Une nouvelle ère de l'informatique

A new era of Information Technology with Quantum Computing

Olivier Hess[1], Jean-Michel Torres[2], Xavier Vasques[3]

[1] IBM Q France Leader & IBM Q Ambassador
[2] IBM Q France
[3] Director of European IBM Systems Center | Montpellier

RÉSUMÉ. L'ensemble des éléments rassemblés ci-dessous s'organise en 4 rubriques. OpenScience remercie remercie les auteurs pour le strict respect qu'ils accorderont à ces dispositions. La taille de ce résumé ne doit pas dépasser une dizaine de lignes. Il est à composer en Arial 9, interligné 13 points.

ABSTRACT. The basics of quantum computing are explained based on quantum mechanics superposition and entanglement effects. The technological characteristics of the quantum computers currently available are described, as well as the programming environment qiskit. The foreseeable fields of application of quantum computing are then reviewed.

MOTS-CLÉS. technologie calcul, quantique informatique, quantique physique, quantique qubit qiskit, cas d'usage IBM.

KEYWORDS. technology quantum, computing quantum, mechanics qubit qiskit, usecase IBM.

Introduction

C'est à partir du début des années 1980, sous l'impulsion du physicien et prix Nobel Richard Feynman que germe l'idée de la conception et du développement d'ordinateurs quantiques : Là où un ordinateur « classique » fonctionne avec des bits de valeurs 0 ou 1, l'ordinateur quantique utilise les propriétés fondamentales de la physique quantique et repose sur des « quantum bits (qubits) ».

Au-delà de cette prouesse technologique, l'informatique quantique ouvre la voie au traitement de tâches informatiques dont la complexité est hors de portée de nos ordinateurs actuels.

L'objectif de cet article est de faire un tour d'horizon de cette technologie. Quels sont les principes du calcul quantique ? pour quelles applications ? où en sommes-nous ? où allons-nous et pour quelles perspectives ?

De l'émergence de la Mécanique Quantique au développement d'une "Théorie de l'information Quantique".

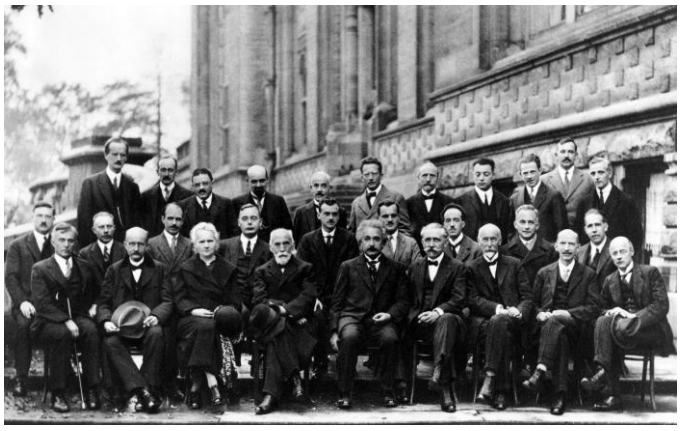

Figure 1. *Congrès de Solvay 1927*

Au début du XX^{ième} siècle les théories de la physique dite « classique » sont dans l'impossibilité d'expliquer certains problèmes observés par les physiciens. Elles doivent donc être reformulées et enrichies. Sous l'impulsion des scientifiques, elle va évoluer dans un premier temps vers une « nouvelle mécanique » qui deviendra « mécanique ondulatoire » et finalement « mécanique quantique ».

La mécanique quantique est la théorie mathématique et physique qui décrit la structure fondamentale de la matière et l'évolution dans le temps et dans l'espace des phénomènes de l'infiniment petit.

Une notion essentielle de la mécanique quantique est la dualité « Onde Corpuscule ».

Jusqu'aux années 1890 les physiciens considèrent que le monde est composé par deux types d'objets ou de particules : d'une part celles qui ont une masse (comme les électrons, les protons, les neutrons, les atomes …), et d'autre part celles qui n'en n'ont pas (comme les photons, les ondes …).

Pour les physiciens de l'époque, ces particules sont régies par les lois de la mécanique Newtonienne pour celles qui ont une masse et par les lois de l'Electromagnétisme pour les ondes. Nous disposions donc de deux théories de la « Physique » pour décrire deux types d'objets différents.

La mécanique quantique invalide cette dichotomie et introduit l'idée fondamentale de la « dualité onde corpuscule » : Une particule de matière ou une onde doivent être traitées par les mêmes lois de la physique : c'est l'avènement de la mécanique ondulatoire qui deviendra quelques années plus tard la mécanique quantique.

De grands noms sont associés au développement de la mécanique quantique comme par exemple Niels Bohr, Paul Dirac, Albert Einstein, Werner Heisenberg, Max Planck, Erwin Schrödinger et bien d'autres.

Max Planck et Albert Einstein, en s'intéressant au rayonnement émis pas un corps chauffé et à l'effet photoélectrique, furent les premiers à comprendre que les échanges d'énergie lumineuse ne pouvaient se faire que par « paquet » et non pas avec n'importe quelle valeur. Un peu comme un escalier qui ne permet de monter que de la hauteur d'une marche (ou plusieurs) mais pas d'atteindre une hauteur quelconque entre deux marches. D'ailleurs, Albert Einstein obtient le prix Nobel de physique suite à la publication de sa théorie sur l'aspect quantifié des échanges d'énergie en 1921, et non pas pour la théorie de la relativité restreinte.

Niels Bohr étendit les postulats quantiques de Planck et d'Einstein de la lumière à la matière, en proposant un modèle reproduisant le spectre de l'atome d'hydrogène. Il obtient le prix Nobel de physique en 1922, en définissant un modèle de l'atome qui dicte le comportement des quanta de lumière. En passant d'un palier d'énergie à un autre inférieur, l'électron échange un quantum d'énergie. Pas à pas, des règles furent trouvées pour calculer les propriétés des atomes, des molécules et de leurs interactions avec la lumière.

De 1925 à 1927, toute une série de travaux de plusieurs physiciens et mathématiciens donna corps à deux théories générales applicables à ces problèmes :

- La mécanique ondulatoire de Louis de Broglie et surtout de Erwin Schrödinger ;
- La mécanique matricielle de Werner Heisenberg, Max Born et Pascual Jordan.

Ces deux mécaniques furent unifiées par Erwin Schrödinger du point de vue physique, et par John von Neumann du point de vue mathématique. Enfin, Paul Dirac formula la synthèse ou plutôt

la généralisation complète de ces deux mécaniques, que l'on nomme aujourd'hui la mécanique quantique. L'équation fondamentale de la mécanique quantique est l'équation de Schrödinger.

$$H(t)\,|\,\psi(t)\rangle = i\hbar\frac{d}{dt}\,|\,\psi(t)\rangle$$

De la Mécanique Quantique au développement d'ordinateurs quantiques

Avant d'aborder le développement d'une "Théorie de l'information Quantique" , revenons sur le fonctionnement d'un ordinateur standard, et la « Théorie de l'information classique », celle qui régit le fonctionnement des ordinateurs tels que nous les connaissons aujourd'hui.

Figure 2. *Ordinateurs "classiques" dans un centre de calcul (crédit : IBM Research)*

Les premiers ordinateurs binaires furent construits dans les années 40 : Colossus (1943) puis ENIAC (IBM - 1945). Colossus a été conçu pour déchiffrer des messages secrets allemands et l'ENIAC conçu pour calculer des trajectoires balistiques. L'ENIAC (acronyme de l'expression anglaise Electronic Numerical Integrator And Computer), est en 1945 le premier ordinateur entièrement électronique construit pour être « Turing-complet » : il peut être reprogrammé pour résoudre, en principe, tous les problèmes calculatoires. L'ENIAC a été programmé par des femmes, dites les « femmes ENIAC ». Les plus célèbres d'entre elles étaient Kay McNulty**,** Betty Jennings**,** Betty Holberton**,** Marlyn Wescoff**,** Frances Bilas et Ruth Teitelbaum**.** Ces femmes avaient auparavant effectué des calculs balistiques sur des ordinateurs de bureau mécaniques pour l'armée. L'ENIAC pèse alors 30 tonnes, occupe une surface de 72 m^2 et consomme 140 kilowatts.

Quelle que soit la tâche effectuée par un ordinateur, le processus sous-jacent est toujours le même : une instance de la tâche est décrite par un algorithme qui est traduit en une suite de 0 et de 1, pour donner lieu à l'exécution dans le processeur, la mémoire et les dispositifs d'entrée/sortie de l'ordinateur. C'est la base du calcul binaire qui en pratique repose sur des circuits électriques dotés de transistors pouvant être dans deux modes : « ON » permettant au courant de passer et « OFF » le courant ne passe pas.

A partir de ces 0 et ces 1 on a donc développé au cours des 80 dernières années une théorie de l'information classique construite à partir d'opérateurs Booléens (XAND, XOR), de mots (Octets), et une arithmétique simple basée sur les opérations suivantes : « 0+0=0, 0+1=1+0=1, 1+1=0 (avec une retenue), et vérifier si 1=1 , 0=0 et $1 \neq 0$).

Bien entendu à partir de ces opérations il est possible de construire des opérations beaucoup plus complexes que les ordinateurs peuvent effectuer des millions de milliards de fois par seconde pour les plus puissants d'entre eux. Tout cela est devenu tellement « naturel » que l'on oublie totalement que chaque transaction sur un serveur informatique, sur un PC, une calculette, un smartphone se décompose en ces « opérations binaires élémentaires »….

Dans un ordinateur, ces 0 et 1 sont contenus dans des « BInary digiTs » ou « bits » qui représentent la plus petite quantité d'information contenue dans un système informatique.

Pour un ordinateur quantique le « qubit (quantum bit) » est l'entité de base, représentant, à l'instar du « bit » la plus petite entité permettant de manipuler de l'information. Il possède deux propriétés fondamentales de la Mécanique Quantique : **Superposition & Intrication.**

La superposition quantique :

Un objet quantique (à l'échelle microscopique) peut exister dans une infinité d'états (tant qu'on ne mesure pas cet état). Un qubit peut donc exister dans n'importe quel état entre 0 et 1. Les qubits peuvent prendre à la fois la valeur 0 et la valeur 1, ou plutôt « une certaine quantité de 0 et une certaine quantité de 1 », comme une combinaison linéaire de deux états notés |0> et |1>, avec les coefficients **α** et **β**.

Donc là où un bit classique ne décrit « que » 2 états (0 ou 1), le qubit peut en représenter une « infinité » !! C'est un des avantages potentiels du calcul quantique du point de vue de la théorie de l'information.

La superposition d'états est représentée sous la forme suivante :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

On peut se faire une idée de la superposition d'états en utilisant l'analogie du ticket de loterie : **un ticket de loterie est soit gagnant, soit perdant**… une fois que l'on connaît le résultat du jeu. Par contre, avant le tirage, ce ticket **n'était ni gagnant, ni perdant**. Il avait simplement une certaine probabilité d'être gagnant et une certaine probabilité d'être perdant, il était en quelque sorte gagnant et perdant à la fois (plutôt beaucoup plus perdant que gagnant, en fait). Dans le monde quantique, toutes les caractéristiques des particules peuvent être sujettes à cette indétermination : par exemple, la position d'une particule est incertaine. Avant la mesure, la particule n'est ni au point A, ni au point B. Elle a une certaine probabilité d'être au point A et une certaine probabilité d'être au point B. Cependant, après la mesure, l'état de la particule est bien défini : elle est au point A ou au point B.

L'intrication quantique :

L'intrication est une autre propriété étonnante de la physique quantique. Lorsque l'on considère un système composé de plusieurs qubits, il peut leur arriver de « lier leur destin » c'est-à-dire de ne pas être indépendants l'un de l'autre même s'ils sont séparés dans l'espace (alors que les bits « classiques » sont complètement indépendants les uns des autres). C'est ce que l'on appelle l'intrication quantique. Si l'on considère un système de deux qubits intriqués alors la mesure de l'état d'un de ces deux qubits nous donne une indication immédiate sur le résultat d'une observation sur l'autre qubit.

Pour illustrer naïvement cette propriété on peut là aussi utiliser une analogie : imaginons deux ampoules, chacune dans deux maisons différentes. En les intriquant, il devient possible de connaître

l'état d'une ampoule (allumée ou éteinte) en observant simplement la seconde, car les deux seraient liées, intriquées. Et cela, immédiatement et même si les maisons sont très éloignées l'une de l'autre (dans des galaxies différentes peut-être).

Ce phénomène d'intrication permet de décrire des corrélations entre les qubits. Si on augmente le nombre de qubits, le nombre de ces corrélations augmente exponentiellement : pour N qubits il y a 2^n corrélations. Si n est grand alors 2^n est un nombre gigantesque. A titre d'exemple, avec 300 qubits, on aurait besoin, pour écrire toutes ces corrélations d'autant de chiffres qu'il n'y a d'atomes dans l'univers visible ! C'est cette propriété qui confère à l'ordinateur quantique la possibilité d'effectuer des manipulations sur des quantités gigantesques de valeurs, quantités hors d'atteinte d'un ordinateur classique.

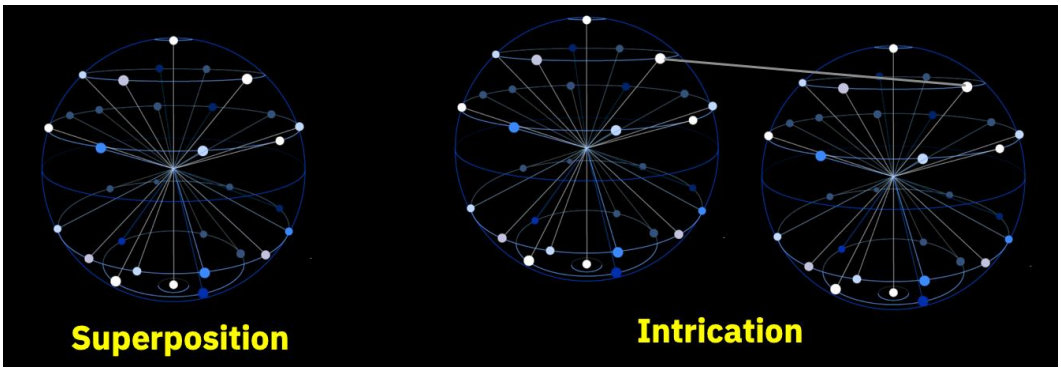

Figure 3. *Superposition et intrication quantiques (crédit : IBM Research)*

La construction d'un ordinateur quantique : une série de défis technologiques.

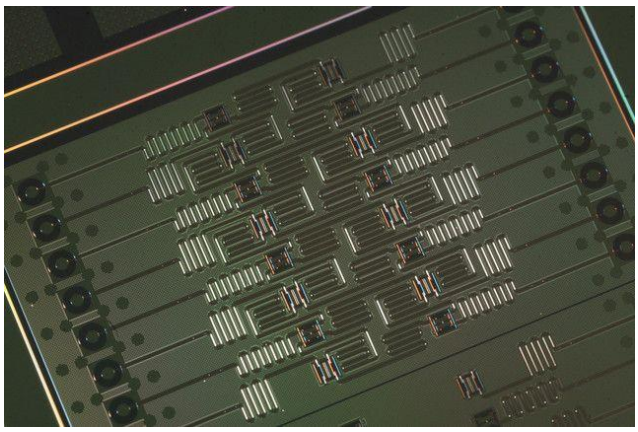

Figure 4 *Qubits supraconducteurs d'IBM (crédit : IBM Research)*

Construire un ordinateur quantique va donc reposer sur la capacité de développer une puce informatique (« un chip ») sur laquelle sont gravées des qubits. Du point de vue technologique, il existe plusieurs manières de constituer des qubits, ils peuvent être faits d'atomes, de photons, d'électrons, de molécules ou de métaux supraconducteurs.

Dans la plupart des cas, pour pouvoir fonctionner, un ordinateur quantique a besoin de conditions extrêmes pour opérer comme par exemple des températures proches du zéro absolu.

Le choix d'IBM est d'utiliser des qubits « Supraconducteurs », construits avec des oxydes d'aluminium (on appelle aussi cette technologie : « qubits transmons »). Comme évoqué ci-dessus pour permettre et garantir les effets quantiques (superposition et intrication) les qubits doivent être

refroidis à une température aussi proche que possible du zéro absolu (soit environ -273° C). Chez IBM ce seuil de fonctionnement est d'environ 20 milliKelvin !

Pour permettre un fonctionnement optimal dans ces conditions extrêmes, la plupart des composants sont … en or !

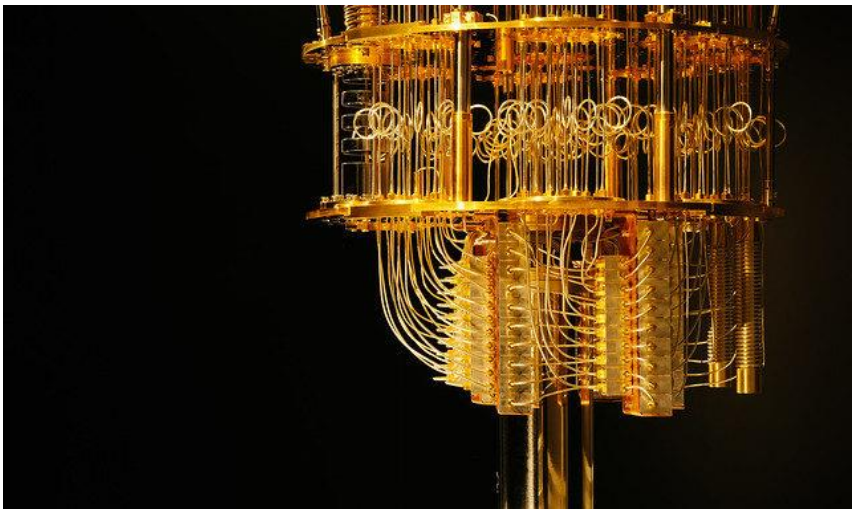

Figure 5. *Machine IBM à 53 qubits (crédit : IBM Research)*

IBM a démontré la capacité de concevoir un qubit unique en 2007 et en 2016 a annoncé la mise à disposition dans le Cloud d'un premier système physique opérationnel doté de 5 qubits et d'un environnement de développement « QISKit » (Quantum Information Science Kit), permettant de concevoir, tester et optimiser des algorithmes pour des applications commerciales et scientifiques. Mise en ligne dès le mois de mai, l'initiative « IBM Q Experience » constitue une première dans le monde industriel.

L'offre actuelle d'IBM repose sur des systèmes physiques à 20 qubits et 53 qubits. La volonté d'IBM est clairement de favoriser l'adoption du calcul quantique et d'accompagner nos clients et partenaires dans cette révolution technologique. Ainsi depuis 2017, IBM construit un écosystème d'entreprises, d'universités, d'organismes de recherche et de startups : le « IBM Q Network » qui comporte plus de 80 membres.

Cette offre dans le Cloud donne également accès de façon gratuite à un émulateur à 32 qubits ainsi qu'un certain nombre de systèmes à 5 et 14 qubits.

Augmenter le nombre de qubits ? Oui mais cela ne suffit pas :

Dans la course au développement d'ordinateurs quantiques, au-delà des qubits, d'autres composantes sont essentielles. On parle de « volume quantique » comme une mesure pertinente de la performance et des progrès technologiques. On définit aussi « l'avantage quantique » c'est le point à partir duquel les applications du calcul quantique offriront un avantage pratique significatif et démontrable qui dépasse les capacités des seuls ordinateurs classiques. Le concept de volume quantique a été introduit par IBM en 2017. Il commence à se généraliser auprès d'autres constructeurs.

Le volume quantique est déterminé par divers facteurs, dont le nombre de qubits, la connectivité, le temps de cohérence, ainsi que la prise en compte des erreurs sur les portes quantiques et des erreurs de mesure, la connexion entre qubits et l'amélioration des couches logicielles.

Et bien évidemment, il faut pouvoir exécuter des tâches sur ces machines, c'est pourquoi IBM a développé une bibliothèque de programmation spécifique appelée QISKit (Quantum Information Science Kit). Il s'agit d'une librairie open-source pour le langage Python, disponible sur qiskit.org. Son développement est très actif, l'ensemble des contributeurs, dont IBM, fait régulièrement évoluer les fonctionnalités de cet environnement de programmation.

```
%matplotlib inline
from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit, execute, Aer
from qiskit.tools.visualization import plot_histogram
backend = Aer.get_backend('qasm_simulator')

# define circuit
qr = QuantumRegister(1)
cr = ClassicalRegister(1)
circ = QuantumCircuit(qr,cr)
circ = QuantumCircuit(qr,cr)
# H X H exemple:
circ.h(qr[0])
circ.x(qr[0])
circ.h(qr[0])
circ.measure(qr,cr)
# see the circuit
circ.draw(output='mpl')
# execution & display
resultat = execute(circ,backend,shots=1024).result()
d = resultat.get_counts(circ)
plot_histogram(resultat.get_counts(circ))
```

Figure 6 *Un programme écrit avec Python et QISKit*

Le calcul quantique, pour quoi faire ?

Un ordinateur quantique n'a pas pour objectif de rendre les mêmes services qu'un ordinateur classique. Quels sont donc les cas de calculs, les classes de problèmes qui vont tirer partie de ces futurs ordinateurs ?

Commençons par quelques exemples simples :

Pour un ordinateur classique faire le produit (multiplication) de deux nombres et obtenir le résultat est une opération très simple : n'importe quelle calculette sait le faire très bien : 7*3 = 21, 6739*892721 = 6016046819 ... et cela même pour de très grands nombres … Mais le problème inverse est nettement plus complexe. Connaissant un grand nombre (par exemple 7859324261 il est très compliqué de trouver P et Q tel que : P x Q = 7859324261.

C'est cette difficulté qui est à la base des techniques de cryptographie courantes. Pour un tel problème, à titre d'exemple on estime qu'un problème qui durerait 1025 jours sur un ordinateur classique, pourrait être résolu en quelques dizaines de secondes sur une machine quantique. On parle pour ce cas d'accélération exponentielle.

Prenez l'exemple d'un labyrinthe. Pour trouver la sortie, un ordinateur classique va explorer chaque piste les unes après les autres de façon séquentielle.

Avec une machine quantique la superposition et l'intrication font que …

– L'ensemble des chemins possibles peuvent être explorés simultanément (superposition),

– Dès que la solution est trouvée (chemin qui conduit à la sortie) la réponse est alors communiquée à tous les autres chemins (intrication) et le problème s'arrête.

La résolution est ainsi potentiellement bien plus rapide qu'avec un ordinateur et un algorithme classique.

Un des domaines dans lequel le calcul quantique pourra apporter les premières contributions significatives est celui de la science des matériaux et de la chimie.

En effet, un ordinateur quantique imite la manière dont la nature « traite » l'information, lui permettant de simuler, de comprendre et améliorer notre compréhension de la nature comme les molécules et leurs interactions ouvrant la possibilité de très grandes découvertes en sciences des matériaux. Des nouveaux types de matériaux seront également possibles comme par exemple des supraconducteurs à température ambiante, ce qui pourrait à l'avenir avoir un impact gigantesque sur les problèmes d'énergie dans le monde.

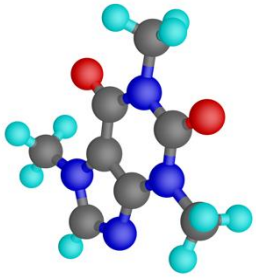

Figure 7. *La molécule de caféine*

Prenons un autre exemple : aucun ordinateur classique au monde ne peut calculer de façon exacte (c'est-à-dire sans aucune approximation) l'énergie de la molécule de caféine, pourtant de taille moyenne avec une quarantaine d'atomes, c'est un problème trop complexe... Aujourd'hui les ordinateurs quantiques sont utilisés pour traiter des problèmes de chimie simples c'est à dire avec un petit nombre d'atomes mais l'objectif est bien sûr de pouvoir adresser des molécules beaucoup plus complexes.

A un peu plus long terme, c'est l'ensemble des domaines où le calcul fait appel à des algorithmes complexes au sens où le temps de calcul ou de la taille mémoire sont tels qu'il n'est pas faisable dans un temps « raisonnable » (par exemple il n'est pas raisonnable, ni utile de passer 10 000 ans pour trouver le code d'une carte de paiement).

Dans ces catégories de problème « éligibles aux ordinateurs quantiques » on trouve beaucoup de cas d'optimisation, dans les domaines logistiques (plus court chemin), de la finance (estimation de risques, évaluation de portefeuilles d'actifs), du martketing (« maxcut », « clique »), de l'industrie et de la conception de systèmes complexes (Satisfiabilité, parcours de graphes).

Le domaine de l'intelligence artificielle est également un champ de recherche actif, et des méthodes d'apprentissage pour les réseaux de neurones artificiels commencent à voir le jour, c'est donc l'ensemble des activités humaines concernées par le traitement de l'information qui sont potentiellement concernées par l'avenir du calcul quantique.

Il y a enfin le domaine de la Cybersécurité et de la cryptographie : l'algorithme de Shor a été démontré voici plus de 20 ans et il pourrait rendre fragile le chiffrage communément utilisé sur internet, mais d'une part il faudra attendre que les machines quantiques soient suffisamment «puissantes» pour traiter ce type de calcul particulier (on parle d'horizon au-delà de dix ans), et d'autre part des solutions de cryptage sont déjà connues et démontrées hors d'atteinte de cet algorithme.

D'ailleurs il se trouve que parmi ces solutions, ce sont aussi des technologies quantiques qui permettent de générer et de transporter des clefs de cryptage de manière absolument inviolable.

De ce fait le domaine des technologies quantiques et du calcul quantique en particulier est considéré comme un enjeu stratégique, et l'Europe, la France et bien d'autres pays soutiennent les efforts de recherche dans ce domaine.

Pour la France, IBM a choisi de créer un centre d'expertise sur le calcul quantique au sein de son site de Montpellier, pour servir de support au développement du calcul quantique en France et à soutenir l'offre d'IBM sur le marché national.

Dans cette logique un projet de collaboration a été mis en place avec le soutien de la région Occitanie avec l'Université de Montpellier : « Projet QuantUM » (https://www-03.ibm.com/press/fr/fr/pressrelease/54572.wss)

Figure 8. *IBM Q System One disponible sur le Cloud (crédit : IBM Research)*

Conclusion

Il résulte de cette exploration que l'informatique quantique représente le début d'une aventure. Elle connait actuellement un rythme d'innovation accéléré car les technologies permettent à présent d'expérimenter les théories imaginées depuis le début des années 1970.

Certains domaines comme la communication quantique ou la métrologie quantique font d'ores et déjà l'objet d'industrialisation et de commercialisation. Le calcul quantique proprement dit est en train d'approcher de très près le moment où il aura l'avantage dans certains cas sur les ordinateurs dits classiques. La communauté s'affaire à développer les systèmes physiques, les environnements de programmation, et les algorithmes, avec des résultats spectaculaires semaine après semaine.

Une chose est certaine : cette aventure fait partie des domaines où l'humanité démontre sa motivation et sa capacité à continuer à comprendre les secrets de la nature et à mettre en œuvre des technologies de plus en plus complexes.

Le chemin promet d'être passionnant !

"The effort to understand the universe is one of the very few things which lifts human life a little above the level of farce and gives it some of the grace of tragedy." (Steven Weinberg)