

Opinions Libres

le blog d'Olivier Ezratty

Comprendre l'informatique quantique – basiques

Après avoir fait le tour des plus grands contributeurs de la mécanique et de l'informatique quantique, passons aux grands fondamentaux de la physique quantique qui nous permettront de comprendre la suite et notamment le fonctionnement des qubits et de leurs diverses techniques de mise en œuvre.

Plusieurs années d'études sont nécessaires pour comprendre les arcanes de la mécanique quantique et ceux qui sont passés par là sont toujours dans l'interrogation à son sujet. Mais on peut se contenter de quelques basiques ici présents pour se préparer à comprendre le fonctionnement des calculateurs quantiques.

Le point essentiel est de bien appréhender la notion de **superposition d'états** qui est à la base du fonctionnement des qubits et de l'énorme capacité de traitement des calculateurs quantiques. L'**intrication** vient juste après et permet d'expliquer comment fonctionnent les portes quantiques dans les calculateurs quantiques, que nous verrons dans la partie dédiée au fonctionnement de ces derniers.

La mécanique quantique est apparue il y a un peu plus d'un siècle pour expliquer le fonctionnement et la dynamique des particules élémentaires. Les principales particules élémentaires à qui s'appliquent les principes de la mécanique quantique sont les **photons** et les **électrons**. Les effets quantiques les plus connus se manifestent sur la phase des photons ainsi que sur les niveaux d'énergie ou les spins d'électrons, ces derniers étant liés en approximation à leur orientation magnétique.

Tous les qubits connus d'ordinateurs quantiques s'appuient sur l'une de ces deux particules. A part le cas des qubits réalisés à base de photons, tous les autres sont à base de différents comportements quantiques d'électrons. C'est le cas des qubits à base de supraconducteurs à effet Josephson qui exploitent des effets très particuliers que nous expliquerons plus tard, reposant sur le comportement des électrons de matériaux supraconducteurs. Les ions piégés, les cavités de diamants, les qubits CMOS et même les qubits à base d'anyons et des hypothétiques fermions de Majorana exploitent eux-aussi les effets quantiques des électrons.

Des phénomènes quantiques peuvent se manifester avec d'autres particules élémentaires comme les atomes, les neutrons et les protons mais ce ne sont pas à ce jour des pistes explorées par les chercheurs dans le contexte du calcul quantique.

Voici un petit schéma de mon cru qui connecte entre eux les principes de base de la physique quantique que nous allons explorer. Il fournit quelques relations de causalité entre ces différents principes. Ainsi, c'est la quantification des propriétés d'un quantum qui aboutit à leur superposition. Cette dernière entraine l'indéterminisme de la mesure de l'état d'un quantum et la notion de réduction.

L'ensemble est représenté mathématiquement par un vecteur d'état qui contient deux nombres complexes, pour ce qui est des quantums à deux états possibles. Les propriétés mathématiques des vecteurs d'état s'expliquent par la dualité onde-particule des quantum et la possibilité d'additionner les ondes liées aux différents états des quantum. La dualité onde-particule est liée à la notion d'intrication qui elle-même explique le théorème de non

clonage ainsi que l'effet tunnel. C'est peut-être approximatif mais permet de se faire une idée de l'architecture d'ensemble.

quantification états quantiques = propriétés physiques discontinues (phase non clonage photon, spin électron, ...] intrication impossibilité de cloner possibilité d'associer des l'état d'un quantum quantums qui partagent des indépendamment de sa propriétés communes source représentation superposition vecteur d'état cohabitation de eprésentant l'état d'un plusieurs états de quantum dualité onde particule effet tunnel plusieurs états de base nature ondulatoire des quantum pouvant être interprété à la fois quantums qui leur comme particule et permet de traverser des réduction comme onde barrières énergétiques résultat de mesure mesure = état de aléatoire de l'état base le plus proche d'un quantum de l'état courant

liaisons entre concepts de la physique quantique

En parcourant de nombreux ouvrages sur la physique quantique et l'informatique quantique, j'ai pu constater que la pédagogie y était des plus variée. Le formalisme mathématique y prend rapidement le dessus de la description physique des phénomènes quantiques. Il est tellement prédominant qu'il ne correspond pas forcément à la réalité physique des quantums. Il est généralement très mal expliqué comme nous le verrons dans la partie suivante pour ce qui est du modèle de représentation de la sphère de Bloch.

(cc) Olivier Exatty, 2018

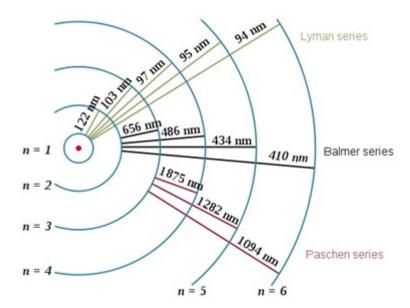
Je vais toutefois essayer de vous épargner cela dans ce qui suit à la fois parce que c'est un véritable tonneau des Danaïdes et parce que cela perdrait une grande majorité de lecteurs. Et même avec ces précautions, rien ne dit que tous vont suivre. Dans la physique quantique, il faut avoir systématiquement l'humilité de reconnaître que l'on ne sera pas forcément compris et/ou que l'on s'est mal expliqué!

Voyons donc cela dans le détail!

Quantification

En physique quantique, les quantums correspondent à des propriétés physiques de particules élémentaires matérielles ou immatérielles qui sont discontinues et non continues. Cela peut correspondre à des états énergétiques, des polarisations pour les photons, ou des orientations magnétiques pour les électrons.

Les orbites des électrons autour de noyaux d'atomes sont définies de manière discrète comme nous l'avons vu dans la **partie précédente** sur l'atome d'hydrogène avec les travaux de Max Planck en 1900, Albert Einstein en 1905 et Niels Bohr en 1913 (schéma *ci-dessous*).



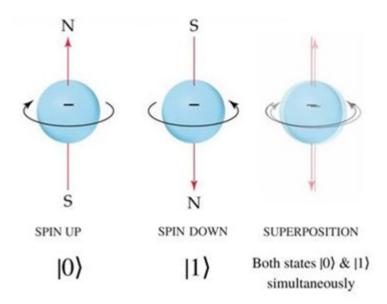
Il existe aussi une correspondance entre l'énergie des photons et les transitions énergétiques discontinues des électrons en orbite autour des atomes. Dans le calcul quantique, ce principe est utilisé un peu partout, surtout pour distinguer deux états clairement séparés dans les qubits.

Les qubits utilisés dans les calculateurs quantiques doivent s'appuyer sur des quantums qui n'ont que deux états possibles qui peuvent être à la fois initialisés, modifiés et ensuite mesurés. Même les qubits supraconducteurs s'appuient sur deux niveaux d'énergie clairement distincts du courant oscillant qui traverse leur isolant à effet Josephson.

Superposition

La superposition a un lien direct avec la quantification qui porte sur les différents états des particules élémentaires.

Les particules quantiques peuvent avoir plusieurs états simultanément, comme le sens de magnétisation du spin d'électron qui est orienté vers le haut ou vers le bas – cf schéma *ci-dessous* –, la polarisation linéaire des photons, qui est horizontale ou verticale après passage au travers de filtres polarisants, ou la fréquence ou l'énergie d'un courant oscillant dans un qubit supraconducteur.

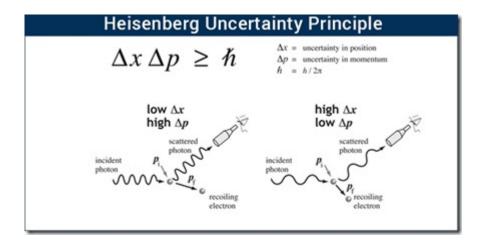


Le principe de la superposition veut qu'une particule élémentaire puisse être simultanément dans plusieurs de ces états quantiques. Dans une interprétation de physique classique, cela serait explicable par une fréquence très élevée des modifications d'états de ces particules. Elle est peut-être inexacte pour les spécialistes mais c'est un moyen intuitif de se représenter ce principe de la superposition.

En calcul quantique, ce principe est utilisé dans les qubits, leur permettant d'avoir en même temps la valeur 0 et 1 au lieu d'avoir seulement l'une des deux valeurs comme avec les bits traditionnels. C'est cela qui permet aux calculateurs quantiques de paralléliser les calculs à un niveau inégalé comparativement aux meilleurs supercalculateurs classiques. S'il n'y a qu'un élément de mécanique quantique à retenir pour comprendre les ordinateurs quantiques, c'est bien celui-ci!

Indéterminisme

Il intervient lors de la mesure de l'état d'un quantum. Le résultat est en partie aléatoire. La mesure de la polarisation d'un photon va donner des résultats différents d'un coup à l'autre dans une proportion de phases qui dépend de son état quantique. Si les photons évalués ont suivi un processus de transformation identique, en réalisant un grand nombre de mesures, on va obtenir une proportion donnée de phases horizontales et verticales.



Si la mesure donne un résultat aléatoire, la proportion des états évalués ne l'est pas pour autant. Réalisée plusieurs fois, elle va converger tangentiellement vers une proportion qui dépend des conditions de préparation d'un quantum. Si on prend l'exemple de photons polarisés à 45°, leur mesure de polarisation verticale et horizontale va converger vers une proportion de 50%/50%. Si les photons mesurés sont polarisés à seulement 5°, la proportion de photons évalués comme étant polarisés verticalement (0°) sera plus grande que celle de deux qui sont polarisés horizontalement.

En informatique quantique, ce principe est utilisé lorsque l'on mesure le résultat d'un calcul en évaluant l'état des qubits de l'ordinateur quantique. Dans les ordinateurs à recuit quantique de D-Wave, on va généralement réaliser cette mesure plusieurs fois pour obtenir une moyenne de 0 et de 1, en exécutant à chaque fois une réinitialisation complète du système et un calcul complet. La recherche de 0 ou de 1 déterministes ou de proportion probabiliste de 0 et 1 donnant une moyenne va dépendre des algorithmes utilisés. C'est un peu l'analogue en informatique traditionnelle de calculs générant un résultat booléen (0 ou 1) ou un nombre flottant (ici, compris entre 0 et 1).

Réduction

La réduction explique dans le détail la nature de l'indéterminisme de la mesure de l'état des quantums.

Lorsque l'on mesure un état d'un quantum, celui-ci est affecté par la mesure. La mesure change l'état du

quantum. Celui-ci se rabat en quelque sorte sur l'état de base le plus proche de son état avant la mesure que l'on appelle un "observable". L'état "pur" avant la mesure est une combinaison d'états de base du quantum. Par exemple, une combinaison de polarisation verticale et horizontale pour un photon.

On appelle aussi cela "l'écrasement de la fonction d'onde de Schrödinger". Pourquoi donc ? Parce que qu'un quantum multi-états superpose plusieurs états distincts qui sont représentés chacun par une fonction d'onde. L'état composite de deux fonctions d'ondes est aussi une fonction d'onde. Lorsque l'on mesure l'état d'un tel quantum, c'est l'état de base le plus proche des états superposés qui est détecté. Et qui devient l'état du quantum qui vient d'être mesuré. Etat qui est associé à une fonction d'onde, celle qui est obtenue par écrasement! Vous suivez ? Non ? C'est normal, ne vous inquiétez pas.

Prenons l'exemple d'un photon de polarité intermédiaire entre la polarité horizontale ou verticale, ou de polarisation circulaire. Il va devenir un photon polarisé horizontalement ou verticalement après sa mesure de polarité.

La notion de réduction est une application pratique du fameux principe d'Heisenberg selon lequel la mesure de l'état d'un quantum influe sur la grandeur à mesurer dans l'infiniment petit, alors que ce n'est pas le cas dans la mécanique newtonienne classique. Le principe d'indétermination d'Heisenberg dit précisément que l'on ne peut pas mesurer à la fois la position et la vitesse d'une particule élémentaire. Intuitivement, cela se comprend : en mécanique newtonienne, l'outil de mesure est en général plus petit que la grandeur à mesurer, comme pour évaluer la vitesse des astres et des planètes. Dans l'infiniment petit, l'outil de mesure est habituellement bien plus grand que la grandeur physique à mesurer. D'où la perturbation sur la grandeur à mesurer!

Pour les puristes, la notion de vitesse et de position des particules n'a pas de sens, pour ce qui est par exemple d'un électron. Sa caractérisation passe par sa nature ondulatoire et par sa description via la fonction d'onde de Schrödinger.

En informatique quantique, ce principe de réduction est en œuvre lors de la mesure de l'état d'un qubit, qui modifie sa valeur en la rabattant à 0 ou 1. Le 0 et le 1 mesuré est, en gros, la valeur la plus proche de son état quantique du moment qui est une combinaison de 0 et de 1. C'est illustré dans le schéma *ci-dessous*. Nous reviendrons sur la signification de alpha et beta dans l'article suivant sur les qubits, ces deux variables étant en fait des nombres complexes ou des vecteurs à deux dimensions.

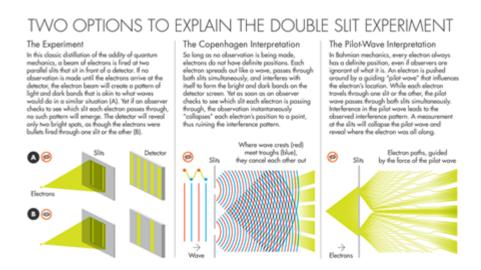
La subtile information contenue dans un qubit qui est représentée par un nombre complexe ou un vecteur à deux dimensions est réduite à 0 ou 1 au moment de sa mesure. Mathématiquement, on a donc bien une réduction d'une information riche comportant l'équivalent de deux nombres flottants à un simple bit!

Cette réduction intervient au dernier moment après les calculs. Pendant ces derniers, les qubits sont modifiés par des portes quantiques qui conservent la richesse de leur information et la combinatoire de leurs valeurs liée à la superposition.

Dualité ondes particules

Les particules élémentaires ont des comportements qui relèvent à la fois des particules avec une masse et comme des ondes avec leurs effets comme l'interférence et le fait qu'elles peuvent s'additionner pour donner d'autres ondes. Un peu comme les couleurs (photons) et les sons (ondes acoustiques) se mélangent.

Diverses expériences comme celle des doubles fentes de Young montrent que les électrons qui sont des particules matérielles avec une masse se comportent à la fois comme des particules et comme des ondes, générant des interférences. Les équations de Planck, Einstein et Bohr donnent la correspondance entre photons et états énergétiques d'atomes liés à la position orbitale des électrons.



La dualité ondes/particules est utilisée dans nombre d'ordinateurs quantiques pour faire interagir des qubits physiques comme des ions piégés avec de l'énergie sous forme de photons émis par des lasers. Les qubits peuvent aussi interférer les uns avec les autres en reproduisant une partie de ce mécanisme d'interférence ondulatoire.

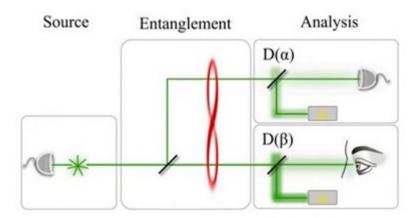
Cette dualité ondes-particules explique aussi pourquoi le formalisme mathématique de la physique quantique s'appuie sur des vecteurs qui peuvent s'additionner comme des ondes.

On comprend donc que les électrons ont cette capacité à se comporter comme des particules et comme des ondes. Mais qu'en est-il des photons ? Ils peuvent se comporter dans certaines conditions comme des particules. Lorsqu'ils atteignent un atome, ils peuvent ainsi lui transmettre un mouvement cinétique. C'est ce qui permet de générer un phénomène physique un peu contre-intuitif : le refroidissement d'atomes avec des lasers. La température est liée au mouvement des atomes dans leur milieu gazeux, liquide ou solide. Si on envoie des photons vers des atomes dans une direction opposée à leur mouvement, cela va ralentir ce dernier et ainsi refroidir l'ensemble ! Ces techniques sont utilisées pour refroidir des atomes à des températures voisines du zéro absolu.

Intrication

Des quantums peuvent être intriqués, à savoir qu'ils peuvent avoir la même fonction d'onde ou représentation quantique alors qu'ils sont distants. Bref, être dans un état quantique similaire, sans être pour autant strictement identique, ne serait-ce qu'au niveau de leur localisation spatiale. C'est le principe de la non localité des propriétés quantiques de quantums intriqués qui perturbait Einstein en 1935. L'intrication est dénommée "entanglement" en anglais.

Ainsi, avec une paire de quantums intriqués, une mesure effectuée sur un quantum aura instantanément un effet sur l'autre quantum, sans attendre un délai de transmission d'information à la vitesse de la lumière entre les deux quantums. C'est le principe de la "non localité" des propriétés quantiques.



Les particules intriquées ne sont pas liées par hasard. Elles ont généralement un passé commun. Par exemple, deux photons intriqués sont le résultat du passage d'un seul photon dans un miroir dichroïque qui les sépare en deux photons de polarisations orthogonales. L'action sur l'un des deux photons a un impact sur l'autre photon comme l'a démontré Alain Aspect dans sa fameuse expérience réalisée en 1982.

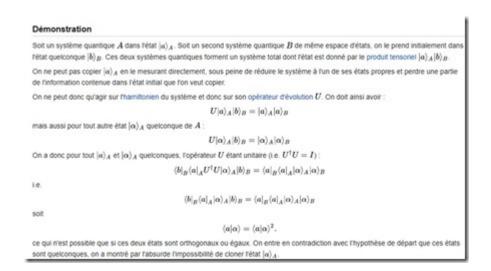
En informatique quantique, ce principe est utilisé dans les portes quantiques à deux ou trois qubits, pour les relier entre eux. Une fois intriqués, les qubits ont le même état quantique indissociable. Cette intrication est associée à une impossibilité de dissocier les quantums ainsi intriqués.

Non clonage

Le théorème d'impossibilité du clonage quantique a été énoncé en 1982 dans un article publié **dans Nature** par William Wootters, Wojciech Hubert Zurek et Dennis Dieks. L'article n'est toujours pas disponible en open source sur un site tel que Arxiv, s'auto-appliquant le principe du non clonage! Mais une version résumée est consultable **ici** (*ci-dessous*).



Il interdit la copie à l'identique de l'état d'un quantum. Le théorème se démontre mathématiquement en six lignes (*ci-dessous*) même si chaque mot de la démonstration nécessite quelques recherches préalables pour être compris ! Il a comme conséquence qu'il est impossible de copier l'état d'un qubits pour l'exploiter indépendamment de son original.

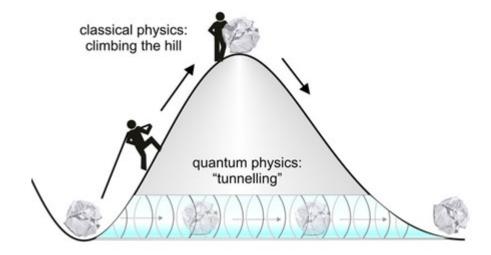


Dans les ordinateurs quantiques, on peut bien dupliquer des qubits via des portes quantiques et l'intrication, mais les qubits résultants sont intriqués et donc en quelque sorte synchronisés. La lecture de la copie détruit l'original par projection de l'état des deux qubits sur le 0 ou le 1 le plus proche de leur état initial.

Cela a un impact direct sur la conception d'algorithmes quantiques et notamment sur les codes de correction d'erreurs des ordinateurs quantiques. Heureusement, ces codes de correction d'erreurs ne nécessitent pas de lire le contenu des qubits clonés et échappent donc aux foudres du théorème de non-clonage.

Effet tunnel

La double nature corpusculaire et ondulatoire de la matière lui permet de traverser des obstacles. Ces obstacles peuvent être des "murs énergétiques".

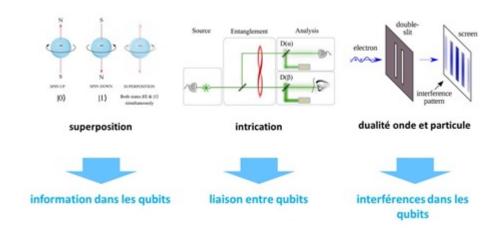


Ce phénomène est utilisé dans les ordinateurs à recruit quantique de D:Wave qui permettent de faire converger un système multi-qubits ("hamiltonien") vers un minimum énergétique correspondant à la résolution d'un problème de combinatoire complexe ou de recherche de minimum énergétique comme en chimie ou en biologie moléculaire.

Applications dans les qubits

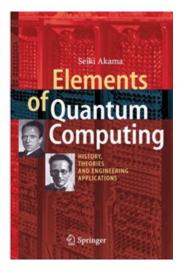
En résumé, voici les trois principes de base les plus importants sur les huit ci-dessus qui sont utilisés dans les qubits et que nous exploiterons dans l'article suivant portant sur ces derniers :

- La **superposition** permet d'avoir des qubits qui sont à la fois dans un état 0 et 1 et nous verrons plus tard dans quelle proportion et comment on la représente mathématiquement.
- L'intrication permet de relier entre eux les qubits pour les synchroniser, ce qui permet notamment d'en faire des copies, mais sans pouvoir en lire leur contenu ni les modifier de manière indépendante.
- La dualité onde-particule permet d'interagir dans certains cas avec les qubits ou de faire interagir les qubits entre eux par interférences dans le cadre d'algorithmes quantiques.



J'en profite pour vous recommander deux ouvrages, l'un sous forme de bande dessinée, le Mystère du monde quantique, de Thibault Damour et Mathieu Burniat et le second qui est téléchargeable gratuitement, Elements of Quantum Computing de Seiki Akama (133 pages) et qui est à la fois concis, précis et assez complet sur les recoins de la mécanique et de l'informatique quantiques, avec qui plus est une bonne vision historique.





Voici quelques autres sources, qui ne manquent pas, pour se faire la main en mécanique quantique : la conférence Introduction à la physique quantique de l'astrophysicien Roland Lehoucq donnée à l'Ecole Polytechnique en juin 2018 (1h16). Il est aussi l'auteur du très intéressant Faire des sciences avec Star Wars en 2015 (83 pages). Vous avez aussi les trois conférences d'Etienne Klein du CEA sur la physique quantique à

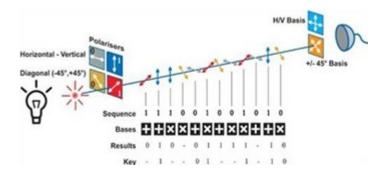
la Cité des Sciences de Paris, datant de 2007 et qui sont remarquables de pédagogie (cours 1, cours 2, cours 3) et durent en tout près de cinq heures ainsi que Comprenons nous vraiment la mécanique quantique de Franck Laloe (45 pages) et qui semble dater d'il y a au moins une quinzaine d'années au vu de sa bibliographie mais qui met au clair de nombreux débats scientifiques au sujet de la physique quantique.

Différentes facettes des applications du quantique

Ma série d'articles est très focalisée sur les calculateurs quantiques mais il ne s'agit pas de la seule application numérique du quantique.

On compte au moins quatre autres grands domaines dans le vaste secteur de l'information quantique :

• La cryptographie quantique qui est un moyen de diffusion de clés quantiques inviolables grâce au principe de l'intrication entre photons, et qui repose soit sur des communications par fibre optique, soit en liaison spatiale avec des satellites comme le font les Chinois avec le satellite Micius depuis 2017. Nous traiterons du sujet dans une partie dédiée. Il faut la distinguer de la cryptographie post-quantique qui est destinée à remplacer les solutions actuelles de cryptographie pour les rendre résistantes aux attaques réalisées avec l'algorithme de Shor tournant dans des ordinateurs quantiques. Nous nous y intéresserons aussi dans une partie dédiée de cette série.



- Les **télécommunications quantiques** qui permettent, grâce à l'intrication quantique de photons ayant un passé commun, de communiquer à distance et instantanément l'état de quantums. C'est un cas plus général que la cryptographie quantique qui en est un cas particulier. C'est un domaine en devenir car pour l'instant, on peut certes envoyer une information très rapidement, mais pas l'exploiter directement. En particulier, l'information a beau être transmise instantanément, donc plus vite que la lumière, on ne peut pas pour autant exploiter cette bizarrerie dans la communication d'informations.
- La **métrologie quantique**, qui permet de mesure des ordres de grandeur de l'infiniment petit avec une très grande précision. C'est un vaste domaine scientifique qui fait l'objet de nombreux travaux de recherche et à la commercialisation de solutions industrielles. Cela comprend les horloges à atomes ou ions froids ultra précises, les accéléromètres et gyromètres à atomes froids qui utilisent de l'interférométrie atomique, les gravimètres qui en sont une variante pour mesurer la gravité avec précision, que fabrique notamment le Français Muquans qui est basé à Bordeaux. Ce sont des marchés de taille modeste.

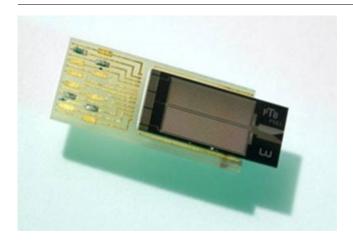
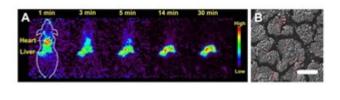


Table 1. Quantum Metrology and Sensing Technologies

Technology	Technological Readinessª	Potential Market
Measurement		
Atomic clocks	Commercial	\$50-\$500 million
Meters for voltage, current, and resistance	Commercial	_
Sensors		
Gravimeters and other atomic interferometers	Commercial	< \$50 million
Quantum inertial motion units	Medium-term	\$50-\$500 million
Atomic magnetometers	Commercial	\$50-\$500 million
Magnetoencephalography	Commercial	\$50-\$500 million
Quantum electron microscopes	Medium-term	\$50-\$500 million
Quantum-assisted nuclear spin imaging	Long-term	< \$50 million
Signal measurement	Medium-term	_

Sources: European Commission (2017) United States Air Force Scientific Advisory Board 2015; interviews.

• L'imagerie médicale quantique qui exploite diverses techniques dont les quantum dots, que l'on trouve aussi dans les écrans LCD pour améliorer leur colorimétrie.



Dans l'épisode suivant de cette série d'articles, nous allons nous pencher sur les fondamentaux des qubits en expliquant leur fonctionnement, leur curieux modèle de représentation mathématique utilisant la fameuse sphère de Bloch puis en faisant un tour rapide de la manière dont ils sont réalisés physiquement.

Cet article a été publié le 1 juillet 2018 et édité en PDF le 15 mars 2024. (cc) Olivier Ezratty – "Opinions Libres" – https://www.oezratty.net