FÉVRIER 2020

Cigref
RÉUSSIR
LE NUMÉRIQUE

Informatique quantique

Comprendre le Quantum Computing pour se préparer à l'inattendu

Édito

Utopie il y a encore quelques années, l'informatique quantique commence à prendre *racine* dans les esprits. Elle porte la promesse de succéder à la loi de Gordon Moore (cofondateur d'Intel) qui prédisait un doublement des capacités de calcul tous les ans … jusqu'à la limite physique de l'atome.

L'atome, c'est bien le point de départ de l'informatique quantique qui utilise des ressources nanométriques (10^{-9}) afin de résoudre les problèmes que les calculateurs actuels ne peuvent aborder.

Les domaines d'application de l'informatique quantique sont aussi variés que la cryptographie, la métrologie, l'optimisation, la simulation, l'analyse des données et l'intelligence artificielle, au travers d'un futur « calculateur quantique universel ». Porté par plusieurs grands acteurs tels que Google, IBM, Microsoft, Atos, l'écosystème du *quantum computing* comprend également de nombreuses startups, surtout nord-américaines mais aussi françaises, et commence à se développer.

Alors que les entreprises aujourd'hui se transforment profondément pour pouvoir anticiper et s'adapter à l'inattendu technologique, elles ne peuvent pas ignorer la révolution quantique qui va sans aucun doute bouleverser l'informatique : de séquentiel puis parallèle, le calcul va devenir « cooccurrent[1] », impactant la programmation et les algorithmes, mais aussi les applications et la sécurité de l'information, faisant naître de nouveaux usages.

Les entreprises doivent donc se préparer à cette rupture technologique qui s'annonce majeure et dont les premiers effets tangibles sont annoncés d'ici 5 à 10 ans[2].

Cette rupture se traduira par de nouvelles manières de penser, par de nouvelles méthodes de travail et de nouveaux outils, ainsi que de nouvelles compétences, tous encore inconnus. Les nouveaux usages qui seront à inventer changeront certainement aussi les *business models* des entreprises comme les organisations qui devront, de nouveau, se transformer pour s'adapter.

Jean-Michel ANDRÉ

DSI du Groupe SEB, Pilote du groupe de travail Cigref

[1] Si une cooccurrence est l'apparition simultanée de deux ou plusieurs éléments ou classes d'éléments liés entre eux, généralement dans un discours, il est alors possible d'imaginer un empilement de deux ou plusieurs instructions ou classes de fonctions, liées entre elles, issues d'un langage de programmation quantique et dont l'exécution simultanée formerait un programme « quantique ».

[2] Ce qui est court en termes de perception : rappelons-nous que Gmail, première messagerie sur le Cloud, a été lancé en 2005, il y a 15 ans.

Remerciements

Nos remerciements vont à Jean-Michel ANDRÉ, DSI du Groupe SEB qui a piloté cette réflexion, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail Cigref :

Nicolas BOUVIER – EIFFAGE

Blaise BRIGAUD - AIR FRANCE KLM

Eric GOUNOT - DASSAULT AVIATION

Samuel HOLLER - RENAULT

Paul LAJOIE-MAZENC – EDF

Bernard LOISEAU - GROUPE SEB

Mohamed MARFOUK - LVMH

Emmanuel MONZIES - GROUPE PSA

Nicolas PERRIN - BANQUE DE FRANCE

Marc PORCHERON - EDF

Sophie POURCHET - FONDATION DE FRANCE

Nous remercions également les intervenants qui ont contribué par leurs apports à notre réflexion :

Mehdi BOZZO-REY – *Global Offering Manager*, IBM Q *startups*

Philippe DULUC – Directeur technique Big Data & Sécurité, Atos

Olivier EZRATTY – Consultant, auteur et conférencier

Olivier HESS – IBM Q Hub France *Leader*, IBM Q *Ambassador*

Sarah LAMOUDI – *Technology Strategist and Advisor* (AI, blockchain, Quantum and Fintech)

Alain SARLETTE – *Senior Researcher* au QUANTIC Lab de l'INRIA

Sébastien TANZILLI – Directeur de recherche au CNRS, Responsable de l'équipe Photonique et information quantiques (PIC) à l'INPHYNI (Institut de Physique de Nice)

.

Ce document a été rédigé par Frédéric LAU, Directeur de mission au Cigref, avec la contribution de Jean-Michel ANDRÉ, DSI du Groupe SEB et des participants aux travaux.

Table des matières

Table des figures

1. Pourquoi s'y intéresser dès aujourd'hui ?

L'innovation est bien souvent basée sur des technologies existantes ou dont les fondements sont, sinon maîtrisés, *a minima* compréhensibles.

L'informatique quantique n'est pas cela.

Elle est difficilement compréhensible et remet en question les principes de logique et d'informatique en vigueur. Encore à un stade de recherche, les technologies qu'elle met en œuvre ne viennent pas de l'électronique, science de l'ingénieur, mais des principes de la mécanique quantique, science du physicien, appliqués à la théorie de l'information[3]. Ces technologies sont encore en phase de recherche et développement et aucune n'a véritablement fait la preuve de sa supériorité sur les autres.

Leur évolution rapide permet de faire des choses irréalisables il y a quelques années encore. Même si les progrès réels sont difficilement mesurables, le nombre de projets quantiques augmente et les niveaux de performances progressent. Une des premières révolutions a permis la mise en œuvre des propriétés quantiques au sein d'objets de la vie courante comme le laser ou les structures électroniques. Ces technologies ont permis, par exemple, la miniaturisation de composants au niveau nanométrique (10^{-9}). Aujourd'hui nous sommes à l'aube d'une nouvelle révolution qui concerne la mesure et le contrôle quantique au niveau des particules.

L'informatique quantique ne remplacera pas l'informatique classique. Elle la complétera dans un certain nombre de domaines : cryptologie, métrologie, simulation et calcul. Et la réalisation des promesses de l'informatique quantique aura un impact certain sur le SI des entreprises et au-delà sur leur modèle d'affaires. Nous quittons l'utopie pour entrer dans le monde du réel et cela ne va pas se faire sans bouleversements :

- Technologiques : les outils mis en œuvre sont très différents de ceux de l'informatique classique.
- *Business* : les promesses (puissance, algorithmique, sécurité) vont certainement changer de nombreux *business models* et processus métiers de l'entreprise.
- Ressources humaines : les compétences nécessaires aux informaticiens du quantique ne seront pas celles enseignées actuellement.
- Culturelles : on ne pense pas « quantique » comme on pense « informatique ».

On pressent donc que l'informatique quantique va transformer les systèmes d'information des entreprises et leur usage, la culture d'entreprise et les compétences des équipes informatiques. Et il

[3] Théorie de l'information de Shannon : https://fr.wikipedia.org/wiki/Th%C3%A9orie_de_l%27information

faut que les entreprises soient prêtes (en termes de compréhension, compétences, et culture) à se transformer le jour où l'informatique quantique sera *a minima* effective et opérationnelle.

L'accès à des ordinateurs quantiques hébergés dans le Cloud permet d'expérimenter des algorithmes hybrides, c'est-à-dire avec un mélange d'informatique classique et quantique. Il sera donc important d'identifier les cas où l'informatique quantique sera applicable de manière utile.

Le *quantum computing* s'inscrit en continuité de la virtualisation des infrastructures du SI qui se développe actuellement. L'architecture globale des SI ne sera peut-être pas modifiée, mais les problèmes que le SI pourra résoudre seront d'un niveau très différent. Comme par exemple, faire tourner des algorithmes d'optimisation à travers un cloud quantique. Et dans 10-15 ans, des problèmes complexes devraient pouvoir être résolus en faisant appel ponctuellement à des machines quantiques en ligne.

L'organisation des processus internes peut aussi être bousculée : par exemple le temps de calcul des éléments statistiques liés au big data risque d'être réduit, obligeant les entreprises à être beaucoup plus réactives. Ce qui aura pour conséquence un remodelage des processus métiers qui pourraient alors être raccourcis avec un impact sur les équipes concernées.

Au même titre qu'avec l'intelligence artificielle ou le big data, technologies qui se sont très vite développées et dans lesquelles il a fallu acquérir rapidement une maîtrise, l'informatique quantique nécessitera de nouvelles compétences qui seront certainement moins informatiques que scientifiques, mais tout de même plus proches de celles de l'ingénieur que du physicien. Néanmoins, au vu de la complexité du domaine, on peut aussi penser que se développeront des langages de haut niveau qui « lisseront » la complexité (mais ce ne sera pas tout de suite) ou bien que la partie véritablement quantique sera déléguée à des fournisseurs sur un cloud, évitant ainsi à l'entreprise d'être obligée de développer des compétences extrêmement pointues et difficiles à acquérir.

Comme pour l'intelligence artificielle et le big data, il faudra aussi éveiller au *quantum computing* des populations qui, sans être expertes du domaine, devront utiliser des applications quantiques. Il ne faudra donc pas sensibiliser, informer et/ou former que les populations techniques, mais également les populations métiers pour leur faire prendre conscience de ce qu'il est possible, ou pas, de faire et où se trouve la valeur ajoutée, notamment *business* : il s'agit de leur faire comprendre la philosophie du quantique plus que son fonctionnement et sa puissance.

L'informatique quantique ne permettra donc pas de résoudre n'importe quoi, n'importe comment, elle impliquera surtout de réfléchir autrement !

Ce changement qui s'annonce majeur doit donc être démystifié et compris dès aujourd'hui par les dirigeants. Et c'est pour aider les entreprises à se préparer à l'inattendu de cette informatique quantique, que le Cigref a monté un groupe de travail sur ce sujet.

La réflexion menée dans ce groupe de travail, piloté par Jean-Michel André, DSI du Groupe Seb, vise à sensibiliser et vulgariser les principes de l'informatique quantique afin de comprendre la portée de ses promesses, ses enjeux et ses opportunités. Et permettre aux entreprises d'anticiper, de se projeter et d'investir sans retard pour le futur.

2. Un mouvement qui accélère

Il ne s'agit pas ici de détailler l'histoire de l'informatique quantique[4]. Mais si l'on souhaite sortir de l'utopie, il parait néanmoins nécessaire de montrer sur quelles bases historiques les technologies quantiques s'appuient, les moments qui l'ont faite progresser, et prendre conscience de l'accélération qui s'est opérée ces 10 dernières années.

L'informatique quantique commence au début du XX° siècle avec les premiers travaux sur la théorie des quantas, initiée par le physicien allemand Max Planck en 1900. Cette théorie a permis de faire le lien entre la physique classique et la physique quantique. C'est en 1925 que les principes de la mécanique quantique ont ensuite été développés par Albert Einstein, Niels Bohr, Louis de Broglie, Werner Heisenberg et bien d'autres scientifiques.

1935

En 1935, Albert Einstein et deux autres physiciens, Boris Podolsky et Nathan Rosen, publient un article qui décrit une « expérience de pensée » pour démontrer que la mécanique quantique, telle que définie à l'époque, est incomplète. Pour résumer, la théorie expliquait que si l'on produit un électron et un positron[5] intriqués dans une expérience, la mesure d'une propriété de l'électron est immédiatement répercutée sur le positron qui « le sait immédiatement » même s'il est à des millions de kilomètres. Einstein spéculait qu'étant donné que ce principe quantique violait les principes de localité[6] et de réalité[7], et que la nature devant être par hypothèse réaliste et locale, la mécanique quantique devait être incomplète. C'est le paradoxe EPR[8] (Einstein-Podolsky-Rosen).

Pour Einstein, cette transmission d'information « plus rapide que la lumière » était inacceptable : il devait exister des variables cachées qui « donnent l'impression » d'une communication immédiate.

[4] Pour cela, lire le travail complet d'Olivier Ezratty : https://www.oezratty.net/wordpress/2018/ebook-pour-comprendre-informatique-quantique/
[5] Positron : antiparticule, de charge électrique positive, associée à l'électron, de charge électrique négative.
[6] Localité : principe selon lequel des objets distants ne peuvent avoir une influence directe l'un sur l'autre.
[7] Réalité : pour qu'une grandeur physique soit réelle, il suffit qu'il soit possible de la prédire avec certitude, sans perturber le système.
[8] https://fr.wikipedia.org/wiki/Paradoxe_EPR

1964

En 1964, le physicien nord-irlandais John Bell propose le principe d'une expérience qui permet de résoudre ce problème. Il formalise la question par des « inégalités[9] », dites de Bell, qui sont évaluées au cours de l'expérience. Si l'inégalité n'est pas respectée, alors le résultat de l'expérience ne peut pas être expliqué par l'existence de variables cachées, et il faut se résoudre à admettre le caractère non local de la nature qu'Einstein refusait. L'état des technologies de l'époque ne permettra de réaliser cette expérience que dans les années 1980 : c'est un scientifique français, Alain Aspect[10] qui la réalisera et montrera que les inégalités de Bell sont bien violées, confirmant ainsi le caractère non local de la physique quantique, que la mécanique quantique était donc bien complète, et que, par conséquent, l'une des hypothèses de base d'Einstein était fausse. Avec cette expérience, Alain Aspect démontrera que le phénomène d'intrication théorisé par Albert Einstein, mais auquel il ne croyait pas, était valide. Nous verrons plus loin dans ce document[11] que l'intrication fait partie des éléments de base de l'informatique quantique.

1981

Les années 1980 sont importantes dans le monde de l'informatique quantique. En effet, en 1981 se déroule la première conférence du MIT (*Massachusetts Institute of Technology*) sur ce sujet. C'est lors de cette conférence qui rassemblait de nombreux scientifiques et physiciens renommés, que nait l'idée d'encoder de l'information dans les états quantiques de la matière.

1 Freeman Dyson
2 Gregory Chaitin
3 James Crutchfield
4 Norman Packard
5 Panos Ligomenides
6 Jerome Rothstein
7 Carl Hewitt
8 Norman Hardy
9 Edward Fredkin
10 Tom Toffoli
11 Rolf Landauer
12 John Wheeler
13 Frederick Kantor
14 David Leinweber
15 Konrad Zuse
16 Bernard Zeigler
17 Carl Adam Petri
18 Anatol Holt
19 Roland Vollmar
20 Hans Bremerman
21 Donald Greenspan
22 Markus Buettiker
23 Otto Floberth
24 Robert Lewis
25 Robert Suaya
26 Stan Kugell
27 Bill Gosper
28 Lutz Priese
39 Madhu Gupta
30 Paul Benioff
31 Hans Moravec
32 Ian Richards
33 Marian Pour-El
34 Danny Hillis
35 Arthur Burks
36 John Cocke
37 George Michaels
38 Richard Feynman
39 Laurie Lingham
40 Thiagarajan
41 ?
42 Gerard Vichniac
43 Leonid Levin
44 Lev Levitin
45 Peter Gacs
46 Dan Greenberger

Figure 1 : Physics of Computation Conference - Endicott House MIT - May 6-8, 1981

[9] Les inégalités de Bell sont les relations que doivent respecter les mesures sur des états intriqués dans l'hypothèse d'une théorie déterministe locale à variables cachées.

[10] http://www.cnrs.fr/fr/personne/alain-aspect

[11] Voir le chapitre 5.1. A la base, 3 principes quantiques

Durant cette conférence, le physicien américain Richard Feynman (prix Nobel de physique en 1965) fut le premier à percevoir le potentiel de l'informatique quantique. Les ordinateurs classiques (machines de Turing) n'étant pas assez performants pour simuler les phénomènes quantiques, il suggéra, dans une phrase devenue célèbre, d'utiliser des simulateurs quantiques, plus simples et contrôlables, pour étudier d'autres systèmes quantiques.

> *"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy"*[12]
>
> Richard Feynman - 1981

C'est la première fois que l'on imagine la possibilité d'un ordinateur quantique ou plutôt de sa simulation ! À partir de ce moment, les travaux vont s'accélérer.

1984

Dès 1984, Charles H. Bennett, d'IBM *Research*, qui avait participé dans les années 70 à l'émergence de la théorie de l'information quantique, et Gilles Brassard de l'Université de Montréal, proposent le premier protocole de cryptographie quantique : BB84, mécanisme d'échange de clés quantiques.

1993

En 1993, un groupe international de six scientifiques, dont Charles H. Bennett, confirme les intuitions de la majorité des auteurs de science-fiction en montrant que la téléportation parfaite est « en principe » possible, mais seulement si l'original est détruit (ce qui peut quand même poser problème !).

1995

En 1995, Peter Shor, chercheur en mathématiques appliquées au MIT, démontre que le calcul quantique avec des Qubits permet l'existence d'un algorithme capable de factoriser en un temps record (quelques dizaines de secondes) n'importe quel entier en un produit de deux nombres premiers[13]. En théorie - en pratique c'est une autre histoire - il était donc possible de casser les codes secrets non seulement des banques mais aussi des États et des armées en utilisant l'algorithme de Shor[14].

L'informatique quantique commence alors à intéresser au-delà de la sphère scientifique puisque l'on comprend que la sécurité des systèmes d'information peut être mise à mal. Et l'on voit très rapidement apparaitre de nouveaux acteurs se trouvant hors de la sphère scientifique.

[12] « La nature n'est pas conventionnelle, que diable, et si vous voulez simuler la nature, vous feriez mieux de le faire avec la mécanique quantique, et bon sang c'est un formidable défi, car ça ne semble pas si facile. »

[13] Par comparaison, en 2010 un nombre codé sur 768 bits a été factorisé par un algorithme s'exécutant une année durant sur 425 ordinateurs classiques à 4 cœurs (record non battu à ce jour !)

[14] https://interstices.info/lalgorithme-quantique-de-shor/

1996

En 1996, David Di Vicenzo, chercheur chez IBM, définit les premiers critères permettant d'avoir un processeur quantique :

- les Qubits doivent être intégrables et réalisables en grand nombre,
- il faut disposer de portes quantiques universelles, capables de réaliser tout algorithme,
- il est nécessaire d'avoir une lecture fidèle en une fois,
- il faut pouvoir réinitialiser efficacement chaque Qubit à l'état 0.

Et la même année IBM présente le premier ordinateur quantique à 2 Qubits.

1997

Mais l'ordinateur quantique est extrêmement fragile car de nombreuses erreurs apparaissent dans les calculs en raison de la « décohérence quantique »[15]. Un mécanisme de correction d'erreurs est donc indispensable. En 1997 Alexeï Kitaev, professeur russo–américain de physique à l'Institut de technologie de Californie et chercheur chez Microsoft a eu l'idée de s'inspirer de la topologie, branche des mathématiques qui étudie les objets et leurs propriétés lorsque ceux-ci subissent des déformations, pour proposer une solution à ce problème.

2001

En 2001, les chercheurs d'IBM arrivent à factoriser le nombre 15 en utilisant l'algorithme de Shor sur leur machine quantique.

2011

À partir de 2011, avec l'arrivée de nouveaux acteurs issus pour la plupart du secteur numérique, tout s'accélère encore. En 2011, la société californienne D-Wave présente le premier ordinateur quantique commercial à 128 Qubits.

2012

En 2012, deux physiciens, David Wineland et Serge Haroche, reçoivent le prix Nobel de physique pour leurs travaux sur le contrôle et la mesure des atomes. Le premier a réussi à contrôler l'état quantique d'ions grâce à des photons, et le second a permis d'étudier le phénomène de décohérence quantique en réussissant à mesurer l'information d'un système quantique sans le détruire.

Ce phénomène de décohérence quantique était un problème : plus ce temps est grand, plus il est possible d'exécuter un grand nombre de portes logiques quantiques[16]. Mais si ce temps n'est pas

[15] Voir le chapitre 5.2. Le Qubit, unité de base de l'informatique quantique

[16] Une porte logique, quantique ou électronique, est la brique de base d'un circuit, électronique ou quantique, élémentaire. En électronique, ces portes sont construites à partir de plusieurs transistors connectés de manière adéquate ; en quantique, elles opèrent sur un petit nombre de Qubits.

suffisant pour exécuter l'ensemble des opérations d'un algorithme, cela ne sert à rien. Cette barrière tombe la même année (2012) quand IBM réussit à exécuter des algorithmes quantiques de manière complète.

2015

En 2015 il est démontré que les algorithmes de correction d'erreur fonctionnent et sont utilisables.

2016

En 2016, Microsoft annonce que l'informatique quantique devient une priorité stratégique. Et IBM rend disponible sur un Cloud public le premier ordinateur quantique. À ce jour plus de 100 000 personnes l'ont utilisé et plus de 140 articles ont été publiés à partir de travaux menés sur cette machine.

2017

En 2017, Atos lance la commercialisation de l'ATOS QLM (*Quantum Learning Machine*) permettant de simuler 30 Qubits, Rigetti lance la production de galettes de silicium destinées au calcul quantique, Intel annonce lui aussi la fabrication d'un circuit de calcul quantique à 17 Qubits. IBM réussit à simuler la structure moléculaire de l'hydrure de béryllium (BeH_2) et atteint avec un ordinateur à 50 Qubits le seuil théorique de la suprématie quantique.

2018

En 2018 Intel dévoile à son tour un calculateur à 49 Qubits, puis Google avec Bristlecone, un processeur quantique de 72 Qubits, et Atos une version de 41 Qubits de l'ATOS QLM.

2019

En 2019, IBM dévoile au CES de Las Vegas le premier ordinateur quantique « compact » de 20 Qubits dénommé IBM Q System One. En octobre 2019, même si les résultats sont controversés, Google annonce avoir atteint la suprématie quantique.

2020

Au CES 2020, IBM a annoncé la mise en ligne d'une nouvelle machine « Raleigh » dotée de 28 Qubits.

L'utopie est finie, le réel s'impose et tous les grands acteurs du numérique qui voient leur écosystème menacé par l'informatique quantique, se lancent dans la bataille.

3. Les enjeux de l'informatique quantique

3.1. Enjeux technologiques

Aujourd'hui il n'est pas d'entreprise qui ne mette en œuvre des ordinateurs ou des moyens de calculs et de communication basés sur des technologies à base d'algorithmes informatiques. Ces technologies, aujourd'hui appelées numériques, suivent une logique de calcul séquentiel, avec de plus en plus de parallélisme, ce qui a permis durant ces cinquante dernières années de diminuer de manière considérable les temps de calcul et de traitement. L'accroissement de la puissance de calcul et la miniaturisation des composants y ont également fortement contribué.

Néanmoins, malgré de nouveaux algorithmes et de nouvelles technologies comme l'intelligence artificielle, il devient aujourd'hui de plus en plus complexe de faire plus rapide. La technologie atteint des limites physiques qui semblent incontournables.

ACCROITRE LA PUISSANCE DE CALCUL

L'informatique quantique porte en elle-même la promesse du dépassement de cette limite : plutôt que de « dérouler » des instructions et des traitements pour arriver à une solution, quitte à explorer toutes les possibilités, il devient alors possible d'envisager d'exécuter simultanément l'ensemble des instructions, d'explorer conjointement toutes les facettes d'un problème pour, au final, donner la solution « en un coup ». C'est le principal enjeu de l'informatique quantique : donner un résultat dans un temps record alors qu'un ordinateur classique mettrait plusieurs jours, mois ou années.

> En 1997, l'ordinateur *Deep Blue* d'IBM qui a battu pour la première fois un champion d'échecs, Garry Kasparov, examinait 200 millions de mouvements possibles par seconde. Avec une machine quantique, il aurait été capable de calculer plusieurs milliards de mouvements en une seconde.

> Comparaison du nombre de bits et de Qubits[17] pour modéliser des molécules :
>
> - Molécule d'eau (H_2O) : 10^4 bits mais seulement 14 Qubits.
> - Molécule de caféine ($C_8H_{10}NO_2$) : 10^{48} bits mais seulement 160 Qubits.
> - Molécule de Pénicilline ($C_{16}H_{18}N_2NaO_4S$) : 10^{86} bits mais seulement 286 Qubits.
>
> *Source IBM Q*

[17] Voir le chapitre 5.2. Le Qubit, unité de base de l'informatique quantique

Les ordinateurs quantiques peuvent donc résoudre des problèmes impossibles à résoudre avec des ordinateurs classiques. Certes, ils ne remplaceront pas les ordinateurs classiques qui sont meilleurs dans des tâches courantes (bureautique, courriels etc…), mais ils seront parfaits pour résoudre les problèmes qui nécessitent une force de calcul conséquente. Par exemple faire de l'optimisation de trajet pour les transporteurs ou pour la planification de vols aériens, faire du chiffrement/déchiffrement, de la recherche dans des grands gisements de données (Big Data) ou encore modéliser des matériaux ou molécules diverses.

LES APPROCHES APPLICATIVES

Aujourd'hui, des programmes de recherche importants étudient ce qu'il est possible de réaliser en termes d'application en exploitant les propriétés d'intrication, de non localité et de superposition[18], propres à un système quantique. Ces travaux ciblent 4 grands domaines : la métrologie, la communication, la simulation et le calculateur universel.

En **métrologie**, c'est-à-dire la science des mesures, c'est une vraie révolution qui permet d'avoir des résultats statistiquement fiables. Même si une information portée par un Qubit est très sensible aux perturbations apportées par son environnement, les travaux menés peuvent permettre de construire des capteurs très sensibles. Aujourd'hui plusieurs projets concrets sont en phase de développement, pour des applications très spécialisées comme le détecteur d'ondes gravitationnelles LIGO, les centrales inertielles, etc… Les principaux acteurs en ce domaine sont Thalès, l'Observatoire de Paris, le NIST[19] et de nombreuses startups.

En matière de **communication**, les corrélations quantiques entre des particules intriquées permettent de coder un message garantissant l'absence d'interception lors de sa transmission. L'un des acteurs est aujourd'hui ID Quantic (à Genève) qui propose la transmission d'informations protégées par des clés quantiques sur environ 100 km. La Chine, l'université de Delft et l'Institut de physique expérimentale de l'Université d'Innsbruck travaillent sur des réseaux de nœuds quantiques fiables, y compris par satellite. L'université Paris Saclay travaille aussi sur des « répéteurs quantiques » pour contrer les pertes en ligne

Aujourd'hui il est possible d'imiter avec un ordinateur classique, une partie d'un système quantique dont on sait comment elle fonctionne : c'est un **simulateur** quantique[20]. Ce type d'outil ne permet pas de simuler l'entièreté de la logique quantique : il faut donc bien cibler ce que l'on souhaite simuler (« il faut poser la bonne question à laquelle la simulation va répondre »). Une simulation permet par exemple d'imaginer des améliorations sur les algorithmes d'optimisation. Certaines méthodes de

[18] Voir le chapitre 5.1. A la base, 3 principes quantiques
[19] NIST: *National Institute of Standards and Technology*
[20] Voir le chapitre 5.3. Les principaux types d'ordinateurs quantiques

simulation sont aujourd'hui considérées comme matures (par exemple la méthode Quantic Monte Carlo[21]) et pourraient représenter une voie combinant à la fois précision, contrôle des erreurs et puissance de calcul en fonction de la taille du système. Mais malgré des succès intéressants, les limitations de ces solutions les rendent encore très marginales. Les acteurs présents sur ce domaine sont aujourd'hui D-Wave, Google sur les circuits électroniques, Atos et Bull sur les simulations classiques mais aussi de grands groupes et de nombreux chercheurs académiques.

Le dernier domaine d'application concerne le **calculateur quantique universel[22]**. C'est l'équivalent d'une machine de Turing[23] mais quantique. Son fonctionnement est classique avec des stratégies de correction d'erreur discrètes et le résultat est probabiliste. C'est une approche qui permet de se concentrer uniquement sur certains éléments : les opérations de base. Plus on augmente le nombre d'opérations de base, plus on accroit la précision. L'accélération de calcul par rapport aux ordinateurs classiques est prouvée pour certains calculs comme la factorisation d'entiers, la recherche de solutions NP[24] ou la résolution de systèmes linéaires creux (*big data* et *machine learning*). Mais le passage de l'informatique classique vers l'informatique quantique ne donne pas systématiquement d'amélioration. De plus il est nécessaire d'avoir une électronique extrêmement performante alors que l'on note une démultiplication des problèmes lorsque l'on multiplie les Qubits. Actuellement on est à 99%[25] de précision sur des petits systèmes (de 5 à 10 Qubits), et pour passer à une échelle efficace, la recherche se concentre sur les stratégies de correction d'erreur scalables, sur des architectures de contrôle efficaces pour grands systèmes et sur l'optimisation de « compilation quantique ». Les acteurs sont IBM, Microsoft, Intel, Google et toutes les grandes universités dans le monde et quelques grosses startups (par exemple Rigetti[26]).

ATTEINDRE « L'AVANTAGE QUANTIQUE »

Les ordinateurs quantiques sont encore très fragiles : les Qubits permettant d'effectuer ces prouesses ne sont pas encore assez stables quelles que soient les technologies employées[27]. Ces mêmes technologies sont diverses et n'ont pas encore fait preuve d'un avantage compétitif évident qui permettrait d'en sélectionner une plutôt qu'une autre. Le second enjeu technologique est là : une fois qu'une technologie produira sans erreur un nombre suffisant de Qubits stables (on estime qu'il faut un millier de Qubits pour avoir un outil utile) et qu'un algorithme pourra s'exécuter de manière complète et répétitive dans des contextes différents, l'accélération se produira. Alors que la loi de

[21] http://www.lcpq.ups-tlse.fr/spip.php?article591
[22] Voir le chapitre 5.3. Les principaux types d'ordinateurs quantiques
[23] https://fr.wikipedia.org/wiki/Machine_de_Turing
[24] https://fr.wikipedia.org/wiki/Th%C3%A9orie_de_la_complexit%C3%A9_(informatique_th%C3%A9orique)
[25] Pour rappel les systèmes classiques (calculs à base de bits) sont précis à 100% : ils ne font pas d'erreur.
[26] https://www.itforbusiness.fr/thematiques/cloud-computing/item/10668-un-cloud-quantique-a-destination-des-entreprises
[27] Voir le chapitre 5.4. Les technologies matures et celles au stade de la recherche

Moore prise au sens commun[28] prévoyait une croissance « simplement » exponentielle (la puissance s'accroit d'un facteur 2, elle double à chaque étape : 2, 4, 8, 16…), la loi de Neven[29] envisage une accélération « doublement » exponentielle (la puissance s'accroit alors d'un facteur « puissance 2 » à chaque étape : 2, 16, 256, 65536…).

> *"By 2023, 20% of organizations will be budgeting for quantum computing projects compared to less than 1% today"*[30]
>
> Brian Burke,
> Chief of research, Gartner
> Sept 2019 - Gartner Symposium/ITxpo

C'est ce rythme d'accélération très rapide qui permet à la communauté scientifique de dire que d'ici 5 ans une équipe va arriver avec un algorithme et un *use case* spécifique qui démontrera ce qu'on appelle un « avantage quantique[31] ».

Nous sommes donc en train d'entrer dans ce moment, qu'IBM nomme la phase « *Quantum Advantage* ». En effet, en 2017 IBM a déjà réussi à simuler la structure moléculaire de l'hydrure de béryllium (BeH_2) et a atteint avec un ordinateur à 50 Qubits le seuil théorique de la suprématie quantique. Plus récemment, en octobre 2019 par un article dans la revue Nature[32], Google annonçait avoir également atteint cette suprématie quantique à l'aide d'un ordinateur quantique de sa conception en réussissant à effectuer un calcul en 3 minutes et 20 secondes alors qu'il aurait pris 10 000 ans s'il avait fallu mobiliser les plus gros ordinateurs existants. Ce résultat est relativisé par IBM qui a montré qu'il était possible d'arriver au même résultat en 2,5 jours avec une technique alternative sur un ordinateur classique. Néanmoins, c'est une prouesse quantique.

QUELS ALGORITHMES POUR L'INFORMATIQUE QUANTIQUE ?

Ce dernier exemple sur la prouesse de Google et la réaction d'IBM est très intéressant car il pose la question de savoir quels algorithmes seront déroulés sur des machines quantiques. En effet il n'y a pas d'intérêt à remplacer l'informatique classique si le gain n'est pas suffisant ou si par une méthode classique on peut obtenir le même résultat dans un temps « acceptable ».

[28] Dans son sens premier, la loi de Moore prédit le doublement du nombre de transistors sur une puce (miniaturisation) tous les 18 mois. Plus récemment, prise dans un sens commun, cette loi concerne le doublement de la puissance de calcul d'un ordinateur sur la même période.

[29] Harmut Neven est le directeur du *Quantum Artificial Intelligence lab*, initiative conjointe de la NASA, de l'association des universités de recherche sur l'espace et de Google Research. L'objectif du QAILab est de faire avancer la recherche sur la façon dont l'informatique quantique pourrait notamment aider au *machine learning*.

[30] « En 2023, 20 % des organisations budgétiseront des projets liés à l'informatique quantique, contre moins de 1 % aujourd'hui »

[31] Certains parlent aussi de « suprématie quantique », c'est-à-dire la capacité supposée d'un ordinateur quantique à faire des calculs qu'un (super)ordinateur classique ne pourrait faire. Atteindre cet horizon permettrait alors de basculer dans une autre dimension jusqu'à présent inaccessible.

[32] *Quantum supremacy using a programmable superconducting processor* – Nature 23 October 2019 https://www.nature.com/articles/s41586-019-1666-5

Aujourd'hui dans les laboratoires de recherche publics ou privés, on sait créer des systèmes quantiques capables de faire des calculs mais la question qui se pose est de savoir quels types de calculs il est pertinent de faire sur un ordinateur quantique car on ne peut pas prendre un algorithme classique et le transformer en quantique.

En fait, faute de technologie réellement opérationnelle et stable, les algorithmes complexes qui pourraient être appliqués à l'informatique quantique n'ont pas encore pu être mis en œuvre. Néanmoins, plusieurs existent et attendent d'être expérimentés. Ils peuvent être rangés dans quatre grandes familles d'algorithmes[33] :

- Les **algorithmes de recherche** d'informations dans des gisements ou structures de données importants ou complexes,
- Les **algorithmes basés sur les transformées de Fourier quantiques**, d'une importance considérable en mathématiques et en cryptologie,
- Les **algorithmes liés aux systèmes complexes** comme dans l'entraînement de réseaux de neurones, la recherche de chemin optimal dans des réseaux ou l'optimisation de processus,
- Les **algorithmes de simulation de systèmes physiques quantiques** qui servent notamment à simuler les interactions entre atomes dans des structures moléculaires diverses, inorganiques et organiques.

Le chiffrement face au quantique

L'algorithme de Shor est l'illustration la plus spectaculaire du calcul quantique ; il a pour objet de résoudre le problème de factorisation en décomposant un grand nombre en un produit de ses facteurs premiers. La cryptographie à clés publiques se base sur ce problème de factorisation pour générer des clés de chiffrement RSA. On est capable avec les algorithmes et les supercalculateurs d'aujourd'hui, de factoriser des nombres ayant environ 250 chiffres, mais au-delà de 500 chiffres cette factorisation devient impossible. De même, à l'inverse, plus la clé comporte un grand nombre de chiffres, plus le temps pour la « casser » en la décomposant en nombres premiers est grand. Alors que plusieurs centaines d'ordinateurs classiques travaillant en parallèle mettraient 1 milliard d'années pour décomposer une clé de 2048 bits, une centaine de secondes serait nécessaire à un ordinateur quantique.

[33] Classification d'Olivier Ezratty - https://www.oezratty.net/wordpress/2018/comprendre-informatique-quantique-algorithmes-et-applications/

3.2. Enjeux stratégiques

Selon le rapport « *Quantum Computing Market & Technologies - 2018-2024* »[34] publié par Industry 4.0 Market Research[35] qui produit des synthèses sur l'impact économique des technologies existantes ou émergentes, le marché mondial de l'informatique quantique va croitre de 24,6% par an. Et lors du *World Government Summit*[36] *2019*, forum d'échanges entre dirigeants, gouvernants et experts, il a été annoncé[37] que le marché mondial de l'informatique quantique quadruplera entre 2023 et 2027, l'investissement dans les logiciels et services associés à l'informatique quantique passant de 2 à 8 milliards de dollars.

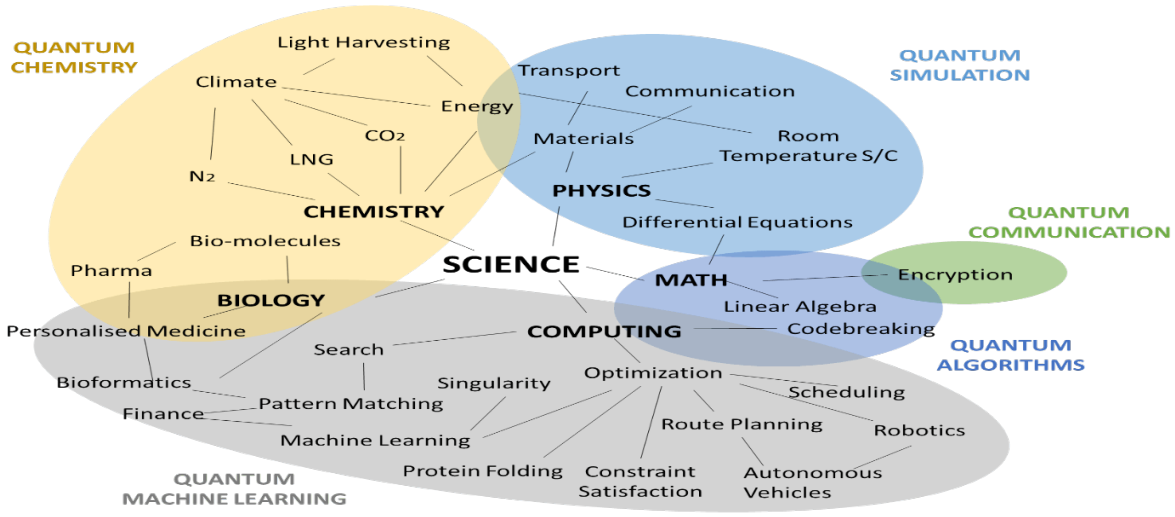


Figure 2 : *Quantum Computing will transform almost every aspect of our technology, science, economy & life*

Source – World Economic Forum, HSRC[38]

L'informatique quantique a le potentiel de modifier les rapports de force dans l'industrie, mais aussi dans le renseignement, les affaires militaires et les équilibres stratégiques. Les entreprises et les États s'y préparent car si l'on considère que les premières applications arriveront d'ici 5 à 10 ans, c'est demain !

La question clé n'est donc plus de savoir s'il y aura un ordinateur quantique, mais qui le construira et en tirera profit. Et le principal enjeu concerne la maîtrise de cette technologie car elle met en danger

[34] https://industry40marketresearch.com/product/quantum-computing-market-technologies/
[35] https://industry40marketresearch.com/
[36] https://www.worldgovernmentsummit.org/
[37] https://www.pwc.com/m1/en/world-government-summit/documents/wgs-quantum-leap.pdf
[38] HSRC : *Human Sciences Research Council*

la sécurisation des communications et du stockage de l'information. C'est devenu un enjeu de souveraineté.

FRANCE

En France, le Premier ministre a confié, en avril 2019, à la députée Paula Forteza une mission sur les technologies quantiques. L'objectif, sur la base de ce rapport, est d'élaborer une stratégie française sur l'informatique quantique. Ce rapport[39] « Quantique : le virage technologique que la France ne ratera pas - 37 propositions pour une stratégie nationale ambitieuse », présenté le 9 janvier 2020, propose d'investir 1,4 milliards d'euros sur cinq ans dans ce domaine, de créer des parcours de formation avec une spécialisation quantique, et de développer à Paris, Saclay et Grenoble trois pôles d'excellence avec des instituts interdisciplinaires en informatique quantique.

Aujourd'hui, la France se positionne comme un *leader* du quantique en Europe avec 18% des startups et 17% des fonds d'investissements[40]. Fort de ce positionnement, Paula Forteza propose dans son rapport de le renforcer en accompagnant, avec Bpifrance, la création d'une cinquantaine de startups jusqu'en 2024, et de créer un fond d'investissement de 300 à 500 millions d'euros dédié aux startups du quantique. Aujourd'hui existent déjà Quantonation[41] qui investit dans toutes les briques de l'informatique quantique, et Génération DeepTech[42] (porté par Bpifrance) qui s'attaque aux grands défis du XXIe siècle.

L'ANSSI[43], qui dépend du Premier ministre, a aussi commencé à travailler sur ces questions. Dans son rapport annuel 2018, l'ANSSI soulignait que « les technologies comme l'intelligence artificielle, la santé connectée ou l'informatique quantique vont bouleverser la manière de faire de la sécurité ». Selon Paula Forteza « l'ANSSI a commencé à travailler sur ces questions, en annonçant par exemple qu'à compter de 2020, elle ne labellisera plus les technologies de chiffrement qui ne résisteraient pas au quantique (*quantic resistant)* »[44].

EUROPE

En Europe, le *Quantum manifesto*, signé par plus de 3 000 acteurs du domaine, dont 156 entreprises européennes et 20 institutions de recherche, a poussé à la création en 2016 du programme européen *Quantum Technology* en s'appuyant sur les initiatives FET (Technologies Futures et Émergentes)

[39] https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf
[40] Source Wavestone : https://www.wavestone.com/app/uploads/2019/10/Quantum-computing-Wavestone-France-Digitale-FR-web-2019.pdf
[41] https://www.quantonation.com/
[42] https://www.bpifrance.fr/A-la-une/Dossiers/Generation-Deeptech-le-futur-de-l-innovation
[43] ANSSI : Agence Nationale pour la Sécurité des Systèmes d'Information
[44] Le Monde Informatique du 10 juin 2019 : https://www.lemondeinformatique.fr/actualites/lire-paula-forteza-deputee-des-francais-de-l-etranger--en-termes-de-souverainete-c-est-une-necessite-de-maitriser-le-quantique-75546.html

Flagship[45]. Et aujourd'hui, dans ce cadre, plusieurs États membres et agences de financement nationales ont lancé le projet FET *Flagship* QuantERA pour soutenir la recherche européenne dans le domaine des technologies quantiques et investir sur 10 ans un milliard d'euros sur des centaines de projets.

ÉTATS-UNIS

Aux États-Unis, le *quantum computing* est devenu un actif stratégique. En 2018, le *National Science & Technology Council* produisait un rapport[46] sur ses enjeux tant économiques et scientifiques que stratégiques et militaires. Quelques mois plus tard, entrait en vigueur le *National Quantum Initiative Act*[47], engageant 1,2 milliard de dollars dans la recherche sur les systèmes d'information quantiques. Cette loi demandait au DOE[48], à la NSF[49] et au NIST[50] d'appuyer la recherche et la formation aux technologies quantiques, mais aussi d'élargir et faciliter les projets de collaboration ou la création de consortiums avec d'autres acteurs des secteurs public ou privé, y compris l'industrie, les universités et les laboratoires fédéraux. Le pilotage de cette initiative se faisant au travers d'un comité du NSCT[51] dédié à l'informatique quantique et comprenant des représentants du NIST, de la NSF, du DOE mais aussi de la NASA, du Ministère de la Défense, de l'ODNI[52] et des Bureaux de la Maison-Blanche chargés du budget et de la politique scientifique et technologique américaine.

Afin de protéger les dispositifs électroniques et informatiques utilisées par les organismes fédéraux américains des futurs outils quantiques de demain, capables de casser les cryptages, le NIST a aussi lancé en 2016 un projet d'évaluation des algorithmes utilisés. L'objectif est que l'ensemble de l'administration américaine utilise en 2024 des algorithmes post-quantiques (appelé aussi *quantic resistant)*. 69 algorithmes ont déjà été évalués en 2018.

CHINE

La Chine investit également beaucoup dans l'informatique quantique. Le 3 mai 2017, Xinhua, l'agence de presse officielle de la République populaire de Chine, a annoncé que les scientifiques chinois avaient construit un premier ordinateur quantique, et qu'en 2018, ils ont établi un record d'intrication avec un

[45] Les projets FET Flagships (fleurons) sont des projets de plus d'1 milliard d'euros rassemblant des acteurs publics et/ou privés. https://qt.eu/
[46] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf
[47] https://www.aip.org/fyi/2019/national-quantum-initiative-signed-law
[48] DOE : *Department Of Energy*
[49] NSF : *National Science Foundation*
[50] NIST : *National Institute of Standards and Technology*
[51] NSTC : *National Science and Technology Council*
[52] ODNI : *Office of the Director of National Intelligence*

système quantique de 18 Qubits[53]. Plusieurs expérimentations ont aussi fait l'objet de communications dont une transmission *via* satellite, protégée par cryptographie quantique. La Chine est aussi en train de mettre en œuvre un réseau de communication quantique à grande échelle.

RUSSIE

Il reste un dernier acteur international, qui communique peu aujourd'hui, c'est la Russie. Néanmoins un article[54] publié le 16 octobre 2019 sur le site IOPScience[55], par un ensemble de scientifiques russes, décrit par le détail les acteurs et l'état de la recherche russe en matière de technologies quantiques.

Les technologies quantiques sont stratégiques et font partie d'un programme national de développement de l'économie numérique russe, *the Digital Economy National Program*, d'un montant global de 25 milliards d'euros et dans lequel le budget dédié aux technologies quantiques devrait y atteindre le milliard d'euros. Les travaux sont soutenus par les organismes gouvernementaux et industriels russes (Rosatom, Rostech, *Bank of Russia*, Rostelecom, Gazprombank, Sberbank…).

Complétant les centres scientifiques renommés existants, plusieurs centres de recherche ont récemment été créés entre 2010 et 2018 : *the Russian Quantum Center* (2010), *The Kazan Quantum Center* (2014), les *NTI*[56] *Quantum Technologies Centre*[57] (2017) et *NTI Center for Quantum Communications*[58] (2018).

Le principal objectif de la feuille de route russe est de construire une pile complète de technologies pour le calcul quantique. Parmi les travaux, on peut citer la démonstration d'opérations de portes logiques quantiques à un et deux Qubits avec une fiabilité démontrée à 95%, la démonstration d'une plateforme de calcul et de simulation quantique à 50 Qubits ; en cryptographie, un dispositif de distribution de clés quantiques a été testé sur des lignes optiques de 32km dans des conditions urbaines, démontrant ainsi l'applicabilité fonctionnelle. L'expertise russe a aussi fortement contribué aux travaux sur le détecteur d'ondes gravitationnelles LIGO.

3.3. Enjeux *business*

En octobre 2018[59] un article publié par IBM démontrait qu'avec les processeurs quantiques disponibles et malgré leurs imperfections (bruits, faible précision…) il était possible d'avoir un avantage quantique. Ce qui signifiait qu'il était alors possible d'imaginer ce que l'on pourrait faire lorsque des ordinateurs

[53] Scientific American : https://www.scientificamerican.com/article/chinese-researchers-achieve-stunning-quantum-entanglement-record/
[54] https://iopscience.iop.org/article/10.1088/2058-9565/ab4472/pdf
[55] https://iopscience.iop.org
[56] NTI : *National Technological Initiative*
[57] À la M.V. Lomonosov Moscow State University (QTC MSU)
[58] À la National University of Science and Technology MISiS
[59] https://www.ibm.com/blogs/research/2018/10/quantum-advantage-2/

quantiques seraient suffisamment puissants et précis. Et cela a excité toute la communauté scientifique mais aussi le tissu économique !

L'accélération de l'intérêt du monde économique et industriel sur le *Quantum Computing* est réelle. Il y a encore 3 ou 4 ans il n'y avait pas grand-chose en termes de réalisation. Mais on commence à voir depuis 2 ans, de plus en plus, une vraie appétence de la part des industriels et des startups qui y travaillent très sérieusement. Cette accélération s'explique d'une part parce qu'il y a un effet d'appropriation des algorithmes par un nombre de plus en plus grand d'entreprises ; d'autre part parce que la plus petite innovation, amélioration ou optimisation (technique, logicielle, physique etc…) fait faire un bond en performances, et certains acteurs, notamment au Canada où s'est développé un important écosystème de startups en ce sens, se spécialisent sur un point particulier pour l'améliorer en développant des bouts de code, des algorithmes etc... Et enfin il y a la capacité de plus en plus grande des entreprises à travailler sur des sujets complexes en partenariat avec le monde de la recherche comme cela a été le cas avec l'intelligence artificielle (IA).

De nombreuses entreprises, bien qu'encore dans des phases d'expérimentation, cherchent donc activement à savoir ce que l'informatique quantique peut apporter dans leur R&D, dans l'élaboration et le fonctionnement de leurs produits et services associés et au final sur leurs résultats nets.

Les applications de l'informatique quantique qui semblent possibles concernent la modélisation moléculaire (ou chimie quantique), l'optimisation, la modélisation financière, la sécurisation des communications par *Quantum Key distribution* (cryptographie) et les activités liées à l'IA et au *deep learning*. En voici quelques exemples.

OPTIMISATION

Daimler travaille ainsi avec IBM et Google et, de la même manière Volkswagen travaille avec Google et D-Wave Systems, pour voir comment les ordinateurs quantiques peuvent aider à résoudre les problèmes d'optimisation des itinéraires de livraison des véhicules ou le flux des pièces dans les usines.

Ces deux constructeurs étudient aussi l'apport de l'informatique quantique pour développer de meilleures batteries en simulant les structures et les réactions chimiques à l'intérieur des batteries et ainsi aider à l'amélioration des véhicules électriques.

En 2011, le géant de l'aérospatiale Lockheed Martin a été le premier acheteur d'un ordinateur quantique fabriqué par D-Wave Systems et a continué d'étudier l'utilisation de cette technologie pour des applications liées à la gestion et à l'optimisation du trafic aérien et à la vérification des systèmes. Toujours dans l'aéronautique, Airbus étudie également comment l'informatique quantique pourrait

contribuer et accélérer ses activités de recherche (Airbus a pour cela investi dans la société de logiciels d'informatique quantique QC Ware[60]).

Dans le secteur financier, JPMorgan travaille avec IBM pour explorer comment les ordinateurs quantiques peuvent contribuer aux stratégies de *trading*, à l'optimisation des portefeuilles de titres, à l'évaluation des actifs et à l'analyse des risques. De même, Barclays participe au réseau IBM Q Network pour déterminer si des ordinateurs quantiques pourraient être utilisés pour optimiser le règlement de grands lots de transactions financières.

MODELISATION DE STRUCTURES MOLECULAIRES

Simuler, *in silico*, de manière exacte, la structure et le fonctionnement de grosses molécules a un intérêt certain pour l'industrie pharmacologique ou pour l'agronomie. Dans ce domaine, Accenture Labs, l'innovateur en biotechnologie Biogen et la société de logiciels quantiques 1QBit[61] étudient les manières d'accélérer la découverte de médicaments en utilisant des calculateurs quantiques pour faire des comparaisons moléculaires. En septembre 2017, IBM a simulé la structure d'une molécule d'hydrure de béryllium à trois atomes. En octobre 2017, Google et Rigetti ont également annoncé OpenFermion, un logiciel de simulation chimique sur ordinateur quantique.

COMMUNICATIONS

La sécurisation des communications est un enjeu majeur pour les gouvernements mais aussi pour les entreprises. Tous les secteurs sont concernés car les données sont au cœur de la plupart des organisations. La cryptologie quantique est parmi les domaines les plus matures (la France est même très bien placée en ce qui concerne les théories et les expérimentations).

Déjà en 2006, une expérimentation de chiffrement quantique avait été mené pour transmettre les informations de la coupe du monde de football. La même année, plusieurs industriels japonais, Mitsubishi Electric Corporation, NEC Corporation, *the Institute of Industrial Science*, et l'Université de Tokyo avaient mis en place un chiffrement quantique pour s'interconnecter. En 2007 c'est le canton de Genève (en Suisse), en partenariat avec l'Université de Genève (UNIGE), qui a expérimenté la sécurisation par cryptographie quantique de la liaison reliant les lieux de dépouillement au centre de données. En 2008, le SECOQC[62] faisait la démonstration du tout premier réseau informatique exploitant une technologie fonctionnelle de chiffrage à clés quantiques (QKD).

[60] https://qcware.com/
[61] https://1qbit.com/
[62] Development of a Global Network for Secure Communication based on Quantum Cryptography: http://www.secoqc.net/

En mai 2019, une expérimentation[63] en coopération avec Orange a été lancée dans la métropole Nice Côte d'Azur pour sécuriser les communications par échange de clés quantiques entre l'Institut de physique de Nice, basé sur le campus Valrose et le centre INRIA Sophia Antipolis (distant de 30km), et avec l'IMREDD[64] dans la plaine du Var comme source d'intrication de l'information.

Pour les communications, l'enjeu véritable est de pouvoir faire du chiffrement quantique sur de très longues distances. À ce sujet, le *Cambridge Research Laboratory* de Toshiba expliquait dans une publication[65] de mai 2018, qu'il était possible d'étendre la portée des communications chiffrées ainsi à plus de 500 kilomètres au travers de fibres standard. Par exemple cela pourrait permettre de relier de manière sécurisée des villes telles que Londres, Paris, Dublin, Manchester et Amsterdam.

MACHINE LEARNING

Dès la mi-2018, TERATEC[66] et un groupe d'industriels ont lancé une initiative particulière sur le quantique, à vocation française et européenne, TQCI (*Teratec Quantum Computing Initiative*). Le noyau de départ regroupe TERATEC, Total, EDF, Dassault Aviation, ATOS, le CEA et le CERFACS[67], et va rapidement être étendu.

Dans ce cadre, des travaux sont réalisés sur les retours d'expérience des participants et sur l'utilisation des technologies quantiques pour les applications de *machine learning*. Un projet est en cours de définition pour d'une part concevoir les algorithmes spécifiques au calcul quantique dans les grands domaines d'applications, d'autre part développer et expérimenter des cas d'usage industriels, et enfin pour former et animer la communauté des utilisateurs.

***HIGH PERFORMANCE COMPUTING* (HPC)**

La France a une position forte à la fois dans les technologies et dans les usages. Des progrès remarquables ont été faits récemment dans les technologies et dans les techniques d'émulation ; le quantique est un axe très important pour le calcul à haute performance et pour les technologies de sécurité et c'est un des plus grands domaines stratégiques de demain. C'est maintenant qu'il faut avancer ! Les industriels, utilisateurs et fournisseurs technologiques sont prêts à participer à un programme d'actions ambitieux dans lequel TERATEC et ses partenaires joueront un rôle clé.

Le quantique sera aussi intégré en 2020 dans le grand programme Européen EuroHPC[68] auquel TERATEC participe.

[63] https://inphyni.cnrs.fr/contenus-riches/actualites/fr/universite-cote-d2019azur-et-orange-collaborent-pour-la-mise-en-place-d2019une-experimentation-en-matiere-de-cryptographie-quantique/@@highlight_view
[64] IMREDD : Institut Méditerranéen du Risque de l'Environnement et du Développement Durable : https://imredd.fr/
[65] https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Press/Toshiba-Redefines-the-Limit-of-Intercity-Secure-Communications/
[66] http://www.teratec.eu
[67] CERFACS : Centre Européen de Recherche et de Formation Avancée en Calcul Scientifique : https://cerfacs.fr/
[68] https://eurohpc-ju.europa.eu/

3.4. Enjeux de formation

Au cours des réunions tenues par le Groupe de travail du Cigref, plusieurs intervenants ont attiré notre attention sur la faiblesse de la formation à l'informatique quantique en France.

Comme nous l'avons écrit précédemment, l'informatique quantique est plus une science du physicien que de l'ingénieur. Mais l'ingénieur est indispensable pour concevoir et industrialiser des produits.

Si l'on considère que les premières applications industrielles apparaitront dans 5 à 10 ans, cela signifie que d'ici 2030 il faudra former, ou *a minima* sensibiliser, au quantique de nombreux étudiants (car on ne pense pas « quantique » comme on pense « informatique »). Il s'agit moins de former de futurs physiciens du quantique que de former de futurs informaticiens au quantique.

De nombreuses universités, tirées par la recherche académique sur la physique quantique, ont mis en œuvre de multiples initiatives. L'Université Côte d'Azur, qui est la première université française à expérimenter un réseau quantique, fait de la sensibilisation/formation auprès des étudiants. L'université de Montpellier, avec le soutien de la Région Occitanie/Pyrénées-Méditerranée, s'est associée à IBM pour créer des modules de formation sur le calcul quantique, l'université de Paris Saclay propose aussi des masters et des doctorats en physique quantique et, fait intéressant, est partenaire d'un cursus d'ingénieur de Centrale Supélec. L'ISAE-Sup Aero propose une formation en ingénierie quantique et miniaturisation ultime. L'Université Paul Sabatier et l'INSA de Toulouse développent aussi leurs formations aux technologies quantiques en s'appuyant sur l'École Universitaire de Recherche (EUR). Certaines Miage, notamment celle d'Evry, s'y intéressent également. Il y a aussi des chaires industrielles, comme celle d'Atos et du CEA[69] qui a été montée en mai 2018.

Mais la plupart des autres établissements d'enseignement supérieur, dont notamment les écoles d'ingénieurs en informatique, n'ont pas intégré les technologies quantiques dans leurs formations alors que c'est un domaine qui va, comme les technologies numériques aujourd'hui, impacter voire transformer les futurs systèmes d'information des entreprises. On peut néanmoins citer Télécom Paris qui a développé dans un cursus sur 3 ans des éléments de base de la mécanique quantique à la cryptographie et aux communications quantiques, en passant par l'informatique et l'algorithmique quantique. Ainsi que l'École Polytechnique qui propose également un Master « physique et applications » spécialisé sur les dispositifs quantiques.

Il y a donc une carence de formations sur le sujet, avec le risque que les entreprises n'aient pas la maîtrise des technologies employées, voire n'en comprennent pas la portée, par manque de compétences.

[69] http://www.cea.fr/presse/Pages/actualites-communiques/sciences-de-la-matiere/atos-cea-anr-chaire-industrielle-informatique-quantique.aspx

Néanmoins, de manière générale, alors qu'avec le *National Quantum Initiative Act* le gouvernement américain demande aux différentes agences et acteurs nationaux d'appuyer et d'investir dans la recherche ET la formation, on ne peut qu'espérer que le futur plan quantique français suive les propositions du rapport de Paula Forteza et prenne en considération ce problème en organisant le développement de formations pour les futures informaticiennes et informaticiens quantiques dont nous aurons besoin.

4. Effervescence de l'écosystème quantique

Malgré un niveau de maturité technologique (TRL[70]) encore bas, de nombreuses entreprises montrent un intérêt certain pour la recherche quantique et y investissent.

Et alors que cela semblait encore difficile il y a quelques années, les chercheurs physiciens du quantique s'associent aujourd'hui avec des géants technologiques et de grandes entreprises. Des écosystèmes de startups se développent aussi très rapidement (en France, au Canada…).

L'ambition de tous ces acteurs est, bien évidemment, de réussir le transfert de la recherche en laboratoire vers l'industrialisation en entreprise.

4.1. Les principaux acteurs

En raison de l'intérêt économique, les plus grandes entreprises mondiales et de nombreuses agences gouvernementales travaillent sur des technologies et logiciels quantiques. Les principaux sont Alibaba, Atos, D-Wave, Google, IBM, Intel, IonQ, Microsoft, Quantum Circuits, Rigetti… Bon nombre de ces entreprises travaillent également en collaboration avec d'importantes équipes de recherche universitaires, et toutes continuent d'enregistrer des progrès importants.

ALIBABA

En juillet 2015, Alibaba, le géant chinois du web s'est associé à l'Académie chinoise des sciences pour former le « *Alibaba Quantum Computing Laboratory*[71] » qui a pour mission de lancer des recherches pointues sur les systèmes les plus prometteurs qui permettraient de réaliser des applications pratiques en informatique quantique.

Alibaba, comme IBM, a mis en ligne un ordinateur quantique expérimental. Plus précisément, en mars 2018, le géant chinois du commerce électronique a donné accès sur le Cloud chinois à un ordinateur

[70] TRL: Technology *Readiness Level*
[71] https://damo.alibaba.com/labs/quantum

quantique de 11 Qubits, développé en collaboration avec l'Académie chinoise des sciences et qui permet d'exécuter des programmes quantiques et de télécharger les résultats.

ATOS

Atos est l'un des leaders européens de l'écosystème quantique. Atos a lancé le programme industriel d'informatique quantique Atos Quantum[72] en 2016 en s'appuyant sur un conseil scientifique composé de nombreux grands physiciens du quantique[73]. Son approche est différente de celle des autres acteurs : partant du principe que ce n'est pas le matériel mais le logiciel et les applications développées qui font le succès du numérique aujourd'hui, Atos a développé en 2017 une plateforme de programmation d'algorithmes quantiques, Atos QLM[74]. C'est un serveur monofonctionnel (*Appliance*) qui simule tout type d'ordinateur quantique (30 à 40 Qubits) et qui est équipé d'un environnement de développement (Atos myQLM). Aujourd'hui Atos QLM compte parmi ses utilisateurs le département américain de l'énergie, mais aussi Total ou l'entreprise Zapata Computing Inc[75].

Atos, avec de multiples partenaires, a aussi un programme de R&D impliqué dans de multiples projets européens comme le projet AQTION[76] qui vise à fournir un accélérateur quantique à ions piégés de 50 à 100 Qubits pour 2023 et le projet PASQuans[77] pour créer des plateformes de simulation quantique jusqu'à 500 Qubits.

D-WAVE

D-Wave[78] est un *pure player* pionnier de l'informatique quantique, basé au Canada, qui a fait la démonstration en 2007 d'une machine quantique de 16 Qubits. En 2011, D-Wave a vendu à Lockheed Martin, D-Wave One, un système quantique de 128 Qubits. Puis en 2013, la Nasa, avec Google, a acquis une machine de 512 Qubits (le D-Wave Two). En 2015, D-Wave aurait franchi la barre des 1 000 Qubits avec le D-Wave 2X, et en janvier 2017 a vendu le D-Wave 2000Q (2000 Qubits) à la société de cybersécurité *Temporal Defense Systems*. En septembre 2019, D-Wave annonçait un ordinateur quantique à 5000 Qubits[79].

Aujourd'hui D-Wave est la seule entreprise à avoir jamais vendu un système de calcul quantique. Cependant, les machines de D-Wave, qui communique très peu, sont controversées d'une part en

[72] https://atos.net/fr/vision-et-innovation/atos-quantum
[73] https://atos.net/fr/2017/communiques-de-presse_2017_11_23/le-conseil-scientifique-du-programme-atos-quantum-se-felicite-des-avancees-significatives-realisees-depuis-un
[74] Atos QLM: *Atos Quantum Learning Machine*
[75] Acteur américain spécialisé dans le domaine des algorithmes quantiques
[76] AQTION: *Advanced Quantum computing with Trapped IONs*
[77] PASQuanS : *Programmable Atomic Atomic Large-Scale Quantum Simulation*
[78] https://www.dwavesys.com/
[79] https://siliconangle.com/2019/09/24/d-wave-debuts-new-5000-qubit-quantum-computer/

raison de la technologie choisie (le recuit quantique[80]) et d'autre part parce qu'elles semblent ne faire que ce pour quoi elles ont été conçues, comme des « automates » quantiques plutôt que des « ordinateurs » quantiques. Néanmoins l'annonce de Google en octobre 2019 sur l'atteinte de la suprématie quantique se base sur une machine D-Wave et démontre leur savoir-faire.

D-Wave commercialise la suite *D-Wave's Ocean Software*, ensemble d'outils pour développer des applications.

D-Wave, comme Alibaba et IBM, a également mis en 2018 dans le Cloud un environnement de développement d'applications quantiques appelé *Leap*. *Leap* permet d'accéder en temps réel à un ordinateur quantique de type D-Wave 2000Q.

GOOGLE

Google travaille d'arrache-pied pour faire de l'informatique quantique une réalité au travers de son *AI Quantum Laboratory*[81]. C'est avec des machines D-Wave que Google s'est lancé dans l'aventure de l'informatique quantique. Mais rapidement Google a développé son propre matériel et a annoncé en mars 2018 un processeur quantique de 72 Qubits appelé « *Bristlecone* ».

En juin 2019, Hartmut Neven, Directeur du *Quantum Artificial Intelligence Lab* de Google, énonce la « loi de Neven » qui suggère que Google pourrait atteindre le point de suprématie d'ici la fin de 2019. Et en effet, en octobre 2019, un article dans Nature[82] indiquait qu'elle aurait été atteinte. Prouesse néanmoins contestée par plusieurs acteurs, dont IBM[83].

Google, comme IBM, pense qu'il est possible d'avoir des premiers résultats tangibles et commercialisables dans les 5 ans à venir.

IBM

Cela fait maintenant plus de 35 ans qu'IBM travaille sur l'ordinateur quantique. En 2016, IBM a mis sur le Cloud à destination du public un ordinateur quantique de 5 Qubits puis de 16 Qubits. En parallèle, pour aider ceux qui souhaitent apprendre et développer, IBM propose le *framework* Open Source Qiskit.

En 2017, IBM a créé IBM Q *Network*[84] qui rassemble une communauté mondiale d'entreprises, de startups, d'institutions académiques et de laboratoires de recherche nationaux de premier plan pour faire progresser l'informatique quantique et notamment explorer des cas d'usage.

[80] https://www.frenchweb.fr/comprendre-linformatique-quantique-adiabatique/335616
[81] https://ai.google/research/teams/applied-science/quantum/
[82] https://www.nature.com/articles/s41586-019-1666-5
[83] Pour comprendre la prouesse de Google : https://www.youtube.com/watch?v=KaRd_eB2qOA
[84] https://www.ibm.com/quantum-computing/

En janvier 2019, IBM a dévoilé une offre commerciale IBM Q *System One* basée sur un ordinateur quantique modulaire et compact destiné à être utilisé en dehors d'un laboratoire de recherche.

INTEL

Le premier producteur mondial de microprocesseurs, Intel, travaille bien évidemment au développement de puces à calcul quantique[85]. Intel a choisi de suivre deux approches de recherche distinctes. La première, menée en collaboration avec le pionnier néerlandais de l'informatique quantique QuTech[86], a abouti à la création d'une puce d'essai de 17 Qubits. En janvier 2018, au CES de Las Vegas, Intel a annoncé la livraison d'un processeur quantique d'essai de 49 Qubits appelé « *Tangle Lake* ».

La seconde approche d'Intel en matière de recherche est interne à l'entreprise. Elle cherche à créer des processeurs basés sur la technologie « *Spin Qubit* » en s'appuyant sur des méthodes traditionnelles et maîtrisées d'Intel de fabrication des puces en silicium. En juin 2018, Intel a indiqué que les tests d'une puce de 26 *Spin Qubit* avaient commencé. La quête de la maitrise de la miniaturisation des Qubits (les Spin Qubits font 50 nanomètres de diamètre) permet à Intel d'envisager d'ici 10 ans la fabrication de minuscules processeurs quantiques contenant des milliers ou des millions de Qubits. Cette technologie suscite néanmoins des doutes sur sa faisabilité à court terme et Intel ne prévoit pas une commercialisation possible avant 2025.

IONQ

IonQ[87] est également un *pure player* de l'informatique quantique. La technologie utilisée est à base « d'ions piégés ». Son objectif vise un ordinateur quantique évolutif qui puisse supporter des applications diverses dans des secteurs industriels variés.

En novembre 2019, IonQ annonçait la création d'*Azure Quantum* en partenariat avec Microsoft. Il s'agit de rendre accessibles les ordinateurs d'IonQ sur le Cloud au travers du Cloud de Microsoft.

MICROSOFT

Microsoft travaille sur l'informatique quantique[88] depuis 1997 avec Alexeï Kitaev, professeur russo-américain de physique à l'Institut de technologie de Californie et chercheur chez Microsoft, qui a eu l'idée de s'inspirer de la topologie pour imaginer une solution à la correction d'erreurs des Qubits.

La stratégie de Microsoft concerne le développement d'ordinateurs quantiques basés sur des Qubits topologiques qui, parce que moins sujets aux erreurs, semblent plus faciles à envisager pour une

[85] https://www.intel.fr/content/www/fr/fr/research/quantum-computing.html
[86] https://qutech.nl/
[87] https://ionq.com/
[88] https://www.microsoft.com/en-us/quantum/

application commerciale. Selon un article paru en mai 2018 dans *Computer Weekly*[89], Todd Holmdahl, *Corporate Vice President Quantum* de Microsoft estime qu'il serait possible d'avoir des ordinateurs quantiques commerciaux sur Azure dans seulement cinq ans.

Microsoft travaille également avec plusieurs universités dans le monde entier où des laboratoires « *station* Q »[90] ont été montés. En février 2019, Microsoft a également annoncé le réseau Microsoft *Quantum Network* rassemblant de nombreux acteurs et visant à développer une « économie du quantique ».

Microsoft, comme IBM et Atos, s'intéresse aussi au codage et en ce sens a notamment mis en ligne, gratuitement, en décembre 2017, un kit de développement en informatique quantique. Ce kit comprend un langage de programmation appelé Q#[91], ainsi qu'un simulateur d'informatique quantique.

QUANTUM CIRCUITS

Quantum Circuits[92] est une startup qui a été créée par Robert Schoelkopf, professeur d'informatique quantique, et d'autres collègues de l'Université de Yale. L'entreprise a réuni 18 millions de dollars et a pour ambition de damer le pion aux géants de l'industrie informatique dans la course à la fabrication d'un ordinateur quantique opérationnel.

RIGETTI

La startup Rigetti est un autre *pure player* de l'informatique quantique. Ce fabriquant de puce quantique a mis en ligne un processeur quantique de 19 Qubits (le 19Q) dans son environnement de développement appelé *Forest*. En 2017, Rigetti avec son 19Q démontrait qu'il était possible de faire progresser de manière significative l'intelligence artificielle en étant capable d'exécuter une tâche d'apprentissage non supervisé (*Unsupervised Machine Learning*).

En 2018, Rigetti, comme plusieurs de ses concurrents, a mis dans le Cloud sa plateforme d'informatique quantique hybride QCS[93]. Et a lancé dans la foulée un concours d'un million de dollars pour qui démontrerait un avantage quantique sur sa plateforme QCS.

Rigetti est actuellement en train de travailler sur l'élaboration d'une nouvelle puce de 128 Qubits prévue pour 2020.

[89] https://www.computerweekly.com/news/252440763/Microsoft-predicts-five-year-wait-for-quantum-computing-in-Azure
[90] https://news.microsoft.com/stories/stationq/
[91] https://docs.microsoft.com/en-us/quantum/language/?view=qsharp-preview
[92] https://quantumcircuits.com/
[93] QCS : *Quantum Cloud Services*

TERATEC

TERATEC[94] est un centre européen de compétences créé par le CEA et des industriels utilisateurs pour maîtriser et diffuser les technologies numériques (supercalculateurs, simulation, *data analytics*, apprentissage machine, IA …) en association avec la recherche scientifique et avec les fournisseurs technologiques, grands et petits, en mode co-design.

TERATEC représente aujourd'hui 80 membres, s'étend sur un campus sur lequel travaillent plus de 250 personnes en Essonne et a une position majeure reconnue en Europe.

4.2. Les acteurs publics en France

De nombreux acteurs publics et des universités françaises sont parties prenantes dans la course vers la maitrise du quantique. En termes de localisation, ces acteurs se situent essentiellement sur 4 régions : en Ile-de-France, en Occitanie, en Provence-Alpes-Côte d'Azur et en Auvergne-Rhône-Alpes.

En Ile-de-France, le **Pôle quantique Paris Saclay**[95] (piloté par Pascale Senellart[96] du CNRS), avec l'**Université Paris Saclay** regroupe une quarantaine d'équipes de recherche sur les technologies quantiques. L'université a aussi monté plusieurs partenariats avec **Thalès**, **Atos**, **EDF**, **IBM** ou **Air Liquide**.

L'Inria[97] est également un acteur important de l'informatique quantique en Ile-de-France. Avec son équipe **QUANTIC**[98], l'Inria cherche à développer des méthodes et des dispositifs expérimentaux assurant un traitement robuste de l'information quantique. Ces travaux se font en collaboration avec le **Laboratoire Kastler-Brossel** de l'**ENS** (École Normale Supérieure), **Yale University**, le **CEA**…

En Occitanie, la filière quantique associe une dizaine de **laboratoires de Montpellier et de Toulouse** qui travaillent avec le **CNRS**. La recherche y est essentiellement centrée sur les capteurs et les communications quantiques. **IBM** y a créé le premier Q Hub en France en coopération avec l'**université de Montpellier**.

En Provence-Alpes-Côte d'Azur, avec le **CNRS**, l'**Institut de Physique de Nice** (INPHYNI) de l'**Université Côte d'Azur** a développé un centre de recherche sur la physique quantique et ondulatoire. L'université collabore avec **Orange** pour la mise en place d'une expérimentation en matière de cryptographie quantique.

[94] http://www.teratec.eu/
[95] https://www.universite-paris-saclay.fr/fr/quantum-centre-en-sciences-et-technologies-quantiques
[96] https://www.universite-paris-saclay.fr/actualites/pascale-senellart-mardon-la-pointe-de-la-deuxieme-revolution-quantique
[97] Institut national de recherche en informatique et en automatique
[98] https://team.inria.fr/quantic/

En Auvergne-Rhône-Alpes, le **CEA** et le **CNRS** pilotent également la recherche quantique au travers de plusieurs laboratoires comme le **LETI**[99], l'**IRIG**[100] ou l'**Institut Néel**[101].

5. Décryptage pour comprendre le quantique

Sans entrer dans les formules mathématiques absconses pour le commun des mortels, voici un ensemble d'éléments qui permettent *à minima* d'être sensibilisé à l'esprit de la physique quantique.

5.1. A la base, 3 principes quantiques

La mécanique quantique s'appuie sur plusieurs principes, plutôt contre-intuitifs, qui, mis ensemble, lui permettent de résoudre des problèmes bien plus rapidement qu'un algorithme classique : le principe d'indétermination (ou d'incertitude) ; la superposition d'états ; le phénomène d'intrication.

LE PRINCIPE D'INDETERMINATION (OU D'INCERTITUDE)

À l'échelle humaine, la nature est déterministe : à un instant **T1** il est possible de déterminer la position et la vitesse d'un objet dans la nature, et de pouvoir calculer dans quel état il sera à un instant **T2**.

Un système quantique, lui, est non déterministe. Les particules peuvent être représentées soit par une onde, soit par un paquet d'ondes. Mais on ne sait pas déterminer à la fois la vitesse et la position d'une particule : si on la représente comme une onde on peut connaître sa vitesse mais pas sa position, si on la représente comme un paquet d'ondes on sait déterminer la position de ce paquet mais pas sa vitesse.

Comme ni sa position ni sa vitesse ne peuvent être mesurées en même temps, dans un système quantique on considère qu'un objet pourrait être « en plusieurs endroits en même temps » ou qu'il n'a pas de localisation tant que la position n'est pas mesurée. C'est le principe d'indétermination, ou d'incertitude.

> Pour comprendre ce principe, imaginons que dans une chambre complètement noire dans laquelle circule un objet très rapidement, il faille prendre en photo l'objet avec un flash. Ne sachant pas où il est, on « mitraille » au hasard. Mais sur les photos produites, soit l'image est nette et l'on peut déterminer où se trouve l'objet mais pas sa vitesse ; soit l'image est floue, on ne peut plus

[99] LETI : Laboratoire d'électronique et de technologie de l'information : http://www.leti-cea.fr/
[100] IRIG : Institut de Recherche Interdisciplinaire de Grenoble : http://www.cea.fr/drf/irig
[101] http://neel.cnrs.fr/

déterminer où se trouve l'objet mais suivant la longueur de la trainée de l'objet, on peut calculer sa vitesse. Il n'est donc pas possible de savoir en même temps où est l'objet et à quelle vitesse il va : on a une information partielle.

LA SUPERPOSITION D'ETATS

La physique classique est outillée de tout un ensemble d'équations mathématiques qui permettent de déterminer l'état d'un objet, sa position, sa vitesse, son poids, etc… Par rapport à un instant donné, il est possible de mesurer précisément la ou les caractéristiques de cet objet sans pour autant le perturber, l'observation ne modifie pas son état. On peut ainsi si l'on connait la masse et la force de la pesanteur, calculer facilement le poids d'un objet à un moment T.

Dans le monde quantique, il n'est pas possible de déterminer ces valeurs pour des particules. Mais on peut les approcher de manière probabiliste. Par exemple, une particule peut être à X% dans un état particulier, à Y% dans un autre état et encore à Z% dans un troisième état... et le nombre d'états peut être infini. D'une certaine manière une particule peut-être « au même moment » *plus ou moins* dans une « infinité » d'états différents. La description d'un système quantique montre donc plusieurs états qui coexistent en même temps. C'est le principe de superposition d'états.

Au moment où l'on fait une mesure, un résultat probabiliste apparait. Et si l'on fait la même mesure sur n particules identiques, c'est la convergence des résultats probabilistes mesurés sur chacune d'entre elles qui donne un résultat acceptable.

Pour comprendre ce principe, imaginons un menuisier[102] qui veut fabriquer à partir d'un morceau de bois une guitare, une chaise, ou tout autre objet sorti de son imagination. Les possibilités sont infinies. Elles sont là, mais sous forme de potentialités : il est probable, en fonction de différents facteurs (marché, clients, temps humide ou non, type de bois etc…) qu'il fabrique l'un ou l'autre objet ou un troisième. Le morceau de bois à lui seul superpose donc toutes ces potentialités. Mais une fois ce morceau de bois travaillé, un seul objet est réalisé et toutes les autres possibilités de réalisation disparaissent.
Si l'opération est répétée n fois, la convergence des objets fabriqués peut nous permettre de dire que cet ébéniste est spécialisé dans la fabrique de guitares, ou de chaises, ou d'un autre objet.

[102] Exemple inspiré de l'article https://www.gbnews.ch/ordinateur-quantique-2-le-principe-de-superposition/

LE PHENOMENE D'INTRICATION

Ce troisième principe de la mécanique quantique indique qu'il est possible de créer un système lié composé de plusieurs particules dont les états dépendent les unes des autres, et ceci quelle que soit la distance qui les sépare (c'est ce à quoi Albert Einstein ne voulait pas croire).

Dans ce système lié, le comportement de chaque particule n'est pas individuel : il se comporte de manière collective. La mesure d'une information sur l'une des particules du système se répercute immédiatement sur les autres où qu'elles soient. On dit que ces particules sont intriquées, c'est le principe d'intrication.

Une fois que l'information portée par une particule du système est connue (mesurée), elle est figée (ou répercutée) sur toutes les autres particules du système et on ne peut plus la changer.

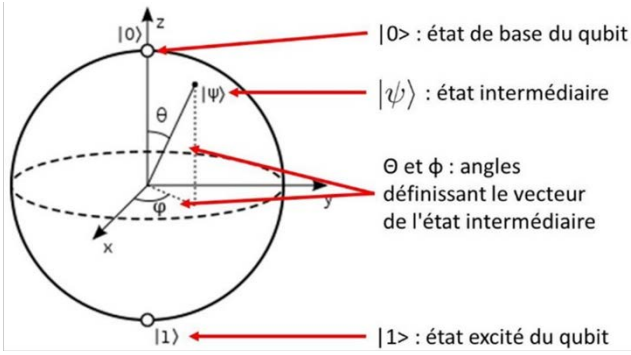
> Pour comprendre ce principe, imaginons que l'on coupe une chemise en deux parties (gauche et droite). À l'aveugle, on met chaque partie de la chemise dans deux boites différentes. Ces deux boites sont envoyées en deux endroits différents, par exemple New-York et Tokyo. Une fois arrivée à Tokyo, la boite est ouverte contenant la partie gauche de la chemise. Du coup on a instantanément l'information que la partie droite se trouve à New-York, et ceci sans ouvrir la boite de New-York. L'information de New-York s'est donc « propagée instantanément » vers Tokyo. De même notre correspondant tokyoïte peut, sans avoir ouvert sa propre boite, appeler son correspondant de New-York et lui demander d'ouvrir sa boite : l'observation du contenu par le correspondant new-yorkais, lui permet de transmettre immédiatement l'information du contenu de la boite de Tokyo sans pour autant l'avoir ouverte. Il y a donc bien une sorte de lien immédiat entre les deux boites quant à l'information sur leur contenu, une sorte de collaboration implicite entre les deux boites.

5.2. Le Qubit, unité de base de l'informatique quantique

BIT *VS* QUBIT / DETERMINISME *VS* PROBABILISME

Comme tout le monde le sait, le bit est l'unité de base de stockage d'une information dans l'informatique classique. Généralement cela correspond à la création d'une charge électrique qui exprime le passage du courant, possible ou pas. Si le courant passe, le bit est à 1, si le courant ne passe pas, le bit est à 0. La lecture du bit ne donne donc que deux valeurs : 0 ou 1. Cette lecture est déterministe : si on la répète plusieurs fois on obtiendra toujours le même résultat.

En informatique quantique, l'unité de base de stockage d'une information est le Qubit. On peut représenter l'état d'un Qubit par un point sur une sphère (qu'on appelle la sphère de Bloch[93]). Cette sphère porte les états que peut prendre une particule : de base ou excité. Imaginons que le « pôle nord » de la sphère soit l'état de base (noté |0>) et le « pôle sud » l'état excité (noté |1>), entre les deux se trouvent une infinité de points possibles : un Qubit peut donc avoir autant d'états quantiques que de points sur une sphère, il peut donc être « plus ou moins » 0 ET « plus ou moins » 1, dit autrement il peut être à la fois dans l'état 0 et dans l'état 1 mais dans une proportion qui est variable : sa lecture est probabiliste.



Source FrenchWeb

Figure 3 : Sphère de Bloch

Tous ces états intermédiaires sont représentés par ce que l'on nomme des vecteurs[103]. Entre le moment où le Qubit est initialisé à 0 et le moment final où l'on lit sa valeur de sortie (0 ou 1), l'information peut être manipulée au travers de ce qui peut prendre une infinité d'états superposés. Au final lorsque l'on lit la valeur du Qubit, on retombe sur un 0 ou un 1 mais avec un retour probabiliste dépendant des paramètres du vecteur de l'état du Qubit. La richesse mathématique du Qubit intervient donc pendant, et seulement pendant, les traitements. Mais pas au départ ni à la fin des traitements.

Alors qu'un ordinateur classique va exécuter N combinaisons ou instructions de manière séquentielle et ne fournira un résultat qu'au bout de la chaine d'instructions, la superposition d'états d'un Qubit permet d'avoir un système à 2^N combinaisons simultanées qui produira une solution immédiate au moment de sa mesure, permettant ainsi de démultiplier la puissance de calcul.

Le principe d'intrication, lui, permet de synchroniser plusieurs Qubits en des lieux différents ou d'en faire des copies. Et si on fait une mesure sur l'un, comme lire l'information transportée, l'ensemble des autres Qubits intriqués en sont immédiatement affectés.

ERREURS, BRUIT ET DECOHERENCE QUANTIQUE

Les technologies mises en œuvre dans les ordinateurs classiques sont aujourd'hui suffisamment performantes pour créer de l'information, la transmettre, la copier, la regénérer, la stocker… Certes les composants électroniques classiques produisent des erreurs, mais aujourd'hui, avec très peu de ressources (mémoire, CPU) il est possible de les corriger pour obtenir un taux de fiabilité de 100%.

[103] https://www.frenchweb.fr/comprendre-linformatique-quantique-qubits/330991

On n'en n'est pas encore là avec les technologies quantiques. En effet elles sont extrêmement sensibles aux interactions avec leur environnement (ce qu'on appelle « le bruit ») et les Qubits tendent à perdre très rapidement leurs propriétés quantiques (superposition d'états, intrication…). C'est ce que l'on appelle la décohérence. Et si la décohérence intervient avant la fin de l'exécution d'un algorithme quantique, cela équivaut à le rendre inutilisable.

Plusieurs stratégies existent pour essayer de résoudre ce problème :

- Soit exécuter des codes de correction d'erreur. Mais eux-mêmes nécessitent des Qubits pour s'exécuter. Ce qui implique au final de pouvoir créer et maintenir en cohérence un nombre de Qubits important (ceux pour l'exécution de l'algorithme et ceux pour la correction d'erreurs) et c'est compliqué aujourd'hui de générer un nombre important (plusieurs centaines) de Qubits. Ce qui implique de ne pouvoir exécuter que des algorithmes courts nécessitant peu de code.
- Ou bien adapter les ordinateurs aux algorithmes (suivant la technologie utilisée, les Qubits sont plus ou moins sensibles à tel ou tel type de bruit). Mais dans ce cas, l'ordinateur devient dédié à un type d'algorithme qui doit néanmoins toujours être optimisé. Des équipes travaillent actuellement à mettre en œuvre une approche par apprentissage pour traduire un circuit quantique en un équivalent algorithmique extrêmement court et adapté à un ordinateur quantique spécifique.

5.3. Les principaux types d'ordinateurs quantiques

LES ORDINATEURS ANALOGIQUES MAIS D'INSPIRATION QUANTIQUE

Ce sont des systèmes « classiques » qui peuvent utiliser des effets quantiques pour résoudre ou émuler un problème spécifique. Ils ont une « programmabilité » limitée mais sont plus rapides que des ordinateurs utilisant des algorithmes conventionnels. Une question subsiste néanmoins : ces simulations logicielles sur des ordinateurs non quantiques obtiennent-elles les mêmes résultats ?

LES ORDINATEURS QUANTIQUES DE GENERATION INTERMEDIAIRE (NISQ)

Ce sont des dispositifs quantiques qui ne sont pas tolérants aux fautes. Ils n'ont pas la précision suffisante mais ils permettent de démontrer que cela marche, que les algorithmes sont valides. Ils sont construits dans le but de démontrer des applications utiles en interagissant avec un système informatique classique, par exemple en chimie ou pour faire de l'optimisation. Aujourd'hui de nombreuses startups travaillent sur ce concept, et notamment avec des algorithmes hybrides (quantique/classique). Pour être vraiment efficaces ils devraient avoir entre 1000 et 5000 Qubits.

LES ORDINATEURS QUANTIQUES UNIVERSELS A TOLERANCE DE PANNE

Ces ordinateurs représentent le Graal de la science de l'informatique quantique. Ils devraient permettre d'exécuter des algorithmes quantiques utiles et accélérer de façon exponentielle les calculs par rapport aux algorithmes classiques. Cependant, pour mettre en place un taux de correction d'erreur quantique efficace, il faudrait que ces ordinateurs aient entre 1 et 5 millions de Qubits.

5.4. Les technologies matures et celles au stade de la recherche

Produire des Qubits stables est essentiel pour pouvoir effectuer des opérations et exécuter de manière complète des algorithmes. Si la théorie de la mécanique quantique date du début du 20ème siècle, les technologies quantiques qui produisent des Qubits qui pourraient être les briques de base d'un ordinateur quantique sont très récentes et surtout diverses. Or si ces technologies savent produire des Qubits de différentes façons, toutes les approches n'ont pas la même maturité ou impliquent des contraintes qui affectent leur efficacité ou orientent les usages possibles.

LES CIRCUITS SUPRACONDUCTEURS

Les technologies à base de circuits supraconducteurs sont celles qui apparaissent comme étant les plus avancées. Elles permettent de créer des Qubits extrêmement rapides et leur assemblage est aussi plus facile. Néanmoins le faible temps de cohérence et le taux important d'erreur des Qubits sont leurs principaux défauts. De plus, la miniaturisation d'un système n'est, pour le moment, pas aisée.

Parmi les pionniers, on compte les chercheurs français du CEA qui ont créé le premier Qubit supraconducteur en 2002. À ce jour, IBM, Intel, Google, Rigetti, D-Wave, l'Inria et d'autres acteurs travaillent sur des circuits supraconducteurs.

LES IONS PIEGES

Les technologies à base d'ions piégés (maintenus sous vide et suspendus par suspension électrostatique) sont également extrêmement intéressantes, pour d'autres raisons : les Qubits produits sont de très bonne qualité. En effet, même s'ils sont assez lents et si dépasser la centaine de Qubits s'avère compliqué, leur isolation vis-à-vis de l'environnement est importante, donc le bruit (générateur d'erreurs) est très faible. De plus ils peuvent être intriqués de manière efficace. Enfin grâce aux lasers, il est aisé de préparer et mesurer des superpositions quantiques intriquées réalisées avec un petit nombre d'ions. Mais le système est encore difficilement miniaturisable.

Il n'y a pas d'équipe en France qui travaille sur les ions piégés. Aux USA, la startup IonQ issue de l'université de Maryland, est le principal acteur qui travaille sur ce sujet avec l'université d'Innsbruck

en Autriche et sa *spin off* AQT. IonQ a notamment créé récemment 80 Qubits inscrits dans des ions piégés et démontré l'avantage quantique[104].

LES QUBITS EN SILICIUM A SPIN D'ELECTRONS (OU QUANTUM DOTS, OU CMOS SELON LES APPELLATIONS)

C'est la voie choisie par Intel et le CEA au Leti et en collaboration avec le CNRS. Elle est poursuivie par plusieurs autres acteurs : l'université de Princeton, l'UNSW en Australie, le CEA-Leti et le CNRS en France, et Quantum Motion Technologies au Royaume-Uni.

LES CENTRES NV

Cette technologie utilise des impuretés dans des cristaux de diamants. Les Qubits sont difficiles à fabriquer de manière reproductible et l'intrication est compliquée à mettre en œuvre. C'est la voie choisie par Quantum Diamond Technologies. Les universités de Delft, Stuttgart, Harvard, Chicago et Hefi travaillent sur cette technologie.

LES FERMIONS DE MAJORANA

Il s'agit de Qubits topologiques qui utilisent une particule singulière, le fermion de Majorana, à la fois particule et antiparticule, et qui possèdent intrinsèquement un état quantique. Bien qu'incertaine à ce jour, l'existence des fermions de Majorana n'étant pas encore prouvée, cette technologie présenterait l'avantage de permettre la création de Qubits très stables et durables, deux paramètres clés de l'efficacité des ordinateurs quantiques. C'est la voie choisie par Microsoft et Bell Labs. Les universités de Delft, du Maryland, de Californie (Santa Barbara) et l'Institut Niels Bohr travaillent également sur cette technologie.

LA PHOTONIQUE QUANTIQUE

Alain Aspect, et son équipe dans les années 1980, avait démontré la réalité des corrélations quantiques non-locales à l'aide de paires de photons. Cette technologie s'appuie sur l'intrication de photons, ces derniers étant la clé pour sécuriser des communications sur des longues distances.

La photonique quantique est une technologie très prometteuse pour le calcul quantique, qui permet de s'affranchir des problèmes de décohérence, de réaliser les calculs à température ambiante et de s'appuyer sur les techniques de nanotechnologies optiques classiques pour réaliser des processeurs à grande échelle. L'université de Paris Saclay, comme l'Université Côte d'Azur avec l'INPHYNI, travaille sur ces technologies quantiques optiques.

[104] Voir le paragraphe « Atteindre l'avantage quantique » du chapitre 3.1. Enjeux technologiques

Au service de la croissance économique et de la compétitivité de nos membres, grandes entreprises et administrations publiques françaises, utilisatrices de solutions et services numériques, par la réussite du numérique

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

1/ Appartenance :
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

2/ Intelligence :
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

3/ Influence :
Le Cigref diffuse, promeut et défend les positions collectives de ses membres sur leurs enjeux numériques. Organisation indépendante de réflexion, d'échange et de production de contenus entre praticiens et acteurs du numérique, le Cigref est une référence reconnue par son écosystème.

www.cigref.fr

21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr