre les optimistes et les pessimistes. **Google**, **IBM** et **Microsoft** pensent atteindre relativement rapidement la suprématie quantique et réaliser des ordinateurs quantiques de plus de 100 qubits de qualité d'ici moins d'une décennie. Leur communication se fait à plusieurs niveaux : pour le grand public, elle est simplificatrice et destinée à marquer les esprits, quitte à enjoliver la mariée. Pour les spécialistes qui peuvent décortiquer leurs publications scientifiques, le regard est évidemment plus nuancé, notamment au sujet de la fiabilité des qubits qu'ils génèrent. Ils communiquent beaucoup sur leurs efforts pour réduire le bruit des qubits pour les rendre plus fiables. Cf **The Era of quantum computing is here. Outlook: cloudy** de Philipp Ball paru en avril 2018 dans Science.

Les pessimistes comprennent notamment le chercheur israélien **Gil Kalai** qui pense que l'on n'arrivera jamais à créer des ordinateurs quantiques avec un faible taux d'erreurs. Il documente son point de vue dans la présentation **Why Quantum Computers Cannot Work** qui date de 2013 (60 slides) qui reprend les points de **How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation** de 2011 (16 pages) ainsi que **The Argument Against Quantum Computers** de Katia Moskwitch publié en février 2017. Selon Gil Kalai, on ne peut pas créer d'ordinateurs quantiques stables à cause du bruit qui affecte les qubits. Il travaille même sur la réalisation de modèles mathématiques visant à prouver l'impossibilité d'outrepasser ces erreurs, même avec les codes de correction d'erreurs quantiques.

**The development of a scientific field** de Cristian Calude et Alastair Abbot en 2016 évoquent le fait que l'avantage des principaux algorithmes quantiques utilisables en pratique génèreraient une accélération modeste quadratique (racine carrée du temps classique) qui pourrait être atteinte sur ordinateurs classiques avec des approches heuristiques. Cette réserve est aussi manifeste dans **Quantum Madness** de Ed Sperling qui faisait le point du domaine en novembre 2017 en rappelant tous les obstacles à surmonter.

Dans **Predictions we didn't make**, en janvier 2018, Kenneth Regan pense qu'un industriel – probablement Google – va prétendre avoir atteint la suprématie quantique en 2018 et qu'il sera rapidement contredit par la communauté scientifique.

Pour le profane un peu éclairé que je suis sur le sujet, il est très difficile de faire la part des choses entre l'incertitude scientifique et l'incertitude technologique. La première est généralement plus difficile à lever que la seconde. Pour le Français **Alain Aspect**, il n'y aurait pas d'obstacle scientifique à la création d'ordinateurs quantiques fiables. Il pense que l'incertitude est uniquement technologique mais qu'il faudra quelques décennies pour la lever. Ce ne serait donc qu'une affaire de patience !

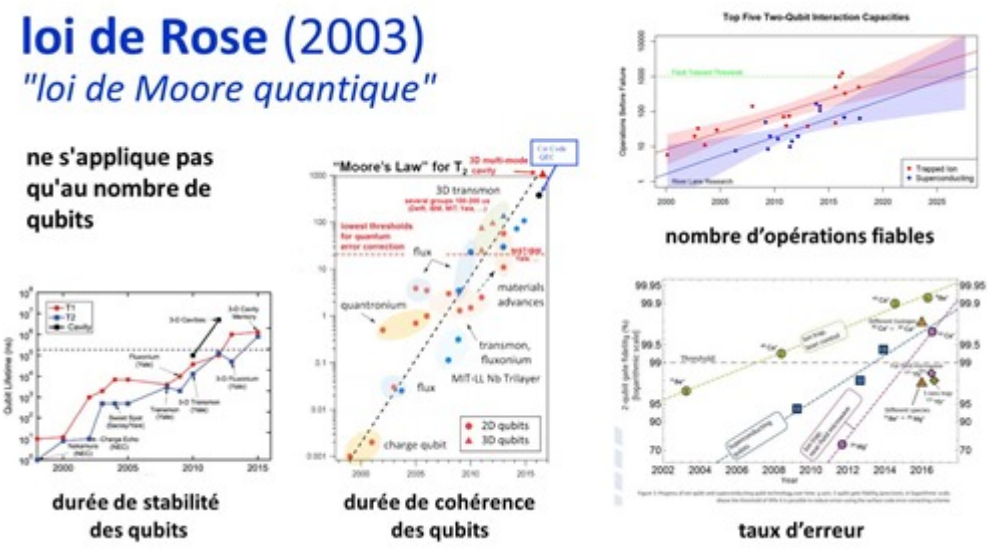



Ce lot d'incertitudes pose des questions existentielles sur la manière de gérer un tel cycle d'innovation au long cours. Quand faut-il investir ? Quand les positions sont-elles prises ? Est-ce que la recherche fondamentale est découplée de l'industrialisation ? Je traiterai de la question dans une partie dédiée aux stratégies industrielles des pays qui s'investissent avec volontarisme dans le quantique.

Mais on peut déjà constater que les variantes de cultures d'innovation et économiques ont un impact sur les approches industrielles. Les grands industriels du numérique tels que IBM, Google, Intel et Microsoft peuvent se permettre d'investir en R&D sur le quantique avec une vision très long terme. Ils ont la profitabilité, le cash et les compétences qui le permettent. Des startups plus ou moins bien financées au Canada et aux USA comme D-Wave, Rigetti ou IonQ peuvent aussi adopter une vision assez long terme, même si elle dépend toujours de leur capacité à commercialiser des prototypes d'ordinateurs quantiques et d'avoir des investisseurs à même de les accompagner sur de nombreuses années avant de voir la couleur de leur retour sur investissement. Les montants correspondants ne sont pas forcément délirants. Rigetti n'a levé à ce jour que $70M, un montant maintenant accessible à des startups françaises dans les biotechs ou le numérique en général.

Les problèmes technologiques à résoudre concernent les matériaux utilisés dans les qubits, la correction d'erreurs, la cryogénie à grande échelle pour pouvoir intégrer un grand nombre de qubits dans un ordinateur et bien évidemment les avancées algorithmiques. L'approche requise est éminemment pluridisciplinaire avec des mathématiques, de la physique fondamentale et de la chimie.

On peut aussi extrapoler les évolutions de ces dix dernières années dans l'informatique quantique. Cofondateur de D-Wave en 1999, Georgie Rose édicta en 2003 son propre équivalent de la loi empirique de Moore, la **loi de Rose**, prédisant un doublement tous les ans du nombre de qubits dans un ordinateur quantique. Jusqu'à présent et depuis 2007, D-Wave a tenu cette promesse.




Mais cette loi exponentielle est aussi observée dans l'évolution d'autres paramètres de fonctionnement des ordinateurs quantiques comme la durée de stabilité des qubits, leur taux d'erreur et le nombre d'opérations consécutives réalisées de manière fiable. Une partie des schémas ci-dessus proviennent de **Technical Roadmap for Fault-Tolerant Quantum Computing**, un rapport UK publié en octobre 2016 et de **cette autre source**.

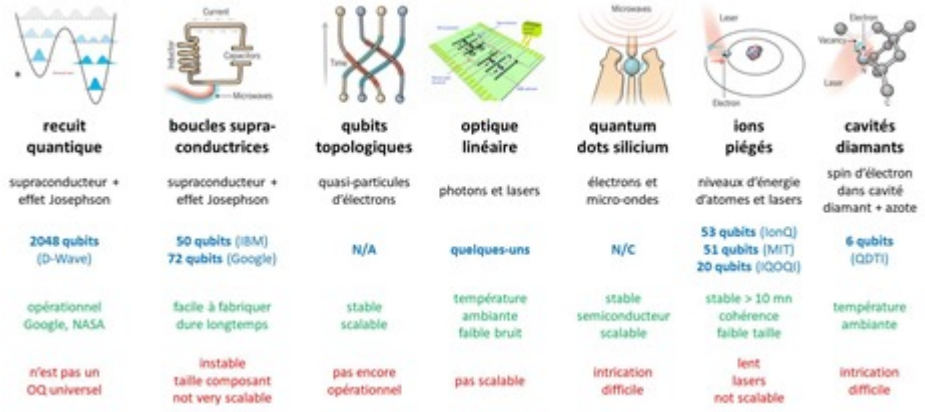
**Les grandes technologies d'ordinateurs quantiques**

Comme nous l'avions vu dans la **partie dédiée aux types de qubits**, il se dégage six grandes catégories d'ordinateurs quantiques :

- Le **supraconducteur** à effet Josephson utilisé par les ordinateurs quantiques universels d'IBM, Google, au CEA ainsi que dans les ordinateurs adiabatiques de D-Wave.
- Les **ions piégés** que l'on trouve notamment chez IonQ, une spin-off de l'Université de Maryland.
- Le **topologique** avec les fermions de Majorana de Microsoft ainsi que Nokia qui n'existent pas encore.
- L'**optique linéaire** qui n'est pas très scalable mais potentiellement prometteuse.
- Les **CMOS** poussés notamment par Intel et le CEA.
- Enfin, les **cavités de diamants** (NV Centers), poussées notamment par la startup QDTI ainsi que par le CEA dans une **approche hybride** cavités diamants et supraconducteurs.

Nombre des entreprises privées de ce cheptel sont associées avec des laboratoires de recherche américains ou européens. Google collabore avec l'Université de Santa Barbara en Californie, IBM et Microsoft avec celle de Delft aux Pays Bas, et IBM avec celle de Zurich.


Ces catégories de technologies ont des niveaux de maturité très différents. Les qubits à base de supraconducteurs sont à ce jour les plus éprouvés. Les ions piégés, les quantum dots, l'optique linéaire et les NV Centers ont du mal à "scaler". Les fermions de Majorana sont encore dans les limbes même si Microsoft s'apprête à annoncer de bonnes nouvelles de ce côté-là.




Autre point, les startups ne sont pas si nombreuses dans ce tableau. D-Wave se porte bien mais Rigetti évolue plus lentement tout comme QDTI et IonQ. Enfin, ce paysage est largement dominé par les USA, même s'il n'intègre pas les initiatives chinoises comme celle d'Alibaba.

---

Nous allons par la suite faire le tour d'une partie des acteurs cités "colonne par colonne" en commençant par la technologie du recuit quantique des **ordinateurs quantiques adiabatiques du Canadien D-Wave** et de leur imitation digitale de Fujitsu. Puis nous passerons aux ordinateurs quantiques universels à base de supraconducteurs. Puis enfin, aux autres technologies.

Cet article a été publié le 8 août 2018 et édité en PDF le 5 septembre 2020.