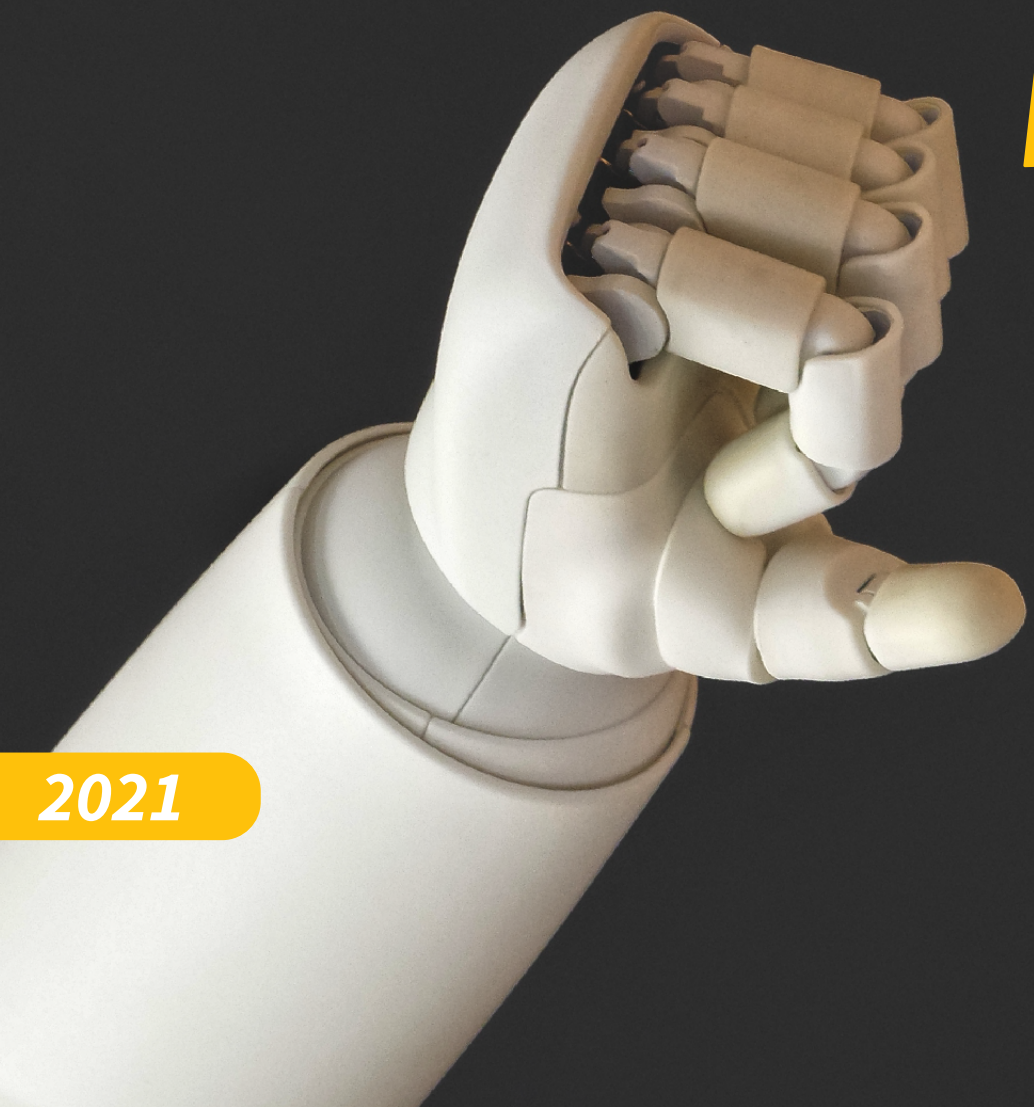
Syd
DIGITAL CARE

#2

Note de
PROSPECTIVE

LA QUANTIQUE, DE NOUVEAUX ENJEUX



source : Unsplash.com

2021

source : Unsplash.com

QUANTIQUE : UN SAUT HISTORIQUE

Avant de parler du futur, parlons du présent. Depuis les années 60, les hommes ont sans cesse cherché à augmenter la puissance des ordinateurs. Des énormes machines de traitement ont été créés à la fin des années 70 et durant la décennie 80. Le but, à l'époque, était d'informatiser des masses considérables de traitements simples. Bull, en France et IBM... dans le reste du monde se sont ainsi fait les adjoints directs des centres de production bancaires, assuranciels et administratifs. Un peu plus tard, des machines plus « petites » ont été déployées pour des traitements simples plus locaux. Il s'agissait de réaliser les comptabilités d'entreprises de belles tailles. Ces technologies ont été baptisées « mini-informatique ». Des machines « propriétaires » avec leur propre système d'exploitation d'abord, puis avec des dérivés adaptés d'Unix se sont déployées dans le monde entier. L'AS 400 d'IBM et les serveurs SUN sont, peut-être, des noms qui vous reviennent en mémoire. Une fois que les processus transversaux simples ont été pris en charge, ça a été au tour des personnes. Le Micro-Ordinateur était né. Des fabricants de processeurs comme Intel et des éditeurs de logiciels comme Microsoft ont réussi le double tour de force de nous convaincre que chacun d'entre nous avait besoin d'un ordinateur et que les serveurs dont nous dépendions pour travailler ensemble devaient aussi disposer de la même architecture interne. Depuis, le milieu des années 90 a donc commencé la course à l'augmentation de la puissance de ces ordinateurs dans un monde « WinTel » quasiment monopolistique.

IA : L'EXIGEANCE DE NOUVELLES ARCHITECTURES

Un premier changement de paysage est apparu avec l'avènement de l'IA (Intelligence Artificielle). Si le processeur de ces ordinateurs était de plus en plus puissant, le reste de la structure du matériel suivait, plus à la traine. Les « gameurs » exigeaient bien des cartes graphiques plus musclées pour améliorer la fluidité de jeux de plus en plus complexes et réalistes.

Et c'est justement des fabricants de ces cartes qu'est venue l'innovation. Les mécanismes de machine learning sur lesquels reposent une grande partie de ce qu'on appelle aujourd'hui l'IA sont fondés sur des réseaux de neurones. Or, ces programmes autonomes et fonctionnant en réseaux apprenants sont plus efficaces sur les processeurs issus des cartes graphiques que sur ceux destinés aux cartes mères. C'est ainsi que la société Nvidia est entrée dans la course. Bien connue de la communauté des joueurs en ligne pour ses cartes graphiques, la société a commencé à proposer ses GPU (Graphical Processor Units) pour concevoir des machines dédiées à l'IA en lieu et place des traditionnels CPU (Computer Processor Units) traditionnellement fournis par Intel. Les supercalculateurs les plus performants destinés à l'IA sont équipés de GPU.

Source : Unsplash.com

Source : Unsplash.com

ENCORE ET TOUJOURS L'IA

Et c'est encore l'IA qui nous pousse aujourd'hui à étudier d'autres architectures. Les plaquettes de silicium découpées avec des tressages de plus en plus serrés – on parle de la limite des 10 nanomètres – arrivent à ses limites. Si la loi de Moore nous expliquait que les processeurs pouvaient doubler de puissance tous les 6 mois, les chiffres annoncés par les fabricants se placent aujourd'hui sur des courbes plus asymptotiques. Or, si l'IA fonctionne aujourd'hui très bien dans des environnements prévisibles, elle montre tous les jours ses limites quand on veut l'utiliser dans « La Vraie Vie ». Le réel oblige en effet les concepteurs de ces systèmes à imaginer l'ensemble des choses qui pourraient se passer, mais aussi, comment se ré-étalonner et décider quoi faire face à l'imprévu. Ce sont notamment les recherches et surtout les essais réalisés sur les voitures autonomes qui ont pointé du doigt cette difficulté.

Que faire donc quand vous avez besoin de plus en plus d'intelligence et que les capacités matérielles sont d'ores et déjà annoncées comme limitées ?

REVENIR SUR LES FONDAMENTAUX DE L'INFORMATIQUE

La micro-informatique, vient de l'informatique. L'informatique vient de l'électronique. Et l'électronique vient de l'électrique. Tout le monde sait qu'un ordinateur fonctionne à partir de 0 et de 1. «0» veut dire que le courant ne passe pas, «1» qu'il passe. C'est aussi simple et fondamental que ça. Et c'est justement ce fondement que l'informatique quantique vient bouleverser.

Depuis le tout début du XX^{ème} siècle (1927 – 5ème congrès Solvay sur la physique quantique), nous savons qu'un électron « tourne sur lui-même » dans un sens ou dans l'autre. Ce mouvement est appelé « spin ». Or, la simple observation de ce même électron peut changer son sens de rotation, son spin. Il est donc coutume de dire que le spin d'un électron est dans un état… Indéterminé. Et c'est justement ce même « flou » que les ordinateurs quantiques exploitent en lieu et place du 0 et du 1.

La conséquence de cette révolution en marche est l'annonce d'ordinateurs 100 millions de fois plus puissants ! Il n'est donc pas étonnant que les firmes, les pays et même les continents se soient lancés dans une course pour atteindre la « supériorité quantique ».

Mais ce chemin ne va pas sans poser quelques difficultés.

Source photos : Unsplash.com

1. L'ISOLEMENT NÉCESSAIRE DES MACHINES :

On l'imagine bien, les traitements quantiques sont très délicats. Ils nécessitent d'être isolé du reste du monde. Une source de chaleur externe pourrait, par exemple, perturber les calculs. C'est la raison pour laquelle les « processeurs quantiques » fonctionnent à une température proche du 0 absolu (- 273,15° C). Pas encore facile d'imaginer des ordinateurs portables quantiques dans ces conditions.

2. LE BRUIT QUANTIQUE

Contrairement à la précédente génération d'ordinateurs, les « processeurs quantiques » qui n'utilisent pas le 0 et le 1 sont naturellement soumis à des micro-erreurs. On appelle la collection aléatoire de ces erreurs le « bruit quantique ». C'est la raison pour laquelle la société Atos a annoncé le 6 avril 2018 que son programme Atos QLM (Quantic Learning Machine) contenait désormais un simulateur de bruit quantique capable de s'appliquer à des machines dépassant les 40 Qbits. De nombreux pays ont déjà fait l'acquisition de ce programme de simulation quantique le plus puissant du monde (Autriche, Finlande, France, Allemagne, Inde, Italie, Pays-Bas, Sénégal, au Royaume-Uni, États-Unis, Japon).

3. DES NORMES INTERNATIONALES DE SÉCURITÉ QUI NE TIENNENT PLUS :

Un des mécanismes de chiffrement les plus utilisés aujourd'hui est le RSA. Il fonctionne à partir d'une clef publique pour chiffrer le message et d'une clef privée pour le décoder. C'est ce mécanisme qui est utilisé, par exemple, dans les achats en ligne et les transactions internet. Il permet de valider que c'est bien votre navigateur qui passe la commande. Un chiffrement RSA met 400 ans à être cassé par un ordinateur classique.

Source photos : Unsplash.com

LA CRYPTOGRAPHIE POST QUANTIQUE, UNE SOLUTION ?

Or, cette cryptographie à clef publique intervient presque partout et dans toutes les communications aujourd'hui sécurisées : les communications sur les réseaux Internet (https, VPN IPSec), les applications mobiles de messagerie (Signal, WhatsApp…), les protocoles de signature électronique, et même les applications de blockchain.

C'est la raison pour laquelle Le NIST (National Institute of Standards and Technologies – US Agency of Commerce Department) a demandé dès 2016 une normalisation des protocoles quantiques et estime, avec la NSA (National Security Administration) que cette menace pourrait être réelle dès 2030. Mais le problème est déjà d'actualité en particulier pour les secteurs qui gèrent des données secrètes et sensibles à longue vie comme la défense, la finance, l'aérospatial, l'énergie, l'automobile, la pharmacie ou la santé. Les hackers utilisent le principe « collecter maintenant et décrypter demain » (« harvest now and decrypt later »). Une organisation disposant de gros moyens de stockage pourrait ainsi enregistrer les transactions cryptées aujourd'hui pour les décoder dans quelques années.

Mais des réponses sont déjà à l'étude comme la « cryptographie post quantique » ou la distribution de clefs quantiques. Et, pour accompagner et dynamiser cette transition, le Président de la République Emmanuel Macron a annoncé le 21 janvier 2021 le plan d'investissement national dans le quantique. Ce plan vise à mettre la France dans le trio de tête mondial des technologies quantiques ; il comprend un investissement de 1,8 milliards d'Euros sur 5 ans, avec un volet de 150 millions d'Euros sur la cryptographie résistante au quantique.

Source photos : Unsplash.com

Source photos : Unsplash.com

ET EN FRANCE ?

*Le 08 juin 2021, **la société Pasqal** annonce avoir levé 25 millions d'euros pour son calculateur quantique basé sur la technologie des atomes froids (Quantonation + Fonds Innovation Défense).*

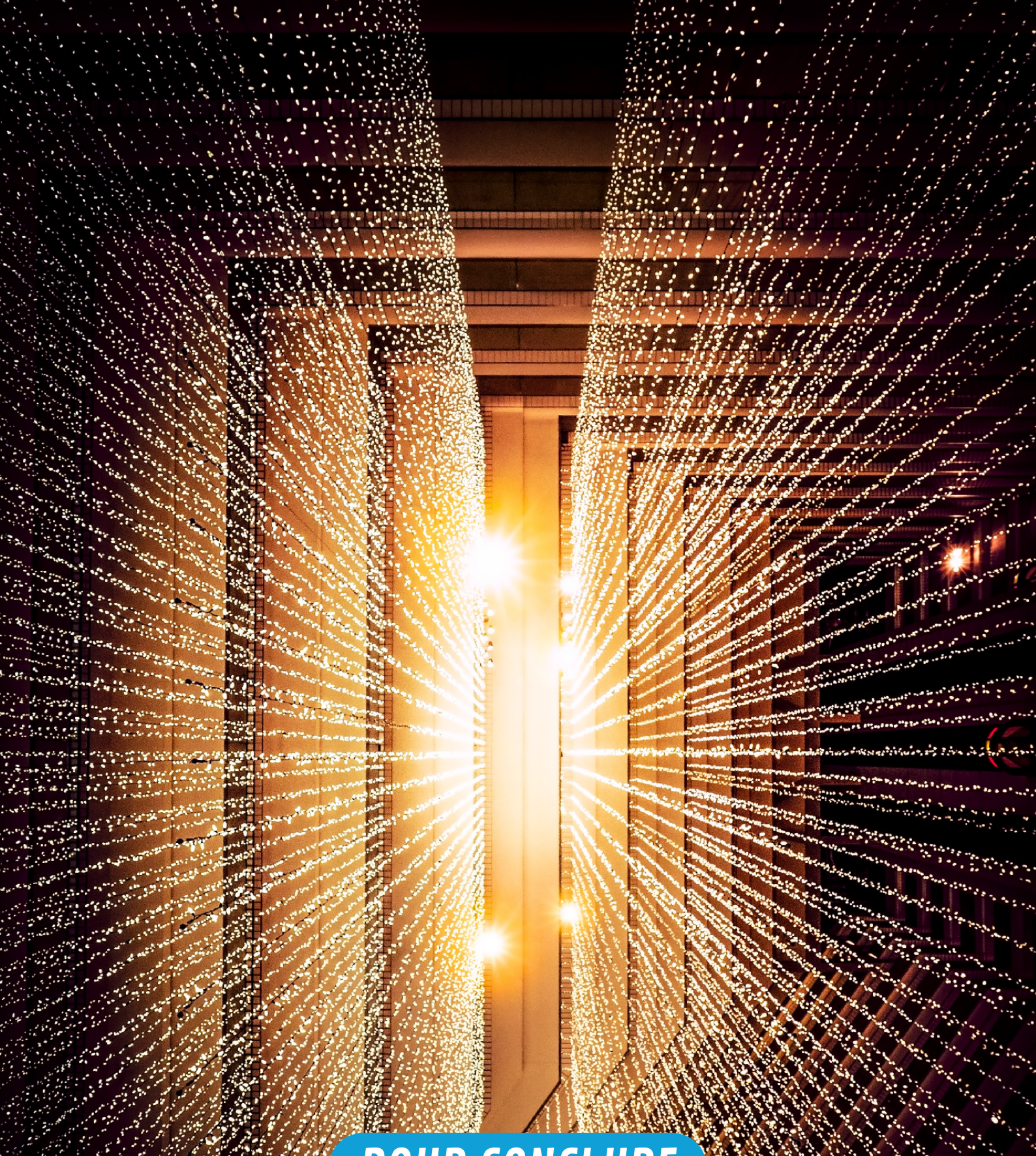
*En 2018 Charles Beigbeder, Christophe Jurczak et Olivier Tonneau créent le fond d'amorçage **Quantonation** dédié à l'ordinateur quantique et ses applications. Le 04 mars 2021, 3 ans et 12 prises de participation plus tard, ils lancent leur premier fonds professionnel de capital investissement Quantonation I avec 21 millions d'euros.*

*Le 17 juin 2020, La startup **Qubit Pharmaceuticals** clôt un tour de table qui lui permettra de mettre sur le marché sa première plate-forme, Atlas, une suite logicielle qui exploite pleinement la puissance de calcul des superordinateurs et futurs ordinateurs quantiques pour co-développer, avec les sociétés pharmaceutiques et biotechnologiques, de nouveaux médicaments plus efficaces et plus sûrs. Qubit Pharmaceuticals est capable de modéliser et simuler de façon précise les interactions entre molécules, et d'identifier le site d'intérêt d'une cible biologique, jusqu'à 1.000.000 de fois plus vite que les solutions existantes. Le 19 juin 2020, Qubit Pharmaceuticals annonce la clôture d'un tour de table de pré-amorçage avec le fonds Quantonation.*

Passer de l'approximation à la prédiction des interactions moléculaires pour développer de meilleurs médicaments

Malgré l'investissement de dizaines de milliards de dollars par an, le développement de nouvelles molécules thérapeutiques reste coûteux, long et risqué. Bien que les méthodes actuelles de criblage et de design in-silico de médicaments aient déjà permis une accélération du rythme de la R&D, la simulation numérique des interactions entre molécules a été jusqu'à présent entravée par la complexité de la physique quantique au niveau microscopique. En prenant en compte des interactions très fines entre les molécules, Qubit Pharmaceuticals est capable de modéliser et simuler de façon précise les interactions entre molécules, identifier le site d'intérêt d'une cible biologique, jusqu'à 1.000.000 de fois plus vite que les solutions existantes. Cela permet à Qubit Pharmaceuticals de résoudre 3 problèmes clés dans ce domaine : la qualité des prévisions, l'interprétabilité des résultats et la rapidité des simulations générant une amélioration et une accélération des pipelines thérapeutiques. Robert Marino, Président de Qubit Pharmaceuticals, a ajouté :
« Avec Atlas et les autres outils que nous développons, nous visons à réduire de moitié le temps et le coût du développement préclinique.

*Et le 30 juin 2021, le **crédit Agricole CIB** annonce le lancement de son projet d'informatique quantique pour améliorer ses algorithmes financiers. La banque va concevoir et développer de nouvelles approches pour améliorer ses algorithmes employés sur les marchés de capitaux et pour la gestion des risques. Elle associera l'informatique traditionnelle et l'informatique quantique. Pour cela, Crédit Agricole noue un partenariat avec les entreprises technologiques Pasqal et Multiverse Computing.*



POUR CONCLURE

La triple course à la suprématie quantique, qu'elle se situe en termes de puissance, d'usages, de défense et de sécurisation est selon nous le plus grand boulversement que notre industrie ait connu depuis l'avènement de micro-ordinateurs. De nouveaux acteurs vont émerger et les entreprises pionnières en la matière prendront un avantage stratégique prépondérant.

Source photos : Unsplash.com

vous avez des questions ?
Envoyez-nous un mail à

contact@syd.fr

Syd
DIGITAL CARE