

Enjeux et prospectives du développement des technologies quantiques

Challenges and Prospects in the Development of Quantum Technologies

Laurent Adatto¹

¹ Laboratoire ISI/Lab RII, Université du Littoral, Côte d'Opale, France, lradatto@yahoo.com

RÉSUMÉ. Cet article se propose d'analyser les multiples facettes relatives à l'avancement des technologies quantiques. Pour cela, les éléments de physique quantique nécessaires au développement de ces technologies sont d'abord explicités selon une perspective didactique. Puis les investissements relatifs aux technologies quantiques sont montrés, à visée exhaustive relativement au plan quantique français, et suivant des éléments de comparaison concernant les principaux plans internationaux d'envergure et les développements propres aux géants du numérique. Un horizon est mis en perspective comprenant facteurs de progrès matériels et sociaux liés aux technologies quantiques. Les risques et écueils potentiels sont aussi explicités, avec une focale particulière sur les éléments de cybersécurité liés aux technologies quantiques. Ainsi, des balises sont développées pour mieux appréhender la révolution quantique qui est en train d'advenir et sera dans un avenir proche à l'origine de bonds colossaux, vecteurs de progrès gigantesques, suivant la puissance prométhéenne quantique.

ABSTRACT. This paper analyzes the multiple facets related to the advancement of quantum technologies. To this end, the quantum mechanics necessary for the development of these technologies are first explained from a didactic perspective. Then, investments related to the progress of quantum technologies are shown, in an exhaustive way regarding the French quantum plan, and following elements of comparison concerning the main international plans and developments specific to digital giants. An overview is drawn up, including drivers of material and social progress related to quantum technologies. The potential risks and dangers are also explained, with a particular focus on the cybersecurity aspects of quantum technologies. Thus, guidelines and indicators are developed so that one can better understand the quantum revolution that is taking place and that will, in the near future, be at the root of colossal steps, vectors of gigantic progress, following on from Promethean quantum power.

MOTS-CLÉS. Technologies quantiques, Physique quantique, Investissements technologiques, Plan quantique, Cybersécurité, Innovation.

KEYWORDS. Quantum technologies, Quantum mechanics, Technological investments, Quantum plan, Cybersecurity, Innovation.

1. Introduction

1.1. Plan et méthodologie

Analyse des éléments de la physique quantique matriciels des technologies quantiques

Cet article se propose d'analyser les enjeux et prospectives liés aux technologies quantiques et à leur potentiel d'innovation radical. Tout d'abord, les éléments matriciels de la physique quantique seront montrés suivant une approche didactique.

Étude de cas du Plan Quantique français avec éléments de comparaison relatifs aux acteurs internationaux d'envergure

Puis seront analysés et détaillés les composants du plan d'investissement quantique français. En ce but une étude de cas sera réalisé. Pour cela, sera adoptée la méthodologie préconisée par Yin [YIN 14] dans la perspective d'examen en profondeur d'une étude étendue à visée globale d'un cas. À savoir, le Plan Quantique français tel qu'il fut lancé en janvier 2021. Considérant l'étendue des éléments relatifs à ce plan, la méthode la plus appropriée selon Yin pour ce type d'étude de cas sera

implémentée basée sur une recherche exploratoire permettant de constituer un inventaire détaillé de connaissances dans un cadre défini. A cette fin, seront systématiquement analysées les données relatives à ce cas qui comprennent les documents officiels des instances publiques liées ainsi que des parties prenantes impliquées dans l'organisation de ce plan, et également les interviews publiées par la presse spécialisée concernant ces investissements technologiques.

Sera montrée l'association du plan à la politique de relance française. Sera mis en exergue le passage de la recherche fondamentale aux développements applicatifs comme volonté du plan, ainsi que l'objectif de valorisation industrielle de la recherche. Sera décrite la démarche pour éviter une captation extérieure des brevets financés par le Plan Quantique français. Sera détaillée la répartition des financements selon les champs constituant les technologies quantiques, ainsi que les secteurs industriels et de haute technologie impliqués. Les éléments de cybersécurité liés aux technologies quantiques seront singulièrement analysés. Seront mis en exergue les risques associés à une main-mise de ces technologies à un stade avancé par des acteurs privatifs. En particulier, le futur ordinateur quantique universel [ANR 22] et ses capacités de calcul phénoménales et sans commune mesure avec les technologies informatiques classiques [INR 22] conférerait à la détention d'une puissance prométhéenne. Dans cette perspective seront analysés les développements quantiques d'envergure des géants du numérique. Enfin, les investissements des grands acteurs étatiques internationaux ayant mis en chantier des programmes analogues au plan français seront comparés.

2. Analyses des éléments de physique quantique au cœur des technologies quantiques

Physique quantique matrice des technologies quantiques

Les technologies quantiques mettent en œuvre des propriétés de la physique quantique qui sont inhérentes de la matière à la dimension de « l'infiniment petit », c'est-à-dire à l'échelle des atomes et en-deçà au niveau de particules subatomiques telles les électrons [LEB 13].

Le concept de physique quantique est apparu en 1900, dans le prolongement des travaux pionniers de Max Planck sur le rayonnement des corps noirs et des vibrations de chaleur engendrées selon une loi corrélée à une constante, ainsi appelée constante de Planck. Suivant ces travaux, puis les recherches postérieures à cette échelle dimensionnelle, est apparue qu'une quantité indivisible permettait d'engendrer une modification d'état. Cette propriété constitue la clé d'entrée dans la physique quantique. Elle a façonné l'étymologie associée : cette quantité indivisible étant intitulée en latin *quantum*, singulier de *quanta*. Elle est liée à une physique propre, quantique, différente du *corpus* physique découvert antérieurement, dites classique. En effet dans la physique classique, le passage d'un état à un autre est progressif et non lié à des valeurs bornées *a minima*.

Intégrée à la physique quantique, la mécanique quantique dont les principales branches sont la dualité onde - corpuscule, double forme de la matière à l'échelle de l'infiniment petit [GAU 21] (ainsi dans le cas de la lumière, photon sous sa forme corpusculaire et longueur d'onde sous sa forme ondulatoire), la superposition quantique (pour l'instant seulement appréhendée de façon théorique et mathématique et considérant qu'une particule ou un ensemble de particules peut être simultanément localisé à différents endroits suivant des probabilités associées différencierées), et l'intrication (deux particules ou ensemble de particules corrélés par leur état quantique quelle que soit la distance qui les sépare). Nous allons à la suite développer ces notions suivant leurs liens avec les technologies quantiques.

Intrication quantique

Ainsi, l'intrication associe de façon parfaite les états de deux parcelles distantes (possiblement selon des distances considérables) comme reliées par un fil invisible de type photonique pour ne former qu'un même système quantique. La cryptographie quantique puise dans cette caractéristique

d'intrication. Par là, à sa complétude de progrès, elle permettra d'engendrer des clés de codage absolu. En effet, casser le codage quantique, si jamais il était possible de le faire, ne pourrait se faire qu'au prix de la destruction de tout le système quantique intriqué suivant la rupture de la liaison photonique, et serait ainsi immédiatement détecté par les agents à l'origine du système.

L'intrication quantique a un potentiel d'innovation radical dans la cryptographie, l'information et l'ordinateur. Ces champs sont ainsi associés à la nomenclature quantique selon cryptographie quantique, information quantique et ordinateur quantique. Illustration du façonnage de technologies de très hauts niveaux par la propriété de l'intrication quantique, l'Union européenne a récemment programmé la mise en orbite d'un système de satellites mettant en œuvre cette technologie d'intrication quantique. De même la téléportation par transmission intégrale de l'information de l'état quantique de la matière devient possible et a même déjà été expérimentée avec succès au niveau de particules, et là encore elle prend le nom de téléportation quantique. Concernant la cryptographie quantique, l'intrication et ses agrégats de particules corrélés quelque soit la distance permettra donc quand opérative une sécurisation absolue. Là où la puissance potentielle de l'ordinateur quantique pourra permettre le décodage de toutes les clés de sécurité cryptographiques actuelles et non issues de la mécanique quantique. Ces enjeux démontrent le niveau d'innovation radicale associé au progrès des technologies quantiques.

Inventions pionnières de la physique quantique

La physique quantique a déjà engendré des innovations conséquentes sur les destinées du monde. Ces inventions pionnières comprennent les transistors, les circuits intégrés, les lasers, et les systèmes de localisation de type GPS [DAS 22].

Caractéristique de superposition quantique

La caractéristique quantique de superposition augure que des particules (matière, photon) puissent être assignées à deux états simultanés. La puissance de calcul de l'ordinateur quantique découle de cette caractéristique de superposition quand les ordinateurs classiques implémentent des instructions binaires. En conséquence, les calculs parallèles de l'ordinateur quantique ont un facteur de développement exponentiel par rapport aux ordinateurs classiques.

Des sciences quantiques à l'informatique quantique

Ainsi à la base de l'informatique quantique, comme montré, le comportement de la matière à l'échelle de l'infiniment petit, où les particules n'obéissent plus aux lois de la physique classique, par analogie celles qui régissent le fonctionnement des ordinateurs traditionnels sur un mode binaire (état 1 ou 0 de l'unité infractionnable du bit), mais à celles de la physique quantique où l'unité dédiée, le Qubit, peut revêtir simultanément les états de 1 et 0, et, au-delà, des combinaisons probabilistes de ces deux états [BID 22]. Telle est l'application du principe fondateur de superposition quantique dans le développement d'une informatique quantique.

Analyse du concept de Qubit

Ainsi, le Qubit est l'élément fondamental vecteur des mécanismes à la base du fonctionnement des ordinateurs quantiques. Parallèlement il est aussi l'unité de mesure de puissance de calcul quantique [ROL 21].

Differences structurelles entre ordinateurs classiques et ordinateurs quantiques

Ordinateurs classiques et ordinateurs quantiques sont fondamentalement différents. Cette dichotomie est présente à de multiples niveaux. Elle concerne la structure, l'architecture, les composants, les procédures opératives et l'algorithmie.

Par là, la puissance de l'informatique quantique, et son algorithmie optimale s'appuyant sur des processus probabilistes, est sans commune mesure avec celle de l'informatique traditionnelle. Et le sera encore davantage au fur et à mesure que les ordinateurs quantiques, ou partiellement quantiques d'abord, pourront intégrer un nombre croissant de Qubits. Ici, se situe encore les limites techniques présentes qui seront apprivoisées dans le futur par la somme des progrès.

L'application des technologies quantiques à l'informatique conduit au fait que les calculs puissent être développés de façon parallèle, aboutissant *de facto* à une augmentation exponentielle de la puissance dévolue [DAS 22].

En outre, le nombre de données toujours plus massif du *Big Data* requiert parallèlement une puissance de calcul en permanence grandissante et qui pourrait rapidement montrer les limites des plus sophistiqués supercalculateurs de la technologie informatique conventionnelle et d'une loi de Moore s'essoufflant. La puissance inouïe de l'informatique quantique constitue l'innovation qui prendra le relais pour juguler cette massification de calculs de données, et de plus permettra des progrès encore insoupçonnés dans de nombreux domaines d'applications informatiques et calculatoires [TEB 14].

Progrès de l'informatique, vers toujours plus de complexité et de sophistication sur des domaines d'application toujours plus larges

Il est en effet prévu que parallèlement aux progrès liés aux ordinateurs quantiques et aux calculs quantiques, les opérations dévolues possibles gagnent *crescendo* en complexité. D'abord opérations sur les stocks, flux, secteur de la finance, concernant le *Big Data* [BID 22], puis calculs ultra complexes liés aux comportements et à la prédition de mouvements des particules infinitésimales, à la chimie et bio-chimie dans une optique de sophistication encore jamais vue, et qui en particulier révolutionneront le domaine de la médecine [GOU 21], et de façon liée, la longévité de la vie humaine.

Informatique quantique, volets matériel et logiciel

Les technologies liées à l'informatique quantique comprennent les facettes matérielle (construction de machines par étapes de simulateurs et ordinateurs partiellement quantiques jusqu'au tant attendu ordinateur quantique universel) et logicielle (algorithmie et développement de futures applications dédiées) [INR 22].

Algorithmie quantique

Dans cette perspective, le développement de compétences et de formations sur l'algorithmie purement quantique constitue un domaine majeur de progrès : adapter la programmation basée sur des algorithmes quantiques aux futurs machines quantiques, et par étapes déjà partiellement quantiques.

Sur la voie du progrès quantique, l'enjeu de la création de standards pour faciliter les coopérations de recherche

Relativement à ce défrichage partant de la recherche fondamentale pour aboutir aux procédures opératives des technologies quantiques, il sera crucial d'établir des *designs* dominants et standards que compétiteurs, et de façon plus avantageuse pour le bien commun, coopétiteurs pourront emprunter. Ceci étant en mesure d'engendrer des synergies et ponts dans ce type de recherches pour contribuer à en faire diminuer le coût très onéreux. Parmi les éléments dont la standardisation pourrait accélérer les processus de recherche, les Qubits éléments clés précédemment explicités. En effet, aujourd'hui plusieurs modèles de structuration des Qubits sont considérés dans la recherche quantique. Ces modèles non standardisés ne sont ni interchangeables ni adaptables d'un dispositif quantique à l'autre. Dans la mesure du possible, des efforts de standardisation sur ces éléments

permettraient une meilleure transposition des expériences et du savoir acquis de différents laboratoires au travers le monde.

Technologies habilitantes comme intermédiaires nécessaires dans l'évolution quantique

La complexité immanente du domaine quantique nécessite le développement de vecteurs intermédiaires aussi appelés technologies habilitantes nécessaires à la production de matériaux d'ingénierie quantique [GAU 21]. Elles incluent lasers, techniques d'engendrement de photons, matériaux de stabilisation des isotopes et dispositifs de cryogénération. Ces derniers permettent un refroidissement extrême des particules de systèmes quantiques.

Cryogénie et refroidissement extrême permettant le fonctionnement de dispositifs quantiques

En effet, le refroidissement extrême nécessaire par la mise en œuvre de certaines technologies quantiques, dont les capteurs quantiques [NIC 21], peut exiger que les particules mises en jeu (atomes, photons...) des dispositifs impartis soient placées dans des conditions de température seulement quelques centièmes au-dessus de 0 degré Kelvin, le « zéro absolu » (correspondant à - 273,15 degrés Celsius) via des dispositifs d'ingénierie nommés cryostats où le mouvement des particules se rapproche de son palier de ralentissement ultime. Cette température extrême étant nécessaire à l'essentiel des techniques d'engendrement de Qubits suivant des particules infinitésimales quasi à l'arrêt. La technique majeure jusqu'à présent fait appel aux propriétés d'inertie thermique de liquide frigorifié. Celui-ci étant principalement obtenu par le mélange de deux isotopes, 3 et 4, de l'hélium.

Capteurs quantiques et liens à la physique quantique

Les capteurs quantiques permettent de déterminer des mesures physiques avec une précision non atteignable par des technologies tiers. Leur fonctionnement s'appuie sur les caractéristiques quantiques d'intrication et de superposition précédemment montrées.

Communication quantique

Parallèlement la communication quantique est aussi bâtie sur la caractéristique d'intrication quantique, de liaison parfaite de particules distantes aux mêmes états simultanés formant un même système quantique. La communication étant cryptée selon le processus de cryptographie quantique [DAS 22].

Technologies quantiques et cybersécurité

Dans ce champ, un secteur majeur des technologies quantiques concerne les enjeux de cybersécurité [GAU 21]. Et, de façon liée, la lutte contre la cybercriminalité par le développement des technologies quantiques. Agrémentée par le développement de parades visant à se prémunir de potentielles attaques cybercriminelles opérées, au moins partiellement, suivant des éléments de technologies quantiques recelant une puissance phénoménale, en particulier apte à casser les clés cryptographiques les plus sécurisées reposant sur l'informatique traditionnelle [BID 22].

France Digitale et le cabinet Wavestone avaient d'ailleurs récemment motivé leur appel au façonnement d'un solide développement quantique, possiblement promu et concerté à l'échelle européenne, pour se prémunir des dangers que faisaient peser les technologies quantiques si employées de façon hostile pour dégrader la cybersécurité, jusque dans le champ des indépendances politiques.

Différenciation entre cryptographie post-quantique et cryptographie quantique

La cryptographie post-quantique doit bien être distinguée de la cryptographie quantique. En effet, la cryptographie quantique met en œuvre les phénomènes quantiques proprement dits, en particulier l'intrication. Tandis que la cryptographie post-quantique entend trouver des parades pour tenter de résister à la future capacité de l'ordinateur quantique de décoder très aisément la cryptographie traditionnelle utilisée aujourd'hui.

Support d'investissements de la cybersécurité lié au développement quantique

Si l'avènement de la « suprématie quantique » portée par la conception de l'ordinateur quantique universel ne pourrait intervenir que suivant le laps de temps conforme aux progrès par étapes de ces technologies ultra-complexes, au moins d'ici dix à vingt ans selon de nombreux experts, la course se joue aussi entre « épée » (ces progrès des technologies quantiques impactant les enjeux de cybersécurité) et « bouclier » (les moyens de s'y prémunir en protégeant les cyber-installations, en particulier stratégiques, clés et algorithmes de chiffrement sécuritaire).

Par là, les financements singuliers de développement d'une cybersécurité (s'appuyant sur des technologies quantiques et non quantiques) apte à résister à la cybercriminalité pouvant s'appuyer sur l'informatique quantique en progrès constant gagneraient à prendre cette mesure et donc être massifs.

En plus du développement technologique de la cybersécurité, les politiques relatives devraient promouvoir la formation de profils experts, en particulier suivant des formations de haut niveau au sein de l'enseignement supérieur universitaire (masters spécialisés, doctorats, post-doctorats, filières de recherche) et des écoles d'ingénieurs. C'est à ce prix qu'une politique visant à la sécurisation face à une cybercriminalité s'appuyant sur les technologies quantiques pourra être déterminante.

Recherche quantique, de très haute complexité et aux voies de défrichage et progression multiples, d'où l'intérêt de financement à long terme

Différentes écoles, voies et méthodes de recherche en ingénierie quantique ultra complexe sont usitées ou serviront pour le développement de l'ordinateur quantique. La recherche dans ce domaine de très haute sophistication et non défriché étant forcément sinuuse et imprédictible. Avec des voies qui mèneront à des progrès notables quand d'autres buteront sur des limites dans l'avancée des travaux prospectifs. Chaque versant pouvant être singulièrement lié à des impératifs, spécifications, coûts, technologies imparies, dont habilitantes, difficultés et avantages. D'où le grand intérêt de financement de cette recherche au long cours que prend en compte le Plan Quantique français comme d'autres plans internationaux. Comme nous allons l'analyser dans la suite de ces travaux.

3. Étude des enjeux liés aux investissements quantiques

Après avoir analysé les éléments de physique quantique matriciels des technologies quantiques, ainsi que les agencements et mécanismes principaux des technologies quantiques, s'appuyant sur cette base d'analyses, nous allons suivant une étude de cas exploratoire comme détaillé en introduction montrer les enjeux des investissements étatiques sous-tendus par le Plan Quantique français. Nous allons de plus analyser comment ils s'articulent par rapport aux autres grands plans internationaux. Les principaux développements des géants du numérique, ainsi que les risques immanents à la puissance quantique seront également montrés.

Lancement du Plan Quantique français

Le 21 janvier 2021, le président Emmanuel Macron a divulgué le dénommé Plan Quantique, programme d'investissement doté d'une enveloppe de 1,8 milliard d'euros sur cinq ans et relatif au développement du secteur des technologies quantiques [ELY 21].

Objectif et pilotage

Le but annoncé du Plan Quantique est de faire de la France un des *leaders* mondiaux des technologies quantiques *via* les leviers publics de financement de projets et de coordination de la recherche et du développement. L'orchestration de la mise en œuvre du Plan Quantique est principalement liée à trois Ministères, ceux de la Recherche, des Armées et de l'Économie, ainsi qu'au Secrétariat d'État au Numérique, au Secrétariat Général pour l'Investissement et à la Banque Publique d'Investissement Bpifrance. Le projet portant officiellement le nom de « Plan Quantique » est aussi associé à la recherche publique *via* le CNRS, l'Inria et le CEA [CNR 21].

Détails de l'approvisionnement financier

En détaillant la dotation, le financement par l'État du Plan Quantique est de 1 milliard d'euros.

Les organismes publics de recherche comprenant donc CNRS, Inria et CEA seront parmi les contributeurs *via* des crédits notamment alloués à des programmes internes de recherche et développement quantique. Les laboratoires associés à ces organismes sont considérés comme un atout majeur du Plan Quantique par leur potentiel synergique quant au progrès quantique [LEV 21].

S'y ajoute une manne provenant du secteur privé (entreprises et fonds d'investissement réunis) de 550 millions. Parmi ces entreprises contributrices du Plan Quantique, les firmes françaises impliquées dans les technologies quantiques, en lien à leur cœur de métier, ou de façon périphérique, notamment relatives aux technologies habitantes : dispositifs non quantiques mais supports nécessaires à l'avancée du développement quantique. Parmi ces champions français liés au Plan Quantique, Air Liquide, Airbus, Atos, STMicroelectronics, Total et Thalès.

Enfin, l'Union européenne approvisionnera la dote à hauteur de 200 millions d'euros.

Capteurs quantiques, Thalès comme spécialiste français

250 millions d'euros du Plan Quantique sont dévolus au développement de capteurs quantiques, objets technologiques décrits en première partie de l'article. Thalès est une des firmes mondiales hautement spécialistes du secteur. L'intégration de la firme au Plan Quantique est par là un grand atout.

Plan Quantique et participation des firmes privées : le cas d'Atos

Illustration de ces participations du secteur privé au Plan Quantique français, le cas d'Atos [MAN 21]. Le géant français et mondial de services numériques Atos, disposant de plus de 110 000 employés à travers le monde et dont le chiffre d'affaires annuel dépasse les 10 milliards d'euros est l'acteur privé français majeur concernant la R&D quantique. Parmi ces développements, Atos a mis au point des simulateurs quantiques réputés mondialement pour leurs qualités et dont firmes numériques internationales, dont à la Silicon Valley, louent les services de ses simulateurs quantiques pour intégrer les résultats à leurs propres développements.

Accueil enthousiaste de l'écosystème lié au quantique

Le plan a été reçu de façon très positive [CEA 21] par l'écosystème français imparti comprenant organismes et laboratoires de recherche, industriels, firmes et entreprises innovantes en lien au secteur quantique, des *start-ups*, parfois directement issues des laboratoires de recherche, aux

champions numériques, en particulier Atos, dont le directeur général assistait à l'annonce présidentielle.

Association à la politique de relance économique

Le Plan Quantique est aussi associé aux processus de relance économique d'inspiration keynésianiste, rendus encore plus pertinents en temps de crise. Le plan est ainsi lié au projet France Relance 2030 annoncé en septembre 2020 et à l'enveloppe prévisionnelle record de 100 milliards d'euros. Ainsi qu'au 4eme Programme d'Investissements d'Avenir (PIA 4) présenté le même mois et doté d'un budget de 20 milliards d'euros consacré à l'innovation et dont plus de la moitié est directement lié à la relance économique. Ainsi, dans le détail le milliard d'euros du financement par l'État du Plan Quantique se décompose comme suit : 600 millions proviennent du quatrième Programme d'Investissement d'Avenir et 400 millions sont issus du budget de la Loi de Programmation Pour la Recherche (LPPR) votée à la fin de l'année 2020.

Nouvelles applications basées sur les technologies quantiques avant même l'avènement de l'ère quantique

Ainsi, si les technologies quantiques constituent assurément un domaine qui façonnera le monde de demain, l'incorporation sociale de nouvelles applications augurées par le Plan Quantique devrait advenir pendant sa mise en place. Naturellement, la stratégie française se poursuivra dans la voie du premier Plan Quantique après sa période dévolue de cinq années.

Plan Quantique et parallélisme avec le Plan Intelligence Artificielle

Le Plan Quantique peut être mis en parallèle avec le projet gouvernemental analogue relatif à la haute technologie numérique datant de 2018, le Plan Intelligence Artificielle. Celui-ci avait été doté d'une enveloppe de 1,5 milliard, mettant aussi en jeu financement public et participations privées. En 2021, ce plan a reçu une rallonge budgétaire, amenant à un total de 2,2 milliards d'euros.

Recherche fondamentale au cœur des coopérations

Les technologies quantiques sont très liées à la matrice de la recherche fondamentale. Ainsi la coopération entre laboratoires, centres de recherche et *start-ups*, de la recherche théorique aux développements applicatifs, prend tout son sens. Dans cette perspective, le Plan Quantique prend nettement en considération la valorisation industrielle de la recherche fondamentale et a pour objet de constituer des ponts et favoriser la mise sur le marché des dispositifs innovants issus, dont innovations de rupture [BER 22].

Plan Quantique et interfaçage avec les secteurs industriels connexes

En outre, le Plan Quantique prend en compte l'interfaçage nécessaire des technologies quantiques avec les industries et secteurs connexes dans la recherche de synergies.

Enjeux de la protection des brevets financés par le Plan Quantique

Lié au Plan Quantique, a été apposé un suivi relatif aux dépôts de brevets émanant des acteurs français du secteur. La crainte est que des brevets portant sur le quantique puissent être rachetés par des entreprises étrangères, notamment celles investissant dans les entreprises françaises impliquées dans le Plan Quantique. Marque de l'extrême sensibilité sur ces enjeux façonnant l'avenir, le décret IEF (Investissements Étrangers en France) qui permet d'examiner nature et contre-partie de ces investissements sera opérant sur le secteur des technologies quantiques.

Répartition des sommes allouées par spécialités liées aux technologies quantiques

La dotation allouée au Plan Quantique se repartit comme suit.

Le développement des calculateurs quantiques sera accrédité de la somme de 430 millions.

Les simulateurs quantiques, qui permettent de mettre en œuvre des programmes quantiques sur des machines ne pouvant à cette étape du progrès encore l'être, recevront 350 millions.

La communication quantique qui nécessite des réseaux et câblages spécifiques sera dotée d'une enveloppe de 320 millions.

Les technologies habilitantes seront financées à hauteur de 290 millions.

La cryptographie post-quantique, prévue pour être capable de résister au déchiffrement par la puissance de calcul quantique, recevra 150 millions d'euros.

L'acquisition publique de matériels technologiques quantiques permettant d'équiper les laboratoires sera accréditée de 70 millions d'euros.

Enfin, une somme ajustable est liée au financement de l'enseignement quantique de haut niveau, classes de masters et d'écoles d'ingénieurs, financement de thèses (au-delà de la centaine déjà prévues), auxquels s'ajouteront des contrats de recherche et post-doc (50 prévus pour l'instant).

Clusters et écosystèmes quantiques français

Dans cette perspective, l'enseignement supérieur en connexion avec les pôles de recherche dont le CNRS est intégré au Plan Quantique. Notamment dans le potentiel de développement de *clusters* et écosystèmes mêlant recherche, enseignement supérieur, laboratoires universitaires, écoles d'ingénieurs, interdisciplinarité et liens avec les entreprises, notamment *start-ups*. Dans ce domaine, le Quantum Engineering Grenoble (QuEnG) constitue un des maillages pionniers de *cluster* quantique français basé sur ces éléments. Le centre de nanosciences du campus de Saclay dispose déjà également d'un haut niveau d'expertise concernant les technologies quantiques.

Firmes françaises au cœur de l'interdisciplinarité des technologies quantiques

Des entreprises françaises dont le domaine principal n'est pas lié au quantique ou à l'ingénierie informatique opèrent cependant, et à haut niveau, dans les technologies quantiques. Parmi elles, Total et EDF. Illustration de l'interdisciplinarité que les technologies quantiques mettent en jeu.

Bouillon de culture des start-ups françaises dans le domaine des technologies quantiques

La France compte déjà plus d'une vingtaine de *start-ups* reconnues dans le domaine des technologies quantiques. Parmi elles, plusieurs ont déjà mis au point des applications pleinement opératives, voire disponibles sur le marché.

Synergies, interdisciplinarité et implication du CNRS

La fédération de recherche CNRS Paris Centre for Quantum Computing (PCQC) apparue en 2014 associe CNRS, Université de Paris et Sorbonne, et bientôt de nouveaux acteurs dont l'Inria dans un objectif de recherche de symbiose et d'interdisciplinarité notamment entre experts des sciences physiques et de l'informatique. De telles synergies à l'intersection des domaines porteurs des technologies quantiques sont hautement vecteurs d'accélération de progrès dans le domaine.

Secteurs technologiques impliqués et intérêt stratégique de financement

Les secteurs industriels et de haute technologie dévolus au Plan Quantique sont éminemment stratégiques. Et, de part les liens qu'ils entretiennent entre eux et à la matrice de recherche fondamentale de la physique quantique et des mathématiques associées, les plus pertinents à fédérer des investissements gouvernementaux de recherche dans une perspective de retombées de très

grande envergure à moyen et long termes. En effet, ces investissements portent en eux l'engendrement d'un essaim de nouvelles applications innovantes et d'avancées technologiques révolutionnaires qui pourraient se réaliser concrètement d'ici peu pour les premières et à une approximation de deux décennies pour celles liées à une accumulation de progrès, dont l'ordinateur quantique universel pleinement opérationnel.

Communication quantique

Comme mis en exergue, 320 millions du Plan Quantique sont dédiés à la communication quantique. La communication quantique est basée sur la caractéristique d'intrication des particules infinitésimales de la physique quantique [DAS 22]. Or, pour être mise en œuvre, la communication quantique nécessite un réseau de câbles spécifique. De tels réseaux sont en projet de développement, en Île-de-France et dans la région de Nice, en lien au Plan Quantique.

Cryptographie post-quantique

La cryptographie post-quantique, qui a reçu une enveloppe de 150 millions liée au Plan Quantique, part, comme indiqué précédemment, du postulat certain que la puissance de calcul de l'ordinateur quantique, quand il sera opérationnel, aura la capacité de venir à bout quasi instantanément des clés de chiffrement cryptographiques traditionnels.

Un leader français dans les technologies habilitantes de cryogénie

La nécessité de maîtriser les techniques de cryogénie a été mise en évidence en première partie de cet article. En France, Air Liquide est l'acteur de pointe du secteur de la cryogénie. La firme industrielle a notamment augmenté son expertise dans le domaine en faisant l'acquisition en septembre 2020 de l'entreprise française ultra spécialisée dans le développement des cryostats, Cryoconcept.

Simulateurs quantiques, outils de transition vers les ordinateurs quantiques

Comme indiqué, une partie des financements du Plan Quantique est liée aux simulateurs quantiques. Ces dispositifs constituent des vecteurs de transition dans le progrès quantique. En effet, les simulateurs quantiques sont basés sur des ordinateurs non quantiques (*de facto*, les ordinateurs complets purement quantiques n'existant pas encore) mais constitués d'une architecture singulière leur permettant de simuler, pour l'instant partiellement, le processus opératif des futurs ordinateurs quantiques. L'architecture de ces ordinateurs de transition ne leur permet bien sûr pas d'engendrer la puissance phénoménale que les ordinateurs entièrement quantiques augureront quand ils seront opérationnels, mais ils constituent une étape de progrès primordiale.

Prométhée et l'ordinateur quantique universel

En effet, un *challenge* énoncé est lié à la course à la fabrication de l'ordinateur quantique universel, pièce maîtresse la plus attendue des technologies quantiques car insufflant le passage vers la « suprématie quantique », locution utilisée par les experts du secteur, dénotant moins une emphase de forme que l'attente du dispositif prométhéen des technologies quantiques. En effet, il ouvrirait la voie à la pleine puissance de calcul où, comme on l'a décrit en première partie de cet article, les processus binaires de l'informatique traditionnelle seraient remplacés par des processus où les particules infinitésimales, atomes ou photons, pourraient revêtir plusieurs états simultanés, comme montré apanage de la physique quantique concernant l'infiniment petit, et permettre des calculs parallèles avec une progression exponentielle pour chaque particule supplémentaire. Il en résultera un différentiel de puissance inouï entre les précédents ordinateurs et les nouveaux ordinateurs quantiques universels.

Prospectives concernant un secteur scientifique de très haut niveau

Les ordinateurs quantiques partiels, dont la puissance de calcul dépassera déjà sans commune mesure celle des supercalculateurs non quantiques, devraient se développer après 2030. Dates et prospectives étant toujours liés à des aléas imprédictibles de la recherche concernant un secteur scientifique de très haut niveau et exploratoire.

Calculateurs quantiques bruités comme illustration d'une technologie intermédiaire dans le progrès quantique

Dans cette perspective et dans un temps proche, une gamme de calculateurs intermédiaires devrait se développer sous le nom de calculateurs quantiques bruités [ECH 22] (ou « Noisy Intermediate Scale Quantum », NISQ). Ces calculateurs intermédiaires devraient être capables de gérer jusqu'à 100 Qubits selon une technologie transitoire et constituerait le support du développement de la programmation quantique et de la mise en œuvre d'algorithmes quantiques. La puissance de calcul attendue serait supérieure à celle des ordinateurs actuels les plus haut de gamme et constituerait un des marches-pieds préalables à l'élaboration des calculateurs intégralement quantiques quand le progrès le permettra.

CEA, un atout français dans la course à la réalisation de l'ordinateur quantique

Le CEA est aussi parmi les rares acteurs mondiaux à développé un projet propre d'ordinateur quantique. Dans cette perspective le Plan Quantique français appuie ce développement de très haute ambition.

Plan Quantique et ambition envers le logiciel métier

En outre concernant l'informatique, par l'entremise du Plan Quantique, la France entend se placer à l'avant-garde du développement de logiciel métier intégrant les technologies quantiques.

Géants du numérique et très haute implication dans le développement des technologies quantiques

Des géants du numérique sont très activement impliqués dans le développement des technologies quantiques. IBM et Google [EPA 21] en particulier y consacrent des sommes pharaoniques et font fonctionner à plein régime leurs très hautes capacités de R&D et puissance financière. Ces géants du numérique sont pour l'instant en avance dans la course au développement de l'ordinateur quantique, et sur certains domaines, en considérant même des plans étatiques.

Expérience quantique de Google témoin des moyens mis en œuvre par les firmes du numérique dans la course à la suprématie quantique

Dans cette perspective, Google a annoncé dès 2019 s'être approché du seuil augurant de la suprématie quantique suivant l'implémentation d'un algorithme sur son prototype d'ordinateur exploitant la technologie quantique et nommé Sycamore. Néanmoins de nombreux scientifiques remettent en cause une partie de l'exploit. Ainsi, si un pas important a été produit *via* l'expérience de Google, l'algorithme mis en œuvre est un algorithme classique implantable sur une machine non quantique. Ce qui n'est pas réfuté par les promoteurs de l'expérience puisque eux-mêmes indiquent que l'implémentation de l'algorithme a pu être réalisée dans le temps record de 3 minutes et 20 secondes là où le plus puissant supercalculateur de la NASA aurait mis 10.000 ans pour la même opération. Implicitement cela signifiant que l'algorithme n'est pas lui-même quantique. Or pour la majorité du monde scientifique spécialisé, la suprématie quantique à proprement dites ne sera atteinte que quand un ordinateur quantique universel implémentera un algorithme purement quantique non traitable par une machine classique. Comme indiqué selon ces experts cette suprématie pourrait être à portée dans un laps de temps d'environ deux décennies. Néanmoins

l'expérience d'avant-garde de Google, ainsi que les grandes avancées d'IBM, talonnant Google, et les initiatives d'autres firmes informatiques témoignent des très importants efforts de R&D des géants du numérique dans la course à la suprématie quantique.

Puissance de calcul informatique gigantesque, risques encourus et nécessité de garde-fou et régulation

A ce niveau, il apparaît fortement souhaitable que cette source de puissance en voie d'apparition à moyen terme soit modérée et régulée. Et notamment ne soit pas détenue par des intérêts privatifs au service d'une firme ou d'un état sans contre-feu, tant la puissance de calcul conférée amènerait à un pouvoir numérique opérationnel sans commune mesure. Ainsi, comme analysé, les clés de chiffrements de sécurité les plus puissantes de l'informatique traditionnelle seraient percées en quelques instants par l'ordinateur quantique universel. Pareillement, le possesseur de l'ordinateur quantique universel pourrait créer une cryptomonnaie dont la sécurisation, dépassant toutes les technologies de *blockchains*, serait absolue. Et qui ainsi comparativement aux autres monnaies et cryptomonnaies bénéficierait d'un avantage concurrentiel irrattrapable. Afin de tenter de se prémunir de ces risques, le développement d'une science de la cryptographie post-quantique en train d'apparaître consistant en la recherche de garde-fou moins susceptible d'être quasi instantanément « hacké » par l'ordinateur quantique universel.

Investissements internationaux liés aux technologies quantiques

Même si l'essentiel des investissements internationaux n'a pas bénéficié d'une présentation aussi encadrée que le Plan Quantique français, par recouplements des sommes attribuées une approximation des investissements peut être dressée comme suit. Les acteurs internationaux exposés sont ceux qui ont une politique proactive d'investissements liés aux technologiques quantiques à leur échelle.

Chronologiquement, la Chine a ainsi annoncé dès 2015 le lancement d'un premier plan quantique de très large envergure selon l'enveloppe record stipulée de 10 milliards d'euros. Même si selon de nombreux experts pour l'instant seulement une partie de la somme aurait été investie. Par ailleurs, des infrastructures de haute qualité et dotées de matériels de pointe ont été construites et abritent de nombreux chercheurs du domaine au sein du laboratoire de recherche de Jian Wei-Pan de Hefei.

En septembre 2018, l'Allemagne a lancé son premier plan quantique doté d'un montant de 650 millions d'euros sur cinq ans. En juin 2020, ce plan a été étendu de façon drastique puisque 2 milliards d'euros lui ont été adjoints.

Stratégie de l'Union européenne où Flagship Quantique

L'Union européenne a introduit son Quantum European Flagship en octobre 2018 doté d'un milliard d'euros sur cinq ans. Le plan européen subventionne déjà une vingtaine de projets. D'un point de vue français, il est à noter que le CNRS est impliqué dans la moitié de ces projets sous financement européen. En outre, la filiale du CNRS, CNRS Innovation, est déjà présente au capital de *start-ups* innovantes du secteur quantique. Les avancements et succès du Quantum European Flagship pourraient établir une illustration exemplaire de plan d'investissement de recherche stratégique européen. Les technologies quantiques et les perspectives de progrès immenses qu'elles recèlent constituent en effet un pôle modèle de progrès économique apte à renforcer la construction européenne.

Les États-Unis ont lancé un plan intitulé National Quantum Initiative Act en décembre 2018, toujours sur une période de 5 années, et suivant l'enveloppe de 1,25 milliard de dollars. 800 millions de dollars ont été ajoutés à cette somme initiale en mars 2020 pour une période de deux ans. Les

États-Unis ont aussi procédé à l'ouverture de trois centres ultra-modernes spécifiquement dédiés aux technologies quantiques.

Le Royaume-Uni, dont l'intérêt d'État pour les technologies quantiques s'était manifesté dès 2013, a en 2019 apporté un milliard de livres sterling pour le développement de ces dispositifs.

La Russie a en décembre 2019 lancé son plan quantique suivant une enveloppe de 750 millions d'euros.

A la fin de l'année 2019, Israël et le Japon ont fait de même suivant des montants respectifs annoncés de 350 et 200 millions de dollars. Témoin de nouvelles coopérations entre états et grandes entreprises, le Japon a passé un accord avec IBM concernant les technologies quantiques, l'une des deux firmes les plus en avance dans le domaine en compagnie de Google comme indiqué précédemment.

L'Inde a emboîté le pas en février 2020 en consacrant 1,12 milliard de dollars à son plan quantique.

Finalité du plan : la France devient le troisième investisseur mondial dans les technologies quantiques, après les États-Unis et la Chine

Avec la formalisation du Plan Quantique de 1,8 milliard d'euros, la France devient le troisième investisseur étatique du secteur. Ramené à une fréquence annuelle d'investissement public consacré aux technologies quantiques, le plan fera passer la France du chiffre de 60 millions d'euros précédemment consacrés à 200 millions d'euros. Seuls États-Unis et Chine sont au-dessus du chiffre français en y investissant près du double.

Suivant cette comparaison internationale, les divisions sectorielles prises en compte dans le Plan Quantique français présentent une analogie avec les plans ou financements étrangers concernant les technologies quantiques. A ceci près que la France prend davantage en considération et alloue relativement plus de fonds aux technologies habilitantes. Pour le reste, le secteur quantique impose à la France comme aux autres pays impliqués, ses propres déterminismes et prismes de recherche à l'aube d'une révolution quantique ayant le potentiel de changer l'avenir du monde.

Bilan : technologies quantiques et intérêt de l'investissement public pour une recherche de long terme

Comme analysé, les technologies quantiques s'appuient fortement sur la recherche fondamentale à partir de la physique quantique. En outre, et renforçant un support de R&D de longue haleine, la chronologie d'essor et de maturité de différentes technologies quantiques, et de dispositifs associés, s'appuie sur des séries de découvertes en gestation et futures. En conséquence, il s'agit d'un secteur où l'investissement public de recherche à long terme est déterminant, ainsi que les partenariats et synergies public privé. D'autant plus que les enjeux et répercussions industrielles multi-sectoriels et économiques sont des plus conséquents et sont amenés à façonner l'avenir comme aucun autre secteur *high tech*.

Les autres puissances mondiales de premier plan, en particulier États-Unis et Chine, les deux *leaders* en terme d'investissements étatiques, ont bien pris la mesure du potentiel quantique. Suivant le Plan Quantique analysé de façon détaillée dans le cadre de l'étude de cas présente, la France souhaite se placer à la troisième place derrière les deux premières puissances mondiales.

Il a en outre été analysé que certaines firmes « géants du numérique » disposent de compétences en ressources humaines, de finance mobilisable, et de R&D interne qui rivalisent dans les faits avec ceux des états. Parmi elles, le *leader* des GAFAM en la matière Google, est très avancé dans le développement des technologies quantiques et IBM non loin.

4. Conclusion

Telles qu'analysées dans cet article, les technologies quantiques, qui comme on l'a détaillé dans une première partie, s'appuient sur la matrice fondamentale des sciences et de la physique quantique vont, en accord avec les centres de la recherche scientifique et prospectiviste impartie, s'imposer comme le plus grand facteur de progrès technologique du XXI^e siècle. En effet même si d'autres technologies novatrices vont avoir un impact majeur, notamment celles communément incluses dans la quatrième révolution industrielle (dont l'avènement des imprimantes 3D, y compris celles de très haut niveau de la médecine *high tech* et de l'aérospatiale, et l'usine 2.0 innovante qu'elles constituent qui seront un vecteur opératif du progrès des secteurs de pointe, de la création de prothèses bioniques à la réalisation de fuselages de très haute précision d'engins spatiaux), les bonds technologiques du secteur quantique permettront d'atteindre une puissance de calcul phénoménal et sans commune mesure avec les supercalculateurs les plus haut de gamme de l'informatique traditionnelle, engendrant communications et cryptographies quantiques au caractère parfait suivant les caractéristiques très singulières de la physique quantique des éléments à l'échelle infinitésimale, particules atomiques, subatomiques, photons, notamment en lien à la caractéristique d'intrication quantique et aux autres propriétés explicitées dans cet article. La puissance de calcul quantique accélérera aussi de façon drastique le progrès médical, de la détection d'anomalies biologiques à l'échelle moléculaire jusqu'à la fabrication de nouveaux médicaments révolutionnaires.

Suivant ces éléments analysés permettant d'expliciter le passage de la physique quantique aux technologies quantiques de la première partie de cet article, la seconde partie a développé une étude de cas sur les investissements quantiques liant agences gouvernementales et acteurs privés dans le cadre du Plan Quantique français, et également en fournissant des points de comparaison avec les grands plans analogues internationaux. Comme il a été montré, élément constituant de cyberpuissance étatique et dernier né des projets nationaux d'envergure, le Plan Quantique français, lancé au début de l'année 2021, et doté d'une enveloppe de 1,8 milliard d'euros sur cinq ans, a suivant cette étude notamment permis d'exposer les enjeux drastiques entourant les politiques de support et R&D des technologies quantiques. Donc d'autant plus primordiaux que, comme analysé, liés à une course entre grandes puissances étatiques, et firmes majeures des TIC, dont Google et IBM. En effet, comme analysé, les géants industriels du numérique, secteur le plus lié aux retombées du développement quantique, de part leurs puissances financières et leurs capacités de R&D, peuvent consacrer des sommes colossales aux projets relatifs aux technologies quantiques. IBM et Google sont les firmes les plus en pointes dans la recherche et le développement quantique, jusqu'à une aptitude à pouvoir rivaliser et même dépasser dans des domaines les plans d'état dans la course à la suprématie quantique. En lien à ces enjeux, a été montré qu'une telle puissance prométhéenne, notamment liée à la course à la « suprématie quantique », à la fabrication d'ordinateurs entièrement quantiques, conférera à ses détenteurs une puissance phénoménale, capable d'influer sur la destinée du monde de demain.

Bibliographie

- [ANR 22] ANR, *PEPR Quantique - Appel à projets Calcul Quantique au Vol*, ANR - Agence Nationale de la Recherche, 2022.
- [BER 22] BERGOUNHOUX J., « Bilan : Un an après son lancement, où en est le plan quantique national ? », *L'Usine Digitale*, 21/01, 2022.
- [BID 22] BIDAN M., FEVRIER R., « Informatique quantique : vers un “quantum management” ? », *Management & Datascience*, Vol.6 N°3 - Juillet, 2022.
- [CEA 21] CEA, *La recherche au cœur du plan quantique*, Site officiel du CEA, Commissariat à l'énergie atomique, 2021.

- [CNR 21] CNRS, *La recherche française au cœur du Plan Quantique*, Publication officielle du CNRS - Centre national de la recherche scientifique, 2021.
- [DAS 22] D'ASCOLI S., BOUSCAL A., *Voyage au cœur de l'atome - La physique quantique en dix innovations spectaculaires*, Éditions First, 213 pages, 28/04, 2022.
- [ECH 22] ECHOSCIENCES, *Chercheurs engagés dans le Plan quantique français*, EchoSciences Bourgogne Franche Comté, Institut UTINAM, Université de Franche-Comté / CNRS, 07/07, 2022.
- [ELY 21] ÉLYSEE, *Présentation de la stratégie nationale sur les technologies quantiques*, Site Officiel de l'Élysée Présidence de la République, 2021.
- [EPA 21] EPA PARIS SACLAY, *Paris-Saclay, épicentre du Plan Quantique*, EPA Établissement public d'aménagement, 05/02, 2021.
- [GAU 21] GAUDEMEN N. (ED), *L'informatique quantique, une révolution*, Livre Blanc sous la direction de Nicolas Gaudemet, Editeur Groupe OnePoint, Juillet, 2021.
- [GOU 21] GOUVERNEMENT FRANÇAIS, « 1,8 M € en faveur des technologies quantiques », *Article gouvernemental officiel catégorie Défense Innovation*, 2021.
- [INR 22] INRIA, *Quantique : anticiper les évolutions de l'informatique de demain*, Inria - Institut national de recherche en informatique et en automatique, 23/02, 2022.
- [LEB 13] LE BELLAC M., *Physique quantique - Fondements* (Tome 1), 3eme édition, Préfaces de Claude Cohen-Tannoudji et Franck Laloë, Savoirs actuels Physique, CNRS Éditions, 534 pages, 2013.
- [LEV 21] LEVY G., « Plan quantique français : première étape à 150 millions d'euros », *Siècle Digital*, 01/10, 2021.
- [LOR 19] LORENZI J.H., GAINNIER B., DURIEUX J., PETIT A. (EDS), *Intelligence artificielle, blockchain et technologies quantiques au service de la finance de demain*, sous la direction de Jean-Hervé Lorenzi, Bernard Gainnier et Joëlle Durieux et le parrainage de Antoine Petit, PDG, CNRS, Finance Innovation Pôle de compétitivité mondial, RB Edition, 296 pages, 2019.
- [MAN 21] MANENS F., « 3 questions sur le Plan quantique, l'investissement de la France dans l'informatique de demain », *Numerama*, 22/01, 2022.
- [NIC 21] NICOT F., « 4 piliers pour une révolution quantique », *Sciences et avenir*, 2021.
- [ROL 21] ROLLIN M., *Informatique Quantique - Qubit*, Altran, part of Capgemini, hal, 2021.
- [TEB 14] TEBOUL B., AMRI T., *Les Machines pour le Big Data : Vers une informatique quantique et cognitive*, fffhal-01096689v2f, 2014.