TRIBUNE
HARWELL

# L'ORDINATEUR QUANTIQUE

## Risques, besoins et opportunités pour les institutions financières

Juin 2020

HARWELL
MANAGEMENT

# Investir dans la R&D quantique, un pari sur l'avenir à (très) long terme ?

**L'ordinateur quantique, un risque pour la cyber-sécurité mais aussi une réponse aux besoins des institutions financières en termes de sécurisation des échanges, d'évaluation des risques et de détection des fraudes.**

**La sécurité informatique** via le cryptage des données est un enjeu majeur pour les banques : transactions financières, système de paiement, sécurisation des données sensibles… Cependant, elle est menacée par l'arrivée potentielle de l'ordinateur quantique et de sa puissance de calculs infiniment plus grande que celle de nos ordinateurs actuels.

Commençons par un peu de théorie pour comprendre comment fonctionne un ordinateur quantique et ce qui le rend si puissant.

Contrairement à la physique classique dont les lois régissent notre quotidien, la physique quantique, elle, est l'ensemble des lois qui s'appliquent au monde de l'infiniment petit : les particules.

**Deux grands principes quantiques** sont à connaître pour comprendre le fonctionnement de l'ordinateur quantique :

***La superposition quantique.***

Dans l'infiniment petit, les particules peuvent se trouver dans un état indéterminé. Alors que la valeur d'un bit est soit 0 soit 1, un qbit (l'élément de base de l'ordinateur quantique) a une valeur indéterminée tant que celle-ci n'est pas mesurée. Une fois mesurée par contre, la valeur est figée.

***L'intrication quantique.***

On peut lier deux objets quantiques ensemble, en les forçant à se trouver dans un état opposé au moment d'une mesure. Par exemple si l'un est + l'autre sera -. Ces 2 éléments sont intriqués. On les sépare (de plusieurs kilomètres). On mesure le premier puis immédiatement après le deuxième, on trouvera toujours le même résultat. Si la mesure du premier est +, la mesure du deuxième sera – et inversement. Pourtant ces 2 objets n'ont pas communiqué entre eux, ils font partie en réalité d'un même système.

## Le fonctionnement d'un ordinateur quantique

Le qbit est l'élément de base de l'ordinateur quantique. Sa valeur repose sur le principe de la superposition quantique. Ainsi la valeur d'un qbit n'est pas 0 OU 1 comme un bit mais 0 ET 1 avec une probabilité d'être 0 et une probabilité d'être 1. Dans un ordinateur quantique, les portes quantiques vont faire varier ces probabilités et donc modifier les valeurs possibles des qbit.
Plus un ordinateur quantique a de qbit, plus la puissance de calcul est forte (comme un ordinateur classique avec les bits) et d'autant plus forte que les qbit sont intriqués entre eux. Ainsi on obtient un système unique et une force de calcul décuplée.

## Deux algorithmes quantiques ont été développés :

***L'algorithme de Shor (1994)***

Cet algorithme permet de factoriser un entier en nombres premiers. Les méthodes de cryptages actuelles utilisent la complexité de la factorisation de très grands nombres en nombres premiers très grands aussi donc. Mais en utilisant l'algorithme de Shor, pour factoriser un entier de 300 chiffres, alors qu'un ordinateur classique aurait besoin de 30 000 ans, un ordinateur quantique le ferait en 10 secondes… la sécurité des données serait mise à mal.

### *L'algorithme de Grover (1996)*

Cet algorithme permet de trouver un élément dans une base de données non triée. Pour illustrer son fonctionnement, prenons l'exemple d'un gymnase avec 1000 personnes dedans. Nous voudrions savoir combien il y a d'hommes de plus de 50 ans et mesurant plus de 1,80m. Un ordinateur classique irait voir chaque personne les unes après les autres pour vérifier si ces conditions sont réunies et après avoir vu les 1000 personnes pourrait donner le nombre de celles recherchées. Un ordinateur quantique lui va demander tout haut aux personnes concernées de lever la main, pour pouvoir les compter. Méthode beaucoup plus rapide.

Si le décryptage des données par un ordinateur quantique est un risque potentiel, le cryptage en est également la solution ! Les calculs quantiques permettraient de crypter les données et transactions de façon complètement sécurisée.

**Les domaines d'application de l'ordinateur quantique** ne se cloisonnent pas à la sécurisation des données. Un autre enjeu majeur des banques pourrait profiter de cette puissance de calcul pour améliorer le processus d'évaluation des risques.

La banque espagnol CaixaBank a récemment partagé les résultats positifs de son test sur l'évaluation de ces risques. La banque a testé sur deux portefeuilles fictifs (hypothécaire et obligations du trésor) deux outils d'IBM : le framework Qiskit et IBM Q System One. L'évaluation des risques a été faite par un ordinateur classique et un ordinateur quantique pour pouvoir comparer les conclusions et le temps de calculs. Les conclusions ont bien été les mêmes pour les deux outils, mais les temps de calculs sont considérablement réduits pour l'ordinateur quantique.

**L'intelligence artificielle** pourrait également profiter de l'ordinateur quantique. Avec une classification des données plus précise qu'avec le machine learning actuel, grâce à l'algorithme de Grover, de nouveaux patterns jusque-là non identifiés par un ordinateur classique pourraient l'être avec un ordinateur quantique, outil efficace pour la détection des fraudes par exemple.

### *Investir dans la R&D quantique, un pari sur l'avenir à (très) long terme ?*

Qu'est ce qui bloque aujourd'hui ? Qu'attendons-nous pour nous servir des ordinateurs quantiques et de leur puissance de calculs ?

### Le temps de cohérence

Pour fonctionner, un ordinateur quantique et ses éléments doivent pouvoir être stables le temps du calcul. Or pour maintenir un qbit (photon, électron, noyau atomique ou ion) stable, il faut les maintenir à une température proche du 0 absolu (-273,15°C) tout en les manipulant… Les technologies actuelles ne permettent pas un temps de calculs suffisant pour exploiter la puissance de calcul nécessaire et recherchée. D'autant que pour avoir suffisamment de puissance, il faut un très grand nombre de qbits intriqués (10 000 pour factoriser un nombre entier de 300 chiffres), et plus il y a de qbits, plus l'environnement est difficile à stabiliser. Le résultat obtenu si le calcul est trop long ne sera pas cohérent et donc inexploitable.

Aujourd'hui IBM et Google détiennent le record du nombre de qbits utilisés par un ordinateur quantique avec 53 qbits. Des géants comme Microsoft, Intel et Honeywell sont également dans la course de l'ordinateur quantique. Des start-up telles que Cambridge Quantum Computing et Zapata Computing elles se concentrent sur les outils logiciels. Enfin JPMorgan Chase investit pour la définition d'algorithmes quantiques dans le secteur financier.

### Les projections pour l'ordinateur quantique

Pour les plus optimistes comme Google ou Microsoft, nous sommes à une dizaine d'année de pouvoir exploiter un ordinateur quantique suffisamment puissant et fiable et ainsi bouleverser le système actuel. D'autres scientifiques eux sont plus pessimistes : l'israélien Gil Kalai, les français Serge Haroche ou encore Xavier Waintal ne sont pas sûrs qu'il soit techniquement possible de créer des ordinateurs quantiques fiables à cause du bruit généré qui affecte les qbits et rendrait les calculs incohérents.

Il est donc difficile de prédire avec certitude si l'ordinateur quantique fonctionnera un jour et si oui, dans combien de temps, 10 ans ? 30 ans ? 50 ans ? Les progrès se font cependant de manière

continue, et déjà aujourd'hui IBM met à disposition la puissance de calcul de son ordinateur quantique via le cloud. Encore faut-il avoir les connaissances nécessaires pour pouvoir créer un algorithme quantique sans quoi l'ordinateur quantique n'est pas utilisable.

### Investissements actuels et futurs

On recense cinq fonds d'investissement spécialisés dans l'informatique quantique dans le monde (français, britannique, russe et canadien) et environ 70 startups. Le français Quantonation, créé fin 2018, investit sur des projets pour la plupart français : coprocesseur optique ou encore sécurité quantique, sur les technologies matérielles et logicielles.

Les ambitions françaises ne s'arrêtent pas là. Le rapport Forteza remis au gouvernement en janvier 2020 détaille le rôle majeur et innovant que la France devrait avoir dans les domaines d'application de l'informatique quantique telle que la cryptographie, les télécommunications ou encore l'IA. Le souhait étant d'investir 1,4 milliard d'euros sur 5 ans, dont 500 millions venant du secteur privé ou de financements européens.

De nombreux projets sont encore à lancer, et les investissements seront indispensables pour permettre à l'hexagone de rester dans cette course technologique.

## NOS EXPERTS

**Sébastien DUPORTAL**
Partner - Practice Assurance, Retail & Digital
Sebastien.duportal@harwell-management.com

**Fabien COURNEE**
Manager Assurance, Retail & Digital

**Flora MATHIOT**
Consultante Confirmée