Informatique quantique : menaces et opportunités

Quelles stratégies pour la France ?

Sophie Lambert, Stephan Agnimel, Bertrand Hassani,
Anthony Rousseau, Stéphane Szymanski

ECOLE DE GUERRE ECONOMIQUE MaCYB 01

2022

"**L’habituel défaut de l’homme est de ne pas prévoir l’orage par beau temps**."
Nicolas Machiavel

INTRODUCTION ET PROBLÉMATIQUE

Aujourd'hui, lorsqu'il s'agit d'aborder les sujets quantiques et cryptographiques, les mythes se confondent souvent avec la réalité. Force est de constater que même avec des technologies classiques, et bien avant l'avènement (futur) des technologies quantiques, les clés de chiffrement, telles que les clés RSA [1] utilisées à grande échelle, sont déjà déchiffrables. La faiblesse déjà établie de ses clés ne fera que s'amplifier avec la technologie quantique, rendant les approches actuelles inutilisables. En effet, aujourd'hui, une clé de 256 bits peut être déchiffrée en cinquante secondes sur des technologies classiques [2] [1]... Pour référence, il est important de noter que depuis le 31 janvier 2021 la taille minimale de la clé RSA émise par SSL.com passera de 2048 à 3072 bits [2], et que l'utilisation à grande échelle de clé de 4096 bits est discuté par les spécialistes. Cependant, l'utilisation d'ordinateurs quantiques viendrait en réalité définitivement mettre en défaut la cryptographie dite traditionnelle.

De manière factuelle, le 21 mai 2019, la Direction Générale des Services Extérieurs (DGSE) lançait un défi d'hacking, le "challenge Richelieu" (Figure 1), qui lui servi- rait vraisemblablement à trouver des recrues pour le domaine encore balbutiant de la cyberdéfense [3]. Parmi les nombreuses épreuves qui s'apparentaient à un panorama complet de la discipline, figurait le déchiffrage d'un message, qui nécessitait de casser une clé RSA. La clé publique et une partie de la clé privée étaient fournies, ce qui rendait la tâche réalisable. C'était sans doute l'épreuve la plus intéressante, car elle envoyait un double message à la communauté : d'une part les clés RSA étaient cassables, ce que chacun savait théoriquement possible, mais un second message était peut-être encore plus intéressant : le temps était venu de pouvoir casser les fameuses clés de sécurité RSA, piliers fondateurs de la sécurité d'Internet réputés à toute épreuve.

Avant l'avènement du Cloud, nombre de figures renommées de la communauté affirmaient qu'il n'y avait pas de puissance de calcul suffisante pour casser les clés RSA. Si les capacités de calculs réelles des datacenters du Pentagone, de la National Security Agency (NSA) ou de la Central Intelligence Agency (CIA), pour ne citer qu'eux, ne sont pas réellement connus, en revanche la puissance des centrales électriques qui sont disponibles à proximité de ces centres de calculs est quant à elle bien connue. Comme nous connaissons la puissance électrique dont a besoin les ordinateurs pour faire les calculs nécessaires, nous pouvons connaître la puissance maximale de calcul de ces datacenters en agrégeant ce qui est fourni par les centrales de la région, et le résultat semble en effet très insuffisant. Cependant, le fait qu'on ne parle plus, de- puis des années, de l'interdiction d'utilisation des clés RSA très large, alors qu'elles étaient encore interdites il y a une dizaine d'année, semblait indiquer que, soit les services de renseignement avaient renoncé à la possibilité de lire certaines communications chiffrées, soit ils avaient trouvé un moyen de les lire, ce qui donnerait au contraire un faux sentiment de sécurité propice à tous les débordements.

1. Rivest, Shamir, and Adleman
2. Un code pour casser des clés RSA peut être trouvé sur https://github.com/fengtan/rsa- breaker, cf annexe A

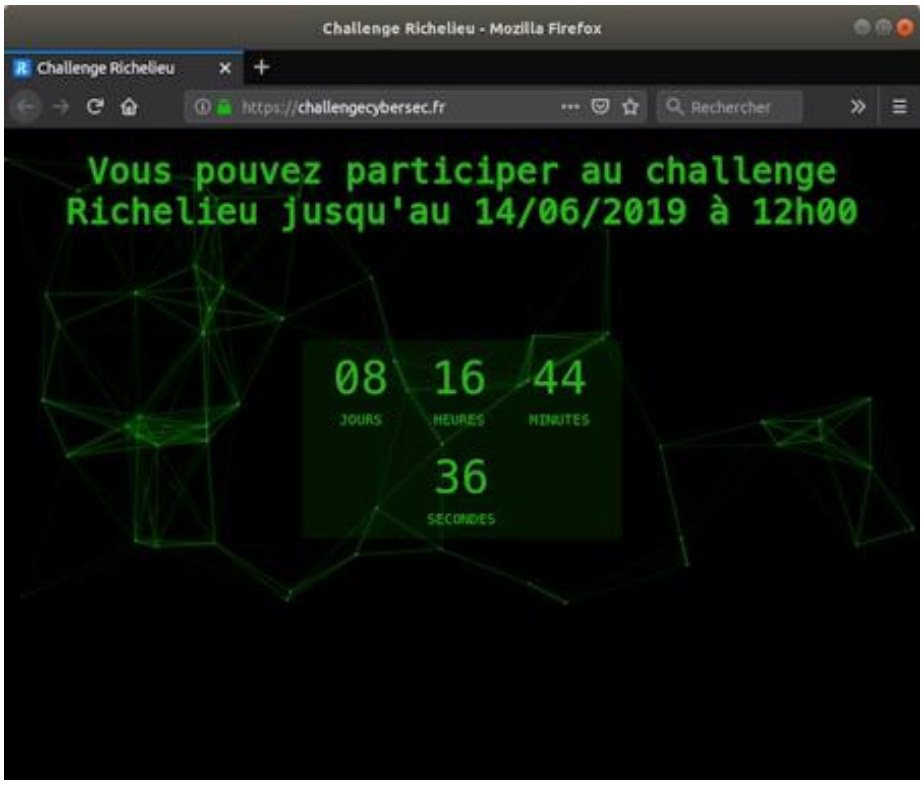

Figure 1 – Solution du Challenge Richelieu proposée sur le git à l'adresse https ://github.com/gw3l/richelieu

Depuis le début des années 2010, il est théoriquement possible de louer des ordina- teurs quantiques mais les premiers ne semblaient limités qu'à des tâches d'optimisa- tion (D-Wave One [4]). Ces dernières années (entre 2018 et 2022), d'autres sociétés ont mis à disposition des entreprises des ordinateurs ou des simulateurs quantiques "programmables". Nous avons donc franchi un palier en termes de cybermenaces. Si la puissance de calcul ne semble pas encore suffisante pour poser une réelle menace à la sécurité informatique, ce n'est sans doute plus qu'une question d'années ([5], [6]), voire de mois avant que ce ne soit le cas. Dès lors, les annonces tonitruantes des constructeurs défrayent régulièrement la chronique, les capacités de calcul semblant s'élever de façon exponentielle, parallèlement à l'avènement d'une nouvelle forme de la loi de Moore (Figure 2).

Il est fort probable que dans un avenir proche, les ordinateurs quantiques seront si avancés qu'ils auront la capacité de simuler des systèmes très compliqués. Ils pour- raient être utilisés pour des simulations en physique, en ingénierie aérospatiale, en cybersécurité et bien plus encore. En effet, les ordinateurs quantiques (Figure 3) laissent entrevoir une compréhension radicalement nouvelle de l'informatique. Une compréhension qui pourrait éventuellement être utilisée pour résoudre des problèmes aujourd'hui considérés comme totalement insolvables. Le domaine semble en effet très riche en potentiel. Les scientifiques qui travaillent sur l'informatique quantique la considèrent comme l'un des outils théoriques les plus intéressants en matière d'évolution de l'intelligence artificielle car elle s'appuie sur philosophies algorithmiques alternatives. Il s'agit d'une calculatrice incroyablement puissante programmée avec une expertise approfondie du domaine. Les ordinateurs quantiques promettent des réponses à toutes sortes de questions scientifiques qui

n’auraient pu être abordée autrement. Ils promettent de profondes percées dans le domaine de l’imagerie, qui rivaliseront même avec les scanners IRM intracellulaires expérimentaux ; ils pour- raient aider à déchiffrer de vastes bases de données actuellement inviolables ou relever des détails insignifiants tels que des signatures géologiques nous avertissant des tsunamis bien avant qu’ils ne se produisent.-

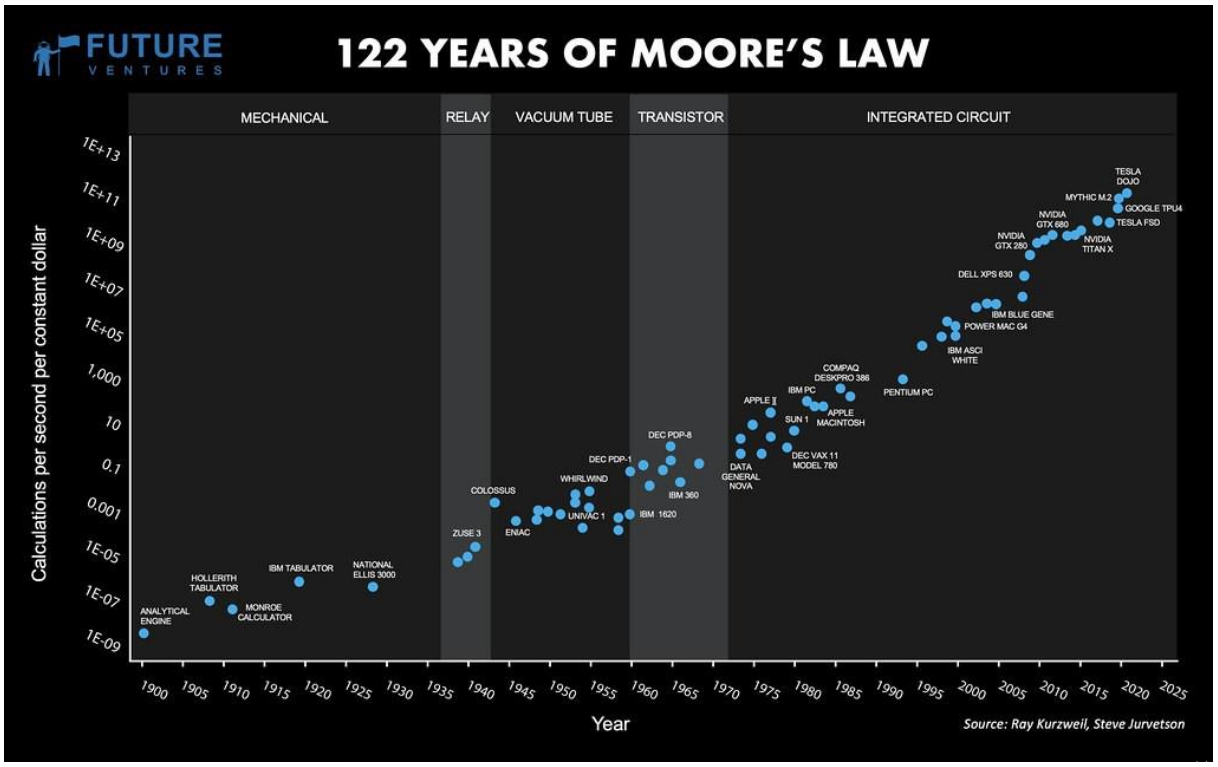

Figure 2 – Illustration de l’évolution de la loi de Moore qui postule un doublement d’une capacité technologique quelconque en un temps donné.

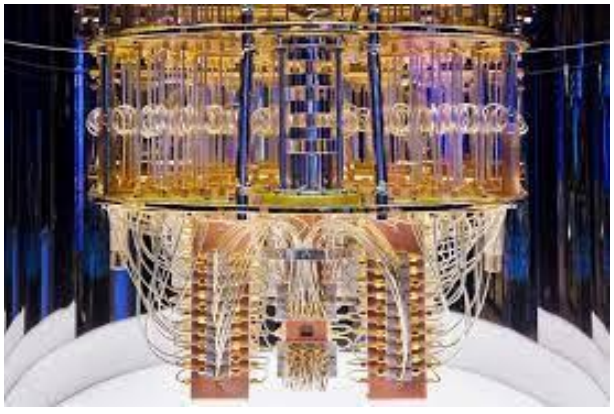

Figure 3 – Ordinateur Quantique d’IBM (Photo : IBM Research)

Cependant, une fois que ces ordinateurs seront construits, il sera potentiellement possible de démêler instantanément les protocoles de chiffrement des données, et compromettre ainsi tous les systèmes dépendants. En d’autres termes, les possibilités dévastatrices semblent infinies... Alors que les ordinateurs quantiques permettent ce

traitement alternatif de l'information, les dangers de piratage augmentent en parallèle. Ces risques de sécurité sont une priorité absolue pour nombre d'acteurs majeurs. La Defense Advanced Research Projects Agency (DARPA) [3] a d'ailleurs lancé de grands défis à l'informatique en offrant un prix de 2 millions de dollars aux pro- positions les plus pertinentes afin de maintenir la pertinence de la cyber puissance américaine et d'éviter une perte potentielle du leadership technologique mondial. Si les ordinateurs quantiques prolifèrent, ils semblent pouvoir menacer tout - pas seulement les dossiers bancaires et les documents médicaux, mais tout. Ils semblent représenter une menace potentielle fondamentale et universelle, qu'il ne semble pas possible de réduire avec la mise en place de nouvelles normes se basant sur les technologies actuelles. Il apparaît cependant que le coût de la recherche et du développement est élevé et les bénéfices une fois le produit fini sont relativement faibles.

L'informatique quantique est un sujet brûlant à l'heure actuelle, qui aura un impact sur la société que nous ne pouvons même pas prévoir si nous ne reconnaissons pas son importance maintenant. La plupart des ordinateurs actuels fonctionnent selon des signaux numériques. Si quelqu'un essaie de pirater l'ordinateur, il transformera ce signal numérique en une autre forme ou l'annulera, ce qui peut être facilement re- marqué. En revanche, les ordinateurs quantiques utilisent des qubits pour les calculs. Ceux-ci sont liés entre eux d'une manière qui les rend sensibles aux changements d'informations et les rendraient potentiellement vulnérables à de nouveaux types attaques. Si quelqu'un parvenait à pirater un ordinateur quantique - ce qui n'est pas encore possible - cela aurait de graves conséquences sur le maintien des normes de sécurité. Le réveil risque donc d'être brutal lorsque les ordinateurs quantiques seront technologiquement réalisables. Ces machines seront capables d'effectuer des calculs en beaucoup moins de temps que n'importe quel ordinateur conventionnel et rendront les chiffrements actuels inefficaces (et ce, peu importe la quantité de bits de la clé RSA ciblée).

En termes simples, les ordinateurs quantiques traitent l'information différemment des ordinateurs numériques actuels. En effet, ils sont capables d'avoir des bits qui se trouvent dans plus d'un état simultanément, ce qui signifie qu'ils peuvent effectuer de nombreux calculs à la fois. Dans un avenir dominé par l'informatique quantique, toute l'informatique ordinaire sera rendue virtuellement obsolète. Les pirates informatiques pourront accéder aux secrets les plus profonds des entreprises sans avoir besoin d'un mot de passe. Pour éviter ce sort, les entreprises doivent adopter des approches de chiffrement qui les protègent de la technologie quantique, mais elles ne peuvent pas se permettre d'arrêter d'innover de manière trop radicale. Par ailleurs, et de façon paradoxale, une approche de chiffrement indéchiffrables n'est pas nécessairement souhaitée par les États car celles-ci risqueraient de provoquer des problèmes liés à la mise en danger de la sécurité nationale. La menace potentielle imminente de l'informatique quantique doit donc être prise au sérieux, mais cela ne signifie pas qu'il faille paniquer. La meilleure façon de se protéger est de planifier à l'avance et de réfléchir aux solutions possibles. L'incorporation d'éléments de cryptographie quantique n'est pas toujours possible pour tous les clients en raison de son coût. Mais cela pourrait contribuer à sécuriser un client important qui ne peut pas risquer de futures interférences dans ses opérations sensibles.

3. https ://www.darpa.mil/news-events/2021-04-02

Et en France...

L'ambition de la France de devenir un leader mondial [7] de la "deeptech" est l'un des secrets les moins bien gardés d'Europe. Le pays dispose non seulement de l'un des plus grands fonds deeptech d'Europe, Bpifrance, mais aussi, et c'est plus important, de la population et du réservoir de talents que constitue un système universitaire de premier ordre, qui aide le pays à devenir un foyer d'innovation. Le quantum est un segment de la technologie profonde où les Français laissent le reste de l'Europe, et en fait la plupart des autres nations, loin derrière. L'ambition de créer un pôle quantique dans la région parisienne (Pôle de Paris Saclay - Figure 4), reliant les grandes entreprises et les startups, est vraiment impressionnante et d'une grande portée. Non seulement la région se concentre sur l'épanouissement des talents locaux, mais elle recherche aussi activement des entreprises étrangères pour installer leur siège européen dans le pôle.

Figure 4 – Pôle Quantique de Paris Saclay (Source : Les Echos)

La France a toujours été à l'avant-garde de la cryptographie et possède l'un des écosystèmes les plus riches pour les pionniers du quantique. Cette histoire com- prend des individus allant des lauréats du prix Nobel de physique, Albert Fert et Serge Haroche, aux recherches pionnières du médaillé d'or du Centre Nationale de la Recherche Scientifique (CNRS), Alain Aspect sur l'intrication quantique et les simulateurs quantiques. Dans cette optique, le gouvernement français a annoncé au début de l'année 2021 une stratégie de 1,8 milliard d'euros pour stimuler la re- cherche sur les technologies quantiques sur cinq ans. L'investissement public dans ce domaine passera ainsi de 60 à 200 millions d'euros par an. Non seulement l'investissement augmente, mais ce que l'on oublie souvent, c'est que les fonds sont canalisés vers différents domaines de l'informatique quantique. La France reconnaît que l'informatique quantique n'est pas une industrie homogène et que divers aspects nécessitent une attention particulière en dehors du développement d'ordinateurs quantiques proprement dits, en effet, la France semble avoir adoptée une approche plus holistique que les autres pays. Si nos voisins Européens que ce soit le Royaume- Uni ou l'Allemagne se sont lancés dans l'aventure quantique bien avant la France, il semble que celle-ci n'est pas réellement pris de retard grâce à des choix judicieux [4].

4. Élément confirmé par Philippe Duluc - CTO d'Atos

PHILOSOPHIE, TECHNOLOGIE ET CRYPTOLOGIE - EVOLUTIONS VERS LE QUANTIQUE

L'informatique quantique a vu le jour en 1980 lorsque le physicien Paul Benioff a proposé une version quantique de la machine de Turing [8]. Richard Feynman et Yuri Manin ont par la suite suggéré qu'un ordinateur quantique avait le potentiel de simuler des choses qu'un ordinateur classique ne pourrait pas faire. En 1994, Peter Shor a mis au point un algorithme quantique permettant de trouver les facteurs premiers d'un nombre entier, avec la possibilité de déchiffrer des communications chiffrées par RSA [9]. En 1998, Isaac Chuang, Neil Gershenfeld et Mark Kubinec ont créé le premier ordinateur quantique à deux qubits capable d'effectuer des calculs, donc programmable. Malgré les progrès expérimentaux constants réalisés depuis la fin des années 1990, la plupart des chercheurs estiment que l'informatique quantique tolérante aux pannes reste un rêve. Ces dernières années, les investissements dans la recherche sur l'informatique quantique ont augmenté dans les secteurs public et privé. Le 23 octobre 2019, Google AI, en partenariat avec la National Aeronautics and Space Administration (NASA) des États-Unis, a affirmé avoir effectué un calcul quantique infaisable sur n'importe quel ordinateur classique, mais la question de savoir si cette affirmation était ou est toujours valable est un sujet de recherche actif. En effet, à ce jour, une certaine mythologie de l'innovation s'est forgée, et il est parfois compliqué de faire la distinction, entre science, fiction et science-fiction [10].

DE L'INFORMATIQUE QUANTIQUE

Dans cette section, nous présentons l'informatique quantique. Nous tenterons de vulgariser les notions scientifiques en nous limitant à l'essence du sujet.
L'informatique quantique est un type de calcul qui exploite les propriétés collectives des états quantiques, telles que la superposition, l'interférence et l'intrication, pour effectuer des calculs. La superposition quantique est un principe fondamental de la mécanique quantique qui stipule tout comme les ondes en physique classique, deux états quantiques (ou plus) peuvent être combinés ("superposés" - Figure 6) et le résultat sera un autre état quantique valide ; et inversement, que chaque état quan- tique peut être représenté comme une combinaison de deux autres états distincts ou plus. Mathématiquement, il s'agit d'une propriété des solutions de l'équation de Schrödinger ; puisque l'équation de Schrödinger est linéaire, toute combinaison linéaire de solutions sera également une solution. L'intrication quantique est un phénomène physique qui se produit lorsqu'un groupe de particules est généré, inter- agit ou partage une proximité spatiale d'une manière telle que l'état quantique de chaque particule du groupe ne peut être décrit indépendamment de l'état des autres. Le thème de l'intrication quantique est au cœur de la disparité entre la physique classique et la physique quantique : l'intrication est une caractéristique principale de la mécanique quantique qui fait défaut à la mécanique classique.

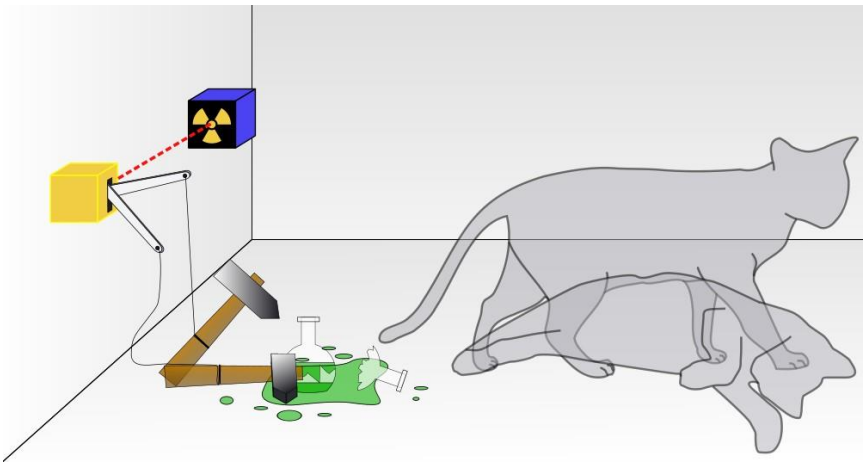

Figure 5 – Illustration de la superposition quantique grace au chat de Schrödinger, simultanément mort et vivant. Source : http ://www.vulgarisation-scientifique.com (Licence Creative Commons Attribution-Share Alike 3.0 Unported)

Le modèle dominant de l'informatique quantique décrit le calcul en termes d'un réseau de portes logiques quantiques. Ce modèle est une généralisation linéaire- algébrique complexe des circuits booléens. Un vecteur représentant tous les états de la mémoire a donc 2^n entrées (une pour chaque état). Ce vecteur "probabilité" représente le fait que la mémoire se trouve dans un état particulier. Dans l'approche classique, la valeur d'une entrée est 1 (c'est-à-dire 100% de probabilité d'être dans cet état) et toutes les autres entrées sont nulles. En mécanique quantique, les vecteurs de probabilité peuvent être généralisés aux opérateurs de densité. Le formalisme du vecteur d'état quantique est généralement introduit en premier parce qu'il est conceptuellement plus simple, et parce qu'il peut être utilisé à la place du formalisme de la matrice de densité pour les états purs, où le système quantique entier est connu.

Partant de l'approche classique, nous commençons par considérer une mémoire simple constituée d'un seul bit. Cette mémoire peut se trouver dans l'un des deux états suivants : l'état 0 ou l'état 1. S'agissant d'une mémoire quantique, celle-ci peut se trouver dans un état de superposition quantique. L'état de cette mémoire quantique à un qubit peut être manipulé en appliquant des portes logiques quantiques, de la même manière que la mémoire classique peut être manipulée avec des portes logiques classiques. Une porte importante pour le calcul classique et quantique est la porte NOT. Les mathématiques des portes à un seul qubit peuvent être étendues pour opérer sur des mémoires quantiques multi-qubits de deux manières importantes. La première consiste simplement à sélectionner un qubit et à appliquer cette porte au qubit cible, sans toucher au reste de la mémoire. Une autre façon consiste à appliquer la porte à sa cible uniquement si une autre partie de la mémoire se trouve dans un état souhaité. Ces deux choix peuvent être illustrés à l'aide d'un autre exemple. En informatique, la porte NOT contrôlée (également appelée C-NOT ou CNOT) constitue quant à elle un élément essentiel de la construction d'un ordinateur quantique à base de portes. Elle peut être utilisée pour intriquer et désintriquer les états de Bell. Tout circuit quantique peut être simulé avec un degré de précision arbitraire en utilisant une combinaison de portes CNOT et de rotations de qubits simples. Par exemple, la porte contrôlée NOT agit sur 2 qubits, et n'effectue l'opération NOT sur le second qubit que lorsque le premier qubit est activé et sinon le laisse inchangé [11].

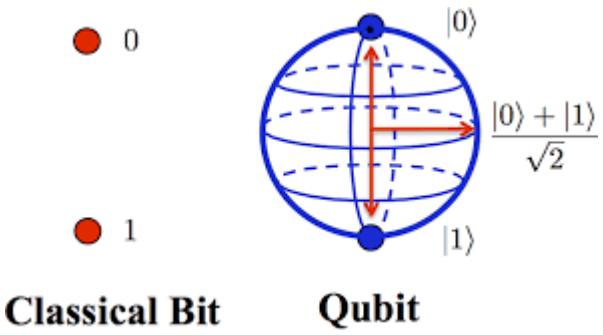

Figure 6 – Illustration de la différence entre un bit et un qubit Source : Zahid Hussain

En résumé, un calcul quantique peut être décrit comme un réseau (Figure 7) de portes logiques quantiques et de mesures [12]. Cependant, toute mesure peut être reportée à la fin du calcul quantique, bien que ce report puisse avoir un coût de calcul, de sorte que la plupart des circuits quantiques représentent un réseau composé uniquement de portes logiques appartenant à une famille de portes assez restreinte. Le choix de la famille de portes qui permet cette construction est connu sous le nom d'ensemble universel de portes, car un ordinateur qui peut exécuter de tels circuits est un ordinateur quantique universel. Un tel ensemble commun comprend toutes les portes à un seul qubit ainsi que la porte CNOT mentionnée ci-dessus. Cela signifie que tout calcul quantique peut être effectué en exécutant une séquence de portes à un seul qubit et de portes CNOT. Bien que cet ensemble de portes soit infini, il peut être remplacé par un ensemble de portes fini en faisant appel au théorème de Solovay-Kitaev.

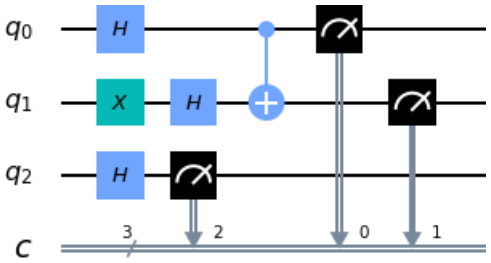

Figure 7 – Illustration d'un circuit quantique (Source : Quiskit 0.36.0)

Les progrès dans la recherche d'algorithmes quantiques se concentrent générale- ment sur ce modèle de circuit quantique, bien qu'il existe des exceptions comme l'algorithme adiabatique quantique [13]. Les algorithmes quantiques peuvent être grossièrement catégorisés selon le type de gain de vitesse obtenu par rapport aux algorithmes classiques correspondants. Les algorithmes quantiques qui offrent une accélération supérieure à un polynôme par rapport à l'algorithme classique le plus connu comprennent l'algorithme de Shor [5] pour la factorisation et les algorithmes quantiques connexes pour le calcul des logarithmes discrets, la résolution de l'équation de Pell et, plus généralement, la résolution du problème des sous-groupes cachés pour les groupes finis abéliens. Aucune preuve mathématique n'a été trouvée qui montre qu'un algorithme classique aussi rapide ne peut pas être découvert, bien que cela soit considéré comme hautement improbable. Certains

problèmes d'oracle comme le problème de Simon et le problème de Bernstein-Vazirani donnent des accélérations prouvables, bien que ce soit dans le modèle d'interrogation quantique, qui est un modèle restreint où les limites inférieures sont beaucoup plus faciles à prouver et ne se traduit pas nécessairement par des accélérations pour les problèmes pratiques.

Lorsque nous parlons d'ordinateur quantique, il n'existe pas à ce jour qu'une seule mise en œuvre physique. En effet, de nombreux candidats différents sont à l'étude que nous pouvons distinguer par le système physique utilisé pour réaliser les qubits. Nous en listons plusieurs ci-dessous [6] :

- Ordinateur quantique supraconducteur (qubit mis en œuvre par l'état de petits circuits supraconducteurs) [15].
- Ordinateur quantique à ions piégés (qubit mis en œuvre par l'état interne des ions piégés) [16]
- Atomes neutres dans les réseaux optiques (qubit implémenté par les états internes des atomes neutres piégés dans un réseau optique) [17].
- Ordinateur à points quantiques, basé sur le spin (par exemple, l'ordinateur quantique de Loss-DiVincenzo [18]) (qubit donné par les états de spin des électrons piégés)
- Ordinateur à points quantiques, à base spatiale (qubit donné par la position de l'électron dans un double point quantique) [19].
- Ordinateur quantique utilisant des puits quantiques artificiels, qui pourrait en principe permettre la construction d'ordinateurs quantiques fonctionnant à température ambiante [20].
- Fil quantique couplé (qubit mis en œuvre par une paire de fils quantiques couplés par un contact ponctuel quantique) [21]
- Ordinateur quantique à résonance magnétique nucléaire (NMRQC) mis en œuvre avec la résonance magnétique nucléaire de molécules en solution, où les qubits sont fournis par les spins nucléaires au sein de la molécule dissoute et sondés avec des ondes radio [22].
- Ordinateurs quantiques NMR Kane à l'état solide (qubit réalisé par l'état de spin nucléaire des donneurs de phosphore dans le silicium) [23]
- Ordinateur quantique vibrationnel (qubits réalisés par des superpositions vibrationnelles dans des molécules froides) [24]
- Ordinateurs quantiques électrons-sur-hélium (le qubit est le spin de l'électron) [25]
- Électrodynamique quantique des cavités (CQED) (qubit fourni par l'état in- terne d'atomes piégés couplés à des cavités à haute finesse) [26]
- Aimant moléculaire (qubit donné par les états de spin) [27]
- Ordinateur quantique ESR à base de fullerène (qubit basé sur le spin électronique d'atomes ou de molécules enfermés dans des fullerènes) [28] .
- Ordinateur quantique optique non linéaire (qubits réalisés en traitant les états de différents modes de la lumière à travers des éléments linéaires et non linéaires) [29]

5. Certains algorithmes quantiques, comme l'algorithme de Grover et l'amplification d'ampli- tude, donnent des accélérations polynomiales par rapport aux algorithmes classiques correspon- dants. Bien que ceux-ci donnent des accélérations quadratiques comparativement modestes, ils sont largement applicables et fournissent donc une solution pour une large gamme de problèmes. De nombreux exemples d'accélérations quantiques démontrables pour des problèmes d'interrogation sont liés à l'algorithme de Grover [14]. En effet, l'algorithme de Brassard, Høyer et Tapp permet de trouver les collisions dans les fonctions deux à un, ou l'algorithme de Farhi, Goldstone et Gutmann qui permet d'évaluer les arbres NAND, une variante du problème de recherche.

6. Cette liste peut être retrouvée sur https://en.wikipedia.org/wiki/Quantum_computing en anglais et de façon plus étendue, nous avons entrepris une lecture des papiers cités afin de la corroborer.

- Ordinateur quantique optique linéaire (qubits réalisés en traitant les états de différents modes de la lumière par des éléments linéaires, par exemple des miroirs, des séparateurs de faisceau et des déphaseurs) [30].
- Ordinateur quantique à base de diamant [31] (qubits réalisés par le spin électronique ou nucléaire des centres de vacance d'azote dans le diamant)
- Ordinateur quantique basé sur le condensat de Bose-Einstein [32].
- Ordinateur quantique à base de transistors - ordinateurs quantiques à chaîne avec entraînement des trous positifs à l'aide d'un piège électrostatique
- Ordinateurs quantiques à base de cristaux inorganiques dopés par des ions de métaux de terres rares [33] (qubit réalisé par l'état électronique interne des dopants dans les fibres optiques)
- Ordinateurs quantiques basés sur des nanosphères de carbone de type métallique [34].

Le grand nombre de candidats démontre que l'informatique quantique, malgré des progrès rapides, n'en est encore qu'à ses balbutiements. Il existe un certain nombre de modèles de calcul pour l'informatique quantique, qui se distinguent par les éléments de base dans lesquels le calcul est décomposé. Pour les mises en œuvre pratiques, les quatre modèles de calcul les plus pertinents sont les suivants :

1. Réseau de portes quantiques - Calcul décomposé en une séquence de portes quantiques de quelques qubits.
2. Ordinateur quantique à sens unique - Calcul décomposé en une séquence de mesures de l'état de Bell[35] et de portes quantiques à un seul qubit appliquées à un état initial hautement intriqué (un état cluster), à l'aide d'une technique appelée téléportation de portes quantiques.
3. Ordinateur quantique adiabatique, basé sur le recuit quantique - Calcul décomposé en une transformation lente et continue d'un hamiltonien initial en un hamiltonien final, dont les états fondamentaux contiennent la solution [36].
4. Ordinateur quantique topologique - Calcul décomposé en tressage d'anyons dans un réseau 2D [37].

La machine de Turing quantique est importante sur le plan théorique, mais la mise en œuvre physique de ce modèle n'est pas réalisable. Il a été démontré que tous ces modèles de calcul - circuits quantiques, calcul quantique à sens unique, calcul quan- tique adiabatique et calcul quantique topologique - sont équivalents à la machine de Turing quantique ; si l'on dispose d'une mise en œuvre parfaite d'un tel ordi- nateur quantique, il peut simuler tous les autres avec une surcharge polynomiale. Cette équivalence n'est pas nécessairement valable pour les ordinateurs quantiques pratiques, car les frais généraux de simulation peuvent être trop importants pour être pratiques.

L'APPROCHE QUANTIQUE PAR RAPPORT A L'APPROCHE TRADITIONNELLE

Dans cette section, nous comparons l'approche quantique par rapport à l'approche traditionnelle.

L'unité de construction de base d'un ordinateur est le bit. Nous savons tous que les bits sont bouléens et correspondent donc seulement aux valeurs 0 et 1. Mais que cela signifie-il concrètement ? Même si ceux-ci jouent un rôle majeur dans l'ordinateur, personne ne s'en occupe directement. Un ordinateur est constitué de circuits et de fils. Nous savons que les

informations sont transportées, stockées et traitées grâce à l'électricité. Un seul fil à l'intérieur d'un ordinateur peut être soit activé soit désactivé (0 ou 1). Un seul fil transporte donc une information de 0 ou de 1. C'est en effet, la plus petite quantité d'informations qu'un ordinateur peut transporter. Avec un fil, vous pouvez transporter deux unités d'information. Ainsi, avec l'augmentation du nombre de fils, le stockage d'informations augmente également. Avec un plus grand nombre de fils, vous pouvez stocker des informations plus complexes [38].

Nous utilisons les systèmes de nombres binaires pour le transfert et le traitement des informations dans un ordinateur. Tous les nombres peuvent être représentés par des combinaisons de 0 et de 1 ou, plus précisément, avec plus de fils à l'intérieur d'un ordinateur, vous pouvez représenter n'importe quoi à partir de nombres, plus précisément des éléments tels que des caractères ou des images. Avec huit fils, nous pouvons stocker jusqu'à 255 nombres décimaux. Chaque lettre d'un texte peut être considérée comme un nombre auquel est associé une représentation binaire. De même, chaque image dans un ordinateur est divisée en millions de pixels. Chaque pixel contient du Rouge-Vert-Bleu (RVB), les valeurs du RVB à l'intérieur de chaque pixel correspondent à un nombre qui, là encore, traite de représentations binaires. De même, les sons sont des ondes, chaque onde sonore peut être représentée dans un graphique de telle sorte que chaque position à l'intérieur de l'onde correspond à une valeur. À partir de ces chiffres, vous pouvez comprendre que tout texte, image, vidéo et son peut être converti en représentations binaires qui peuvent ensuite être traités par des fils à l'intérieur de l'ordinateur.

Un développeur code également dans des langages de haut niveau comme python, java, ruby, etc., ce qui représente un ensemble d'instructions qui sont à nouveau converties en binaire, plus précisément en bits de 0 et de 1. La cellule est l'unité structurelle, fonctionnelle et biologique de base de tous les organismes connus. De même, les bits sont l'unité de base de l'informatique classique. Nous connaissons tous les capacités des ordinateurs classiques. Avec les progrès de l'informatique, un ordinateur peut désormais être entraîné à apprendre par lui-même, comme dans les voitures qui conduisent toutes seules ou les robots imitant les humains. En effet, l'intelligence artificielle permet aujourd'hui la reconnaissance de la parole humaine, la reconnaissance d'image en deux ou trois dimensions, la compréhension des émotions et des comportements humains, entre autres. Les supercalculateurs sont des ordinateurs aux performances de très haut niveau. Il existe des supercalculateurs qui peuvent effectuer plus de cent quadrillions de FLOPS (opérations en virgule flottante par seconde).

Cependant, ces supercalculateurs reposent sur des approches classiques et traditionnelles, et celles-ci ont les limites suivantes. Le calcul classique a été l'épine dorsale de notre société. De la radiotélévision à l'envoi de robots sur Mars. *"Mais beaucoup des plus grands mystères du monde et des plus grandes opportunités potentielles restent hors de portée des ordinateurs classiques"*, déclare Stefan Filipp, un scientifique quantique à IBM Research. *"Pour poursuivre le rythme des progrès, nous devons compléter l'approche classique par une nouvelle plate-forme, qui suit son propre en- semble de règles. C'est l'informatique quantique".*

L'informatique quantique possède une capacité de calcul supérieure à tout ce que les ordinateurs classiques actuels pourront jamais atteindre. En effet, les ordinateurs quantiques

peuvent effectuer des calculs à une vitesse exponentielle (littéralement) par rapport aux ordinateurs binaires classiques actuels. Ils sont donc suffisamment puissants pour combler les lacunes qui existent aujourd'hui dans les prévisions météo- rologiques, la découverte de médicaments, la modélisation financière et de nombreux autres domaines complexes. Fondamentalement, un ordinateur classique stocke les informations sous la forme de 0 et de 1 appelés bits, tandis qu'un ordinateur quantique utilise des qubits pour coder ses informations. Dans le cas de l'informatique classique, les bits ont deux états, mais ici, dans l'informatique quantique, les qubits peuvent être en superposition et peuvent se trouver en n'importe quel point de la sphère de Bloch (8) ci-dessous qui représente les 0, 1 et superpositions afférentes.

L'acte de mesurer un qubit change l'état du qubit. Avec la mesure, le qubit passe de l'état de superposition à l'un des états classiques. Les ordinateurs classiques codent l'information en bits, chaque bit codant deux valeurs possibles, 0 ou 1. Un qubit code deux valeurs simultanément, 0 et 1. Deux bits classiques codent une des quatre valeurs possibles (00, 01, 10, 11) alors que deux qubits codent une superposition que conque des quatre états simultanément, bien que nous ne puissions obtenir qu'une seule de ces valeurs lors de la mesure. Quatre qubits codent toute superposition de seize valeurs simultanément, et ainsi de suite, de manière exponentielle. Cent qubits peuvent coder plus d'informations que ce qui est disponible dans les plus grands systèmes informatiques actuels.

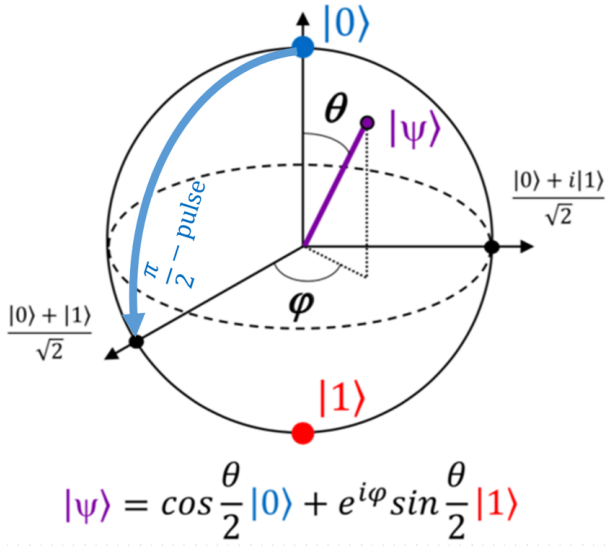

Figure 8 – Qubit : Sphère de Bloch

CRYPTOGRAPHIE - DES PREMICES AU POST QUAN- TIQUE

Après avoir présenté les éléments technologiques, nous nous proposons de discuter des impacts sur les méthodes et approches de chiffrement, c'est à dire la cryptographie.

En effet, depuis aussi loin que remonte la civilisation, les personnes ayant un statut social important, comme les chefs d'états ou les marchands, ont éprouvé le besoin de communiquer à distance avec leurs homologues en toute discrétion. Les missives étaient portées par des messagers de confiance, généralement codées dans un langage connu des

seuls auteurs et destinataires, et dûment authentifiées par une marque distinctive, comme les sceaux imprimés dans l'argile que l'on retrouve dès la civilisation Uruk, 4000 ans avec JC [39]. Si on insiste sur les méthodes de chiffrement dans la transmission des messages, l'authentification de l'auteur est aussi importante que le message lui-même. Un défaut d'authentification ouvre en effet la porte à l'usurpation d'identité, qui est le problème principal d'une nuisance très actuelle comme le "phishing".

Au fil du temps, les procédures de chiffrement des messages et d'authentification de leurs auteurs évoluèrent et se complexifièrent, du "code de César", en passant par la machine Enigma [40] des Nazis pendant la seconde guerre mondiale. Ces tech- niques restèrent encore relativement artisanales jusqu'à l'arrivée de l'ordinateur, puis de l'interconnexion des ordinateurs au niveau mondial avec internet. Le besoin d'échanger massivement des messages de façon sécurisée, fonctionnalité qui n'avait pas été prévue dans les protocoles internet, devint alors limitant pour l'adoption d'internet comme mode de transmission des données, que ce soit au niveau des états ou des entreprises.

Les contraintes de chiffrement des messages changèrent alors de nature par rapport à ce qui s'était fait depuis des millénaires. En effet, on communiquait précédemment en mode "one to one", avec une personne connue avec laquelle on avait précédemment convenu d'un code. Et ce message était porté par un tiers de confiance, dont la vie dépendait du fait que ce message resterait confidentiel. On devait passer brutalement à une communication " one to many" avec des personnes que l'on ne connaissait pas, sans avoir la possibilité de se rencontrer physiquement pour échanger un code. Car tout est là : On ne peut pas transmettre d'informations de façon sécurisée à un tiers via le réseau internet si on n'a pas convenu au préalable d'un code, car un tiers peut espionner le réseau. Et pour transmettre le code, il faut un moyen de communication sécurisé...

En effet, le principal problème de la confidentialité des messages envoyés par inter- net n'est pas lié au chiffrement lui-même, qui peut être fait de façon fort complexe et théoriquement impossible à casser, ou plus simplement avec une approche basique mais robuste de type XOR (opérateur du ou exclusif). Le problème vient du fait qu'il faut forcément une clé pour crypter un message suivant la méthode dite "symétrique", c'est à dire que la clé pour chiffrer le message est la même que celle utilisée pour le déchiffrer. Par conséquent on ne peut pas envoyer la clé qui va servir à crypter le message par le même canal que le message lui-même, sinon le pirate récupérera la clé avec le message, ce qui rend tout chiffrage inutile. Il n'y a aucun moyen de sortir de ce problème. Jusque dans les années 60, les communications entre la Maison Blanche américaine et le Kremlin étaient chiffrées avec une clé, laquelle était apportée par un diplomate dans une valise. On n'imagine pas évidemment aller voir son interlocuteur pour lui remettre la clé de cryptage avant de lui envoyer un mail.

C'est donc pour pallier ce problème que furent inventées les méthodes de crypto- graphie "asymétriques" où la clé utilisée pour le chiffrement est différente de celle utilisée pour le déchiffrement du message. L'intérêt de ce procédé est que l'on peut communiquer la clé qui sert à crypter (appelée clé publique) aux personnes qui veulent vous envoyer des messages. Même si le message chiffré est intercepté en cours de route, personne ne pourra le déchiffrer, car pour cela il faut la clé de déchiffrement ou "clé privée" que vous êtes seul à posséder. La clé privée permet également de s'authentifier auprès des tiers. Dans la pratique, le chiffrement asymétrique est utilisé généralement pour transmettre une clé de

chiffrement symétrique, lequel est beaucoup moins gourmand en calculs, et les messages sont ensuite transmis avec un chiffrement symétrique, sans risquer que la clé soit découverte.

La dernière génération de ce système à clé publique / privée, qui est actuellement un des piliers de la sécurité de l'internet est le système de clés RSA (du nom de ses trois inventeurs, Rivest, Shamir et Adleman). Bien que peu d'utilisateurs de l'internet soient conscients d'utiliser ce système, il est néanmoins omniprésent dans l'utilisation quotidienne d'internet. Le https par exemple (http sécurisé) ainsi que tous les autres protocoles sécurisés (SSH, SFTP notamment) utilisent ce système. Les Blockchains, qui servent à gérer les cryptomonnaies mais également d'autres nombreux produits dérivés comme les NFT sont basées sur ce système. Les QR codes utilisés pour les passes sanitaires sont basés également sur cette technique.

Pourtant, ce système de chiffrement asymétrique, même s'il est utilisé depuis près de 20 ans, n'en est pas pour autant inviolable. Théoriquement, il est même tout à fait possible de le casser. Il est important de comprendre que ce système ne repose pas sur une sécurité absolue du système, mais sur le fait que l'attaquant ne dispose pas (en théorie) des ressources de calcul suffisantes pour casser le code, et que même s'il les possédait, compte-tenu de la puissance de calcul nécessaire, cela lui prendrait tellement longtemps (en milliers d'années) que la réponse ne pourrait servir à personne.

Le système de clés RSA repose sur un problème de mathématique bien connu : la difficulté de factoriser un nombre composé par la multiplication de deux grands nombres premiers. Il n'y a pas de méthode permettant d'obtenir rapidement ce résultat, il faut faire des divisions jusqu'à trouver le bon nombre Dans le système de clés RSA, l'application cherche donc aléatoirement deux grands nombres premiers p et q, et les multiplie l'un par l'autre pour obtenir le nombre n qui sera le "module de chiffrement". A partir de ce module de chiffrement, l'application va créer une clé publique et une clé privée, en ajoutant quelques éléments secondaires. Pour connaître la clé privée, le pirate informatique doit donc tout d'abord se procurer la clé publique. Comme leur nom l'indique, les clés publiques sont rarement très protégées, elles sont même parfois disponibles sur des annuaires presque publics. Cette première étape est donc souvent assez facile à réaliser. Il faut ensuite extraire de la clé publique le module de chiffrement, ce qui ne pose pas de problème, et diviser ensuite ce nombre par tous les nombres possibles jusqu'à trouver l'un des deux di- viseurs, ce qui fournira également le second du même coup. C'est là que réside le problème.

Prenons un exemple :

Imaginons que le nombre n extrait de la clé publique soit

$n = 182276298679$

Nous savons que ce nombre est composé de deux diviseurs de même taille, p et q. Le nombre n faisant douze chiffres, les deux diviseurs font probablement chacun six chiffres, car on va prendre les nombres premiers les plus grands possibles, pour rendre le calcul plus complexe. Pour trouver le premier diviseur, nous allons donc commencer par diviser notre

nombre n par le plus petit nombre premier de six chiffres. Fort heureusement, il existe des listes de nombres premiers jusqu'à plusieurs milliards, nous allons donc consulter une table qui va nous indiquer ce plus petit nombre premier à six chiffres :

p = 100129

Il nous faut alors calculer le reste de la division de n par p et ce reste doit être égal à 0. On utilise pour cela l'opérateur Modulo, qui nous donne le reste d'une division d'un nombre par un autre.

182276298679*Mod*100129 = 65273

Le reste de la division est 65273. p n'est donc pas diviseur de n. Nous allons devoir recommencer cette opération jusqu'à tomber sur la bonne valeur de p, en passant comme argument la liste de tous les nombres premiers de six chiffres. Après de nombreux calculs nous arrivons à :

182276298679*Mod*201769 = 0

p = 201769

Pour trouver q il nous faut donc poser :

182276298679/201769 = 903391

q = 903391

Extrait de la liste des nombres premiers de 2 à 1000 milliards

Il y a tout d'abord un nombre important de problèmes liés à la complexité de l'implémentation. En effet, si l'utilisation du chiffrement est transparente pour les utilisateurs quand ils utilisent un navigateur avec le protocole https sécurisé, il en va tout autrement pour celui qui désire par exemple accéder à un service de transfert de fichier SFTP par clé RSA. Cette utilisation est de fait réservée à des informaticiens. Il y a peu de chances que des utilisateurs bureautiques sans bagage spécifique puissent créer une paire de clé publique / privée et l'utiliser dans un contexte professionnel. En effet, il faut pour commencer créer la paire de clés avec un outil aussi peu intuitif que Putty sur Windows, ou en lignes de commande sur Linux. Il y a de plus deux formats de clés possibles. Lequel est le bon ? Il faut ensuite charger la clé publique, la mettre au bon endroit, faire des choix sur des éléments techniques sur lesquels vous n'avez aucune compétence, puis il faut paramétrer le logiciel qui va utiliser la clé, et là encore il n'y a rien d'intuitif dans ce processus. Et si ça ne marche pas comment fait-t-on ? A qui peut-on s'adresser ?

L'enjeu de la sécurité étant toutefois important, on peut alors essayer de régler le problème en ayant un responsable technique qui va créer les clés pour chaque utilisateur, les installer, et ce dernier n'aura plus qu'à l'utiliser. Mais on se heurte alors à un autre aspect : les clés doivent être créées sur l'ordinateur sur lequel elles seront utilisées. Il ne sert à rien en effet de créer des clés secrètes si c'est pour les envoyer ensuite par courriel à son utilisateur qui est par exemple en télétravail (chose que l'on voit dans de nombreuses entreprises avec les mots de passe), ou par un réseau sur lequel celles-ci peuvent être interceptées.

De plus, si nous utilisons la clé pour nous authentifier auprès d'un service en ligne, nous n'allons plus pouvoir lors de nos déplacements lire les courriels avec notre téléphone portable, parce que cela nécessiterait d'avoir la clé également sur notre portable. Ce qui suppose de la transférer, et ouvre ainsi une possibilité d'interception de la clé dans le transfert, mais aussi une fois qu'elle est sur le téléphone portable. Les clés doivent également être mises à jour régulièrement. Qui va s'en occuper ? Et selon quelle procédure ? On voit que même si les clés RSA sont une avancée pour la sécurité dans de nombreux domaines, leur mise en place effective est complexe et l'ajout de complexité supplémentaire est rédhibitoire pour de nombreuses utilisations bureautique déjà chronophages.

En 2019, les spécialistes de la cryptographie pensaient encore faire évoluer le système de clés RSA en augmentant simplement la taille des clés. Cette augmentation devait suffire pour être tranquilles pendant de nombreuses années mais cette approche toutefois ne sera probablement jamais mise en place. D'une part parce que l'allongement des clés augmente également très fortement la complexité des calculs, et la quantité d'information à transférer. Et tout cela a un coût technique qui limite en réalité l'augmentation de la taille des clés. Mais le principal problème, qui n'était encore envisagé que de façon théorique par les spécialistes il y a seulement encore trois années, est l'arrivée de l'informatique quantique.

La cryptographie quantique est la science qui consiste à exploiter les propriétés de la mécanique quantique pour effectuer des tâches cryptographiques. L'avantage de la cryptographie quantique réside dans le fait qu'elle permet l'exécution de diverses tâches cryptographiques dont il est prouvé ou conjecturé qu'elles sont impossibles en utilisant uniquement la communication classique (c'est-à-dire non quantique). Par exemple, il est impossible de copier des données encodées dans un état quantique. Si l'on tente de lire les données codées, l'état quantique sera modifié en raison de l'effondrement de la fonction d'onde (théorème du non-clonage). Cela pourrait être utilisé pour détecter l'écoute clandestine dans la distribution de clés quantiques (QKD).

La cryptographie quantique utilise des particules individuelles de lumière, ou photons, pour transmettre des données sur un fil de fibre optique. Les photons représentent des bits binaires. La sécurité du système repose sur la mécanique quantique. Ces propriétés sécuritaires sont les suivantes :

1. Les particules peuvent exister à plus d'un endroit ou état à la fois.
2. Une propriété quantique ne peut être observée sans la modifier ou la perturber.
3. Des particules entières ne peuvent être copiées.

Ces propriétés font qu'il est impossible de mesurer l'état quantique d'un système sans le perturber. Les photons sont utilisés pour la cryptographie quantique car ils offrent toutes les qualités nécessaires : Leur comportement est bien compris et ils sont des vecteurs d'information dans les câbles à fibres optiques. L'un des exemples les plus connus de cryptographie quantique est actuellement la distribution de clés quantiques (QKD), qui fournit une méthode sécurisée d'échange de clés.

La profession se prépare depuis des années à l'arrivée de l'informatique quantique. En effet, le National Institute of Standards and Technology (NIST) se penche depuis 2017 sur le chiffrement post-quantique, basé sur le même principe de clé publique
/ clé privée, mais avec d'autres méthodes que la factorisation de grands nombres. Par définition, la cryptographie post-quantique est une branche de la cryptographie visant à garantir la sécurité de l'information face à un attaquant disposant d'un calculateur quantique. Cette discipline est distincte de la cryptographie quantique, qui comme indiqué précédemment vise à construire des algorithmes cryptographiques utilisant des propriétés physiques (plutôt que mathématiques) pour garantir la sécurité. En l'effet, les algorithmes quantiques de Shor, de Grover et de Simon (cité ci-dessus) étendent les capacités par rapport à un attaquant ne disposant que d'un ordinateur classique. S'il n'existe pas à l'heure actuelle de calculateur quantique représentant une menace concrète sur la sécurité des systèmes déployés, ces algorithmes permettent de résoudre certains problèmes calculatoires sur lesquels sont fondés plusieurs approches.

En novembre 2017, date annoncée à laquelle les candidats devaient présenter leurs méthodes candidates au post-quantique, le NIST reçut soixante-neuf propositions. En 2022, arrivés au troisième et dernier tour de sélection, il reste cinq à sept candidats en lice, avec plusieurs méthodes de chiffrement. Sur sept méthodes candidates, cinq sont basées sur des problèmes de réseau connu d'une manière générique comme le problème NTRU [7]. Le chiffrement utilisant des clés publiques privées basées sur le problème NTRU est déjà ancien et il est utilisé dans certains domaines comme le RFID [8]. Des bibliothèques sont disponibles en langage java et en C# pour implémenter ce système. La communauté scientifique s'accorde pour dire qu'il n'y a pas d'attaque connue sur le système de cryptage utilisant NTRU, même avec les ordinateurs quantiques. On peut donc penser que NTRU est le Graal de la cryptographie qui va pouvoir remplacer RSA. Néanmoins, l'expérience montre qu'entre des expérimentations réalisées par quelques chercheurs dans des laboratoires scientifiques et la mise en place à grande échelle d'applications sécurisées dans un contexte professionnel, il peut se passer beaucoup d'évènements imprévisibles.

Tout d'abord, sans même remettre en question le principe lui-même de NTRU, sur lequel il existe relativement peu de données disponibles pour le moment, entre le principe du système, son implémentation et sa mise en place, des failles peuvent apparaître et être exploitées par les attaquants. Depuis les années 80 et la "crise du logiciel" on sait que tout système informatique complexe va inévitablement contenir des erreurs. La correction des bugs fait partie du cycle de vie des appli- cations informatiques. Ainsi, même avec un système parfait, une habile exploitation d'une imperfection de son implémentation pourrait permettre d'hacker les clés. Ensuite On va retrouver les problèmes des clés RSA actuelles : cela restera limité aux standards de l'internet, la mise en place de ces clés dans un contexte professionnel bureautique ne sera pas plus simple. Pour illustrer un peu plus avant les approches post-quantiques, nous présentons ci-dessous, les cinq les plus fréquemment évoquées. Cette liste peut être aussi partiellement retrouvée en anglais sur https://en.wikipedia.org/wiki/Post-quantum_cryptography, les papiers cités ont été étudiés afin de vérifier l'intégrité de celle-ci :

1. Cryptographie basée sur les treillis : cette approche inclut des systèmes cryptographiques tels que l'apprentissage avec des erreurs, l'apprentissage en anneau avec des erreurs (ring-LWE), l'échange de clé en anneau avec des erreurs et la signature en anneau avec des erreurs, les anciens schémas de chiffrement NTRU [9] ou

GGH [10], et les signatures NTRU et BLISS [11] plus récentes. Certains de ces schémas comme le chiffrement NTRU ont été étudiés pendant de nombreuses années sans que personne ne trouve une attaque réalisable. D'autres, comme les algorithmes ring-LWE, ont prouvé que leur sécurité se réduisait à un problème de pire cas. Un groupe d'étude [41] sur la cryptographie post quantique a suggéré que la variante Stehle-Steinfeld de NTRU soit étudiée en vue d'une normalisation [42, 43].

2. Cryptographie multivariée : elle comprend des systèmes cryptographiques tels que le schéma Rainbow, qui repose sur la difficulté de résoudre des systèmes d'équations multivariées. Diverses tentatives de construction de systèmes de cryptage sécurisés à équations multivariées ont échoué. Cependant, les schémas de signature multivariés pourraient servir de base à une signature numérique quantique sécurisée [44].

7. NTRU : algorithme de chiffrement, connu également sous le nom NTRUEncrypt
8. RFID : Radio Frequency IDentification

1. Cryptographie basée sur le Hash : cette catégorie comprend des systèmes cryptographiques tels que les signatures Lamport et le schéma de signature Merkle, ainsi que les schémas plus récents XMSS et SPHINCS. Les signatures numériques basées sur le hachage ont été inventées à la fin des années 70 par Ralph Merkle et ont été étudiées depuis comme une alternative intéressante aux signatures numériques basées sur la théorie des nombres comme RSA et DSA. Leur principal inconvénient est que pour toute clé publique basée sur le hachage, il existe une limite au nombre de signatures pouvant être signées à l'aide de l'ensemble correspondant de clés privées. Ce fait a réduit l'intérêt pour ces signatures jusqu'à ce que l'intérêt soit relancé en raison du désir d'une cryptographie résistante aux attaques des ordinateurs quantiques. Il convient de noter que tous les schémas ci-dessus sont des signatures à temps unique ou à temps limité [45].
2. Cryptographie basée sur me code : cette catégorie comprend les systèmes cryptographiques qui reposent sur des codes correcteurs d'erreurs, tels que les algorithmes de chiffrement de McEliece et de Niederreiter et le schéma de signature de Courtois, Finiasz et Sendrier. La signature originale de McEliece, qui utilise des codes aléatoires de Goppa, a résisté à un examen minutieux pendant plus de quarante ans. Cependant, de nombreuses variantes du schéma de McEliece, qui cherchent à introduire plus de structure dans le code utilisé afin de réduire la taille des clés, se sont révélées peu sûres. Un groupe d'étude
   [41] sur la cryptographie post quantique a recommandé le système de cryptage à clé publique de McEliece comme candidat pour une protection à long terme contre les attaques des ordinateurs quantiques [44].
5. Cryptographie basée sur les courbes elliptiques isogéniques supersingulières : ce système cryptographique s'appuie sur les propriétés des courbes elliptiques supersingulières et des graphes d'isogénie supersingulière pour créer un remplacement de Diffie-Hellman avec secret de transmission. Ce système cryptographique utilise les mathématiques bien étudiées des courbes elliptiques super singulières pour créer un échange de clés de type Diffie-Hellman qui peut servir de remplacement simple et résistant à l'informatique quantique pour les méthodes d'échange de clés Diffie-Hellman et Diffie-Hellman à courbe elliptique qui sont largement utilisées aujourd'hui [46].
6. Résistance quantique des clés symétriques : à condition d'utiliser des clés de taille suffisamment grande, les systèmes cryptographiques à clé symétrique comme AES et SNOW 3G sont déjà résistants aux attaques d'un ordina- teur quantique. En outre, les systèmes et protocoles de gestion des clés qui utilisent la cryptographie à clé symétrique au lieu de la cryptographie à clé publique, comme Kerberos et la structure d'authentification des réseaux mo- biles 3GPP, sont également intrinsèquement sûrs contre les attaques d'un ordinateur quantique. Étant donné qu'elle est déjà largement déployée dans le monde, certains chercheurs recommandent d'étendre l'utilisation de la ges- tion des clés symétriques de type Kerberos comme moyen efficace d'obtenir dès aujourd'hui une cryptographie post quantique [47].

9. N-Th Degree Truncated Polynomial Ring
10. GGH : chiffrement Goldreich-Goldwasser-Halevi
11. BLISS : signature Bimodal Lattice Signature Scheme

Mais concernant la sécurité du système lui-même, on peut tout de même constater que, quel que soit le système choisi, l'essentiel de la sécurité de l'internet reposera sur lui. Le principal danger étant la possibilité d'utiliser l'informatique quantique pour casser les codes qui vont être produits, on peut se demander si le risque a bien été évalué. En effet, quasiment aucun chercheur n'a pu pour le moment utiliser d'ordinateur quantique, et la programmation, et même l'algorithmique permettant d'utiliser ces machines en sont encore à leurs balbutiements. Tout ce qui a été fait jusque-là est de l'émulation d'ordinateurs quantiques. Et le nombre de chercheurs qui ont travaillé dans ce domaine est encore assez réduit.

Le développement de la puissance de ces machines semble suivre une courbe similaire à la loi de Moore, avec une augmentation beaucoup plus rapide que tout ce qui avait été prévu. On peut aussi imaginer que l'on va pouvoir mettre à profit ces machines pour utiliser ce que l'on appelle communément « l'intelligence artificielle
» pour trouver des solutions originales à des problèmes que les humains n'ont pas découvertes. Nul ne sait ce qui va sortir du chapeau quantique dans les années qui viennent. Et compte-tenu des immenses enjeux stratégiques de la sécurité internet, tout ce qui va être possible de faire sera fait. On n'est plus dans des programmes de recherche scientifiques, on est dans des luttes de pouvoir au niveau mondial, et des dizaines de milliards vont être dépensés pour en prendre le contrôle. Alors s'il n'existe pas aujourd'hui de méthode pour casser la méthode de cryptage NTRU, ou quelle que soit celle qui sera choisie, sa sécurité va être mise à rude épreuve.

Un autre paramètre est également à prendre en compte. Si la communauté scientifique du début des années 90, après la chute du mur de Berlin, vit une coopération mondiale pour le développement de l'internet (avec néanmoins une nette prééminence des États-Unis) , il en va tout autrement en 2022, dans un monde qui se fragmente à nouveau entre un groupe à domination américaine vs un autre dominé par la Chine et la Russie. Si un chercheur d'un des deux « blocs » trouve la clé qui permet de casser le code, rien ne dit que la nouvelle va se répandre. Il serait beaucoup plus profitable d'exploiter cet avantage concurrentiel qui leur laissera une longueur d'avance sur leurs adversaires.

MENACES OU OPPORTUNITÉS POUR LA SOCIÉTÉ

Comme l'intelligence artificielle, la microélectronique, les technologies de la santé, de l'énergie ou du spatial, les technologies quantiques font partie de ces quelques clés du futur que les nations veulent maîtriser et contrôler. La physique quantique a déjà donné depuis la moitié du 20ème siècle des applications qui sont rentrées dans notre quotidien : le transistor, les lasers, les GPS, les leds, ce qui structure l'internet même et l'informatique. A l'heure actuelle, nous sommes au cœur d'une deuxième révolution où tout s'accélère : des problèmes clés pourront se résoudre à travers le quantique. Le calcul quantique permettra de résoudre des problèmes insolubles avec l'informatique classique, les temps de calcul seront drastiquement réduits, les capteurs quantiques permettront une navigation sans GPS, etc.[48].

Ces technologies sont une opportunité, elles vont radicalement changés la donne dans la lutte contre le réchauffement climatique, dans le développement durable de la production agricole et donc avec une série d'applications concrètes complètement inestimables. A l'heure où les supercalculateurs du monde entier sont mobilisés pour rechercher des traitements pour lutter efficacement contre la covid-19, les ordinateurs quantiques pourraient devenir dans le futur, l'une des armes les plus puissantes jamais conçues contre les crises sanitaires. L'industrie bénéficiera ainsi de tout nouveaux outils de simulation et d'optimisation, et ce dans les domaines de la sécurité, de la défense et de la cybersécurité. L'informatique quantique va ainsi permettre de réaliser des applications de grandes technologies mêmes celles que nous n'imaginons pas encore.

L'informatique quantique suscite a cet effet les plus grands espoirs : imaginons dans la santé, un ordinateur quantique permettant la création de médicaments, protéines et enzymes beaucoup plus efficaces, car il permettra d'explorer le fonctionnement des molécules et de simuler leurs interactions avec un niveau de complexité inédit. Dans les transports, l'énergie, la logistique, la finance, le marketing ou encore la cybersécurité, l'informatique quantique pourrait identifier très rapidement les situations les plus optimales grâce à sa capacité à traiter simultanément tous les scenarii issus d'une masse toujours plus importante de données.

De nombreuses nations aspirent à devenir leader de l'informatique quantique. Mais, avec les milliards d'investissements qui affluent, il ne sera pas facile d'arriver en tête. Les gouvernements du monde entier annoncent des programmes nationaux de sou- tien au développement de l'informatique quantique et des stratégies quinquennales ou décennales. Et à mesure que les pays débloquent des budgets, il devient évident qu'une compétition acharnée se met progressivement en place. Les nations veulent s'assurer qu'elles seront au niveau, lorsque les technologies quantiques commenceront à montrer une certaine valeur dans le monde réel.

Avec un marché mondial estimé à 830 millions de dollars d'ici deux ans, l'informa- tique quantique promet aux pays qui s'imposeront dans cette compétition technologique mondiale un avantage commercial et sécuritaire, voire militaire, considérable [49].
Force est de constater à ce stade que, comme beaucoup d'autres domaines techno- logiques et/ou scientifiques, les États-Unis et la Chine dominent ce nouveau marché disruptif.

Aux États-Unis, la coordination inter-agences fédérales des recherches sur le quan- tique a démarré en octobre 2014. Quatre ans plus tard, la recherche et le développement des technologies quantiques étaient érigées en priorité nationale par le "National Quantum Initiative Act"(NQIA) [50] avec un premier investissement de 1,2 milliard de dollars. D'autres tout aussi massifs sont issus des secteurs privés et des Big Tech (Google, IBM, Microsoft) qui désirent ardemment participer à la suprématie Américaine dans le domaine du quantique.

La Chine a mis un pied dans la course au quantique lors de son 13ème Plan quin- quennal (2016-20), en prenant rapidement l'avantage face aux États-Unis dans les télécommunications quantiques et en rattrapant son retard dans le calcul quantique. Le pays lançait ainsi, en 2016, le programme "Quantum Experiments at Space Scale" ou "Micius", pour y mener de multiples expériences de communication quantique entre l'espace et le sol [51] . En 2017, le gouvernement chinois annonçait la construc- tion d'un laboratoire national pour les sciences de l'information quantique de 10 milliards de dollars, dans le cadre d'une grande poussée dans ce domaine [52]. Un investissement payant puisqu'en décembre 2020, le principal groupe de recherche quantique chinois annonçait avoir créé le premier prototype d'ordinateur quantique, appelé "Jiuzhang", pouvant traiter en 200 secondes, ce qu'un supercalculateur classique traite en 600 millions d'années [53].

On le constate, la guerre du quantique est ouverte et tous les coups sont permis. Ainsi, après la bataille des smartphones, celle de la 5G, les États-Unis ont décidé de s'attaquer aux technologies quantiques "made in China". Les États-Unis ont ajouté en 2021 huit sociétés chinoises spécialisées dans les technologies quantiques sur leur liste noire. Ils affirment que ces entreprises posaient un danger pour la "sécurité nationale" américaine, car ce domaine de la science et de l'ingénierie est devenu un enjeu majeur.

Les enjeux se devinent, il faut être précurseur dans tous les secteurs de l'informa- tique quantique. Les stratégies d'investissements et de coopérations se dessinent. Elles font naître des alliances mettant en exergue des enjeux géopolitiques. Les opportunités scientifiques et commerciales de l'informatique quantique sont bien réelles mais quand est-il des menaces ?

LES MENACES SONT-ELLES REELLES ?

Existe-t-il vraiment une menace ? l'informatique quantique viendra-t-elle a bout de nos systèmes de sécurisation actuels ?

La communauté internationale semble se déchirer sur le sujet et les avis divergent. Le NIST, la NSA ou encore l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) prennent au sérieux la problématique de cybersécurité engendrée par l'arrivée des ordinateurs quantiques. L'ANSSI vient de réaffirmer cette position le 4 janvier dernier dans sa publication sur la transition vers la cryptographie post quantique [54].

A l'opposé, certains cryptographes ne partagent pas cet avis et doutent officiellement des progrès dans le calcul quantique. Lors de la convention RSA en 2017, Whitfield Diffie, cryptographe et expert en sécurité chez Cryptomathic, suggère que cela ne vaudrait pas la peine de s'inquiéter car *"nous serons tous morts d'ici là"*[55].En réalité, les clés de cryptographie sont déjà « relativement » faibles. Adi Shamir, cryptographe et co-

inventeur de RSA, déclarait lors de cette même convention qu'il y avait *"plus de chances que le crypto-système RSA soit brisé par des tentatives classiques"*[55].

Selon Daniel Estève, directeur du groupe de recherche Quantronics au Commissariat à l'Etude Atomique (CEA) et membre de l'Académie des Sciences Française : *" Les acteurs du secteur ont tendance à faire de la communication sans grand fond "*[56].

Devant ces débats d'experts, tour à tour rassurants ou alarmistes, la presse elle-même ne sait sur quel pied danser. On voit se multiplier des articles sérieux cherchant à informer mais aussi des articles qui cherchent à faire le buzz, avec des titres comme *"Pourquoi l'informatique quantique n'est pas une menace pour la sécurité » [*57] du journal Belge, Le Soir, ou *"Cybersécurité : qu'est-ce l'apocalypse quantique et devons- nous avoir peur ?"*[58], de la British Broadcasting Corporation (BBC). Qui croire ?
Pourtant, en s'intéressant de plus près aux articles scientifiques plus qu'aux "experts" des différentes rédactions journalistiques, la menace semble bien réelle et se porte essentiellement sur nos méthodes cryptographiques et leurs applications à la sécurisation des données.

Claus Peter Schnorr, mathématicien et cryptographe à l'université de Francfort, dans son article « Fast factoring Integers by SVA Algorithms » déclare que *" le crypto système Rivest-Shamir-Adleman (RSA) est mort (2021)."*[59]. En effet, l'algorithme de Shor peut être utilisé pour casser le cryptosystème RSA, l'échange de clef Diffie-Hellman ou la cryptographie à courbe elliptique [60].

Chercher à sauver RSA est une course perdue d'avance.
Certains considère que *"les algorithmes à clef publique reposant sur la factorisation [. . . ou] sur la difficulté du calcul d'un logarithme discret peuvent être considérés cassés par un attaquant quantique"*[61].

De facto, toutes nos protections algorithmiques classiques, nos secrets seraient à nus, obsolètes, notre confiance en nos écosystèmes aussi bien financiers qu'étatiques se retrouverait anéantis. Un risque systémique majeur pourrait en découler et impacterait également notre souveraineté : Nous serions face à l'apocalypse quantique.

Les communications sécurisées, les systèmes sécurisés de paiements, les transactions financières, les cryptomonnaies, reposent tous sur les protocoles de chiffrement asymétriques. La sécurité de ces protocoles dépend principalement du fait qu'il faudrait plusieurs milliers d'années à des ordinateurs classiques pour casser un code. Or, ce déchiffrement est théoriquement réalisable et en très peu de temps pour un ordinateur quantique. D'où la menace réelle pour les systèmes de chiffrement actuels.

En conséquence, le danger porte sur :

- Le secret des cartes bancaires et des transactions bancaires.
- L'authentification lors de l'établissement d'une connexion Secure Socket Layer (SSL)/ Transport Layer (TLS), et donc la plupart des transactions commerciales sur internet.
- L'authenticité des signatures électroniques de documents.
- La confidentialité de PGP, S/MIME et tous les protocoles d'enveloppe digitale à chiffrement asymétrique, et donc de l'échange de documents.

De surcroît, l'algorithme de Grover peut être utilisé pour retrouver les clefs symétriques AES [12], inverser le hash d'un mot de passe, et plus généralement, pour inverser SHA256 si l'espace des mots initiaux est trop petit, comme dans le minage de bitcoin.

Ce qui ajoute au danger actuel :

- Les cryptomonnaies (bitcoin, ether…).
- Les mots de passe.
- Le chiffrement DVB-CSA [13] utilisé par les systèmes de télévision numérique.
- Le chiffrement MPEG-CENC [14] utilisé par la plupart des DRMs audio et vidéo.
- Etc.

Si la menace n'est pas immédiate, car avoir accès à un ordinateur quantique a un coût encore élevé, la crainte du "récolter maintenant, déchiffrer plus tard" est bien réelle et actuelle. Le risque porte donc sur les transactions actuelles, mais aussi sur les transactions et documents passés, en particulier sur les communications, les cer- tificats, licences, mails etc.

Toute industrie qui utilise largement la cryptographie (commerce, bancaire, trans- port, pharmaceutique. . .) est susceptible de s'écrouler en cas d'attaque massive. Il ne faut pas non plus sous-estimer le risque qu'une attaque ne soit pas violente et visible, mais cachée et pernicieuse, à la façon des "Advanced Persistent Threats".
La génération de quelques transactions bancaires pourrait être rémunératrice, la dé- stabilisation lente d'un état est une opportunité, voir à ce sujet les attaques contre l'Ukraine en janvier 2022[62].
A ce jour, nombreux Etats ont accès à ces ordinateurs quantiques.

Le rapport de l'académie des sciences américaine de 2019[63] indique page 97 que, pour casser une clef RSA 2048, il faudrait disposer d'un calculateur qui a autour de 2300 qubits logiques. Pour obtenir un Qubit logique avec correction d'erreur, il faut au minimum cinq qubits physiques, "The Perfect Magic 5"[64] selon Nathan Babcock, chercheur à L'Institute for Quantum Science and Technology (IQST) qui se base sur l'article "Quantum Circuits for Stabilizer Codes"[65]. De fait, les clés RSA 2048 pourraient être obsolètes en 2025 compte-tenu de l'évolution des perfor- mances des ordinateurs quantiques, notamment la gamme proposée par D-Wave [66].

C'est en effet l'horizon de menace annoncé les experts les plus pessimistes (NIST, Michele Mosca 15. . .) qui tablent à horizon 2025 alors que les plus optimistes (Gart- ner, Boston Consulting Group, Commission Européenne [69]) voient une fenêtre à 2035-2040. Devant l'urgence, il est souhaitable d'agir. Eleni Diamanti, chercheuse au CNRS et membre du Paris Center for Quantum Computing déclarait que : "La communauté mathématique prend très au sérieux la menace de l'ordinateur quantique" [56].
Devant la menace sécuritaire, les nations se positionnent, entraînant avec elles, les entreprises et les startups. Une réponse globale se met en place.

12. AES : Advanced Encryption Standard.
13. DVB-CSA : Digital Video Broadcasting-Common Scrambling Algorithm.
14. MPEG-CENC : Moving Picture Experts Group - Common Encryption.

DEVANT LA MENACE QUANTIQUE, LA REPONSE EST MONDIALE

Aujourd'hui, les calculateurs quantiques sont principalement des outils de laboratoire, disponibles uniquement pour une toute petite communauté d'experts au sein d'entreprises privées ou de laboratoires académiques prestigieux.

Pourtant les leaders commerciaux ont une stratégie de prise de position qui les conduit à diffuser et/ou louer leur technologie au-delà de leur propre entreprise.

La problématique actuelle est que l'implémentation de calculateurs quantiques ré- clame des ressources financières très conséquentes en particulier parce que, par définition, les calculateurs actuels sont classiques, et ne peuvent donc pas simuler correctement les composants quantiques. Ils réclament aussi des ressources technologiques en conception et fabrication de composants électroniques hautement intégrés. Il n'est donc pas étonnant de voir dans la liste des acteurs sur ce domaine, plusieurs des GAFAM et entreprises de renommée mondiale, largement financés par les États.

Plus généralement, les démarches de ces différents acteurs privés sont similaires :

- Cofinancer la collaboration entre la recherche universitaire et leurs propres laboratoires de recherche, et beaucoup publier.
- Poser des brevets pour bloquer le marché.
- Mettre au point des calculateurs quantiques réels, qui peuvent être mis à disposition à travers le Cloud.
- Définir un langage de programmation, qui peut servir à la simulation sur ordinateur classique ou à la programmation de leurs calculateurs quantiques.
- Chercher des applications réalistes avec des partenaires industriels prestigieux qui sont dans des domaines d'application où le calculateur quantique peut beaucoup apporter.

Le site Sifted [70] dresse un panorama des investissements en calculateur quantique, et en particulier sur la frénésie de brevets, destinée à protéger ces investissements, et éventuellement rapporter des royalties. On commence à voir une hausse notable (de 7% à 19%) des entreprises qui consacrent plus de 17% de leur budget IT aux technologies de calcul quantique [71].

Comme nous l'avions vu au début de ce chapitre, le marché de l'informatique est déjà là (pour rappel : 830 millions de dollars pour 2024). C'est ce que confirme aussi le cabinet McKinsey, dans un rapport publié en 2020. Il voit la décennie à venir comme celle de l'avènement de cette technologie, qui générera d'après lui 1000 mil- liards de dollars d'ici 2035 [72] ! ! !

Rien d'étonnant donc, à ce que les entreprises, des mastodontes (1ère partie) au startups (2ème partie) se placent sur ce marché. Les financements des États (3ème partie) y contribuant fortement, créant ainsi des opportunités pour faire avancer la science et développer de nouvelles technologies.

15. Michele Mosca est le co-fondateur et directeur adjoint de l'Institute for Quantum Computing de l'université de Waterloo (Canada) auteur du théorème de l'inégalité [67] et d'un article sur la préparation de la cybersécurité face à l'ordinateur quantique [68]

LES ACTEURS PRIVES MAJEURS

- **Google**

  Google est fortement impliqué dans le développement des ordinateurs quantiques, d'ailleurs depuis 2014 il s'est lancé dans la fabrication de son propre ordinateur quantique. Hébergé par la NASA, son laboratoire, le Quantum AI Lab met l'accent sur le développement matériel mais aussi logiciels via des applications liées à l'intelligence artificielle. Les solutions matérielles sont décrites dans le document : Google Quantum AI Hardware [73] via le développement en interne de SOC (System On Chip) avec le dernier en date, le Sycamore (2018) et du calculateur quantique Weber (2021) disponible sous forme d'Infrastructure As A Service (IAAS). Sa solution logicielle vise à être indépendante des solutions matérielles. Elle est basée sur le langage Cirq [74], Open Source, et propose un environnement de développement très complet, dont de nombreuses librairies. A ce jour, Google aurait atteint la suprématie quantique [75], point où l'ordinateur quantique va au-delà des capacités de l'ordinateur classique.

- **Microsoft**

  Microsoft s'est lancé très tôt dans le développement d'une solution quantique en finançant, dès 2005, les recherches de l'université de Californie - Santa Barbara. Puis en 2017, Microsoft a lancé son langage de programmation, le Q# accompagné d'une documentation importante. Axé sur le logiciel et le Cloud, via "Azure Quantum Open Cloud", le matériel ne semble pas être une priorité pour Microsoft. Microsoft informe la communauté sur ses avancées via sa newsletter : Azure Quantum Newsletter [76].

- **Amazon**

  L'offre publique d'Amazon est portée par AWS, une plateforme disponible dans le Cloud. L'accent est mis sur la disponibilité du service, sa tarification à l'usage, et la disponibilité. Amazon met à disposition des plateformes matérielles qui permettent d'expérimenter 3 types de calculateurs quantiques, basés sur des pièges à ions de IonQ, des super-conducteurs de chez Rigetti et des dispositifs de recuit en provenance de D-wave.

- **IBM**

  Conscient des difficultés du domaine, IBM fait d'abord la promotion des ap- plications avec des grands partenaires (Mercedes, Exxon Mobil, CERN), et collabore étroitement avec les gouvernements Européens [77]. IBM, très actif dans les travaux de recherche fondamentale, se consacre à la vulgarisation de l'informatique quantique [78], il décline sa gamme de solutions pour trois cibles : le business, les chercheurs, les programmeurs. IBM a annoncé le 16 Novembre 2021 une puce "Eagle", à Cent vingt-sept qubits [79], et prévoit une puce à mille qubits pour fin 2023 [80] !

  Le calculateur d'IBM qui comporte des processeurs quantiques est appelé "Quantum System One" [81]. Son coeur de calcul quantique est pour l'ins- tant basé sur la puce Falcon, et il pourra être upgradé avec Eagle qui vient d'être annoncé. Ce calculateur est disponible en version commerciale pour les entreprises depuis octobre 2019.

La programmation se fait avec l'outil Qiskit [82] (Qiskit, 2022), qui est un SDK open-source. Le blog d'IBM [83] permet de suivre les avancées de cet acteur majeur.

- **Alibaba**

  Alibaba, via la création de son Laboratoire en 2015 (Alibaba Quantum Computing Laboratory), a choisi d'investir dans sa propre technologie de calculateurs quantiques. En 2018, Alibaba lançait un processeur quantique de onze qubits, et un simulateur permettant d'expérimenter virtuellement un cœur à soixante-quatre qubits.

  La cryptographie en général, la génération de clefs quantiques dans le Cloud [84], l'adaptation des protocoles en fonction des niveaux de sécurité requis sont les enjeux majeurs des investissements d'Alibaba, l'objectif étant de maîtriser la sécurité des transactions financières, en particulier pour Alipay. A la différence de ses concurrents américains, Alibaba communique peu.

- **Baidu**

  Baidu se concentre sur les couches applicatives et l'utilisation de technologies externes, il met à disposition depuis 2018 et la création de son laboratoire une Plateforme As A Service (PAAS), Quantum Leaf. Tout comme Alibaba, il semble bien intégré avec les laboratoires de recherche publics Chinois.

Souvent cités,

- **D-Wave**

  D-Wave est une société canadienne souvent présentée comme pionnière dans le calcul quantique, qui vend ou loue des calculateurs quantiques. Son éco- système logiciel est particulièrement développé.

- **Rigetti Computing**

  Rigetti Computing est une société californienne qui vise à réaliser un calculateur quantique entier. De nos jours, ils mettent à disposition dans le Cloud une plateforme permettant de développer des algorithmes utilisant trente-six qubits.

- **Atos**

  Côté Français, Atos, est l'acteur français de pointe sur le développement de l'informatique quantique. Nous aborderons plus en détails cet acteur majeur dans le Chapitre suivant sur la réponse française.

LES FONDS D'INVESTISSEMENT ET LES STARTUPS

Bien que de nombreuses sociétés de capital-risque aient réalisés des investissement dans les startups quantiques, le nombre de fonds d'investissement spécialisés (Figure 9) dans ce domaine est en revanche très faible, seulement six dans le monde.

Figure 9 – Les fonds d'Investissement en Quantique

La technologie quantique est regardée comme un investissement risqué en raison de la complexité de la technologie et du manque de visibilité sur les retours sur investissement. Les investissements actuels sont réalisés en majorité par des fonds spécialisés en deeptech.

Dans le monde, des programmes d'incubation et d'accélération pour les startups quantiques ont vu rapidement le jour. Les principaux sont situés au Canada (Crea- tive Destruction Lab), au Royaume-Uni (Unit DX), aux Etats-Unis (Duality, par- rainé par Amazon, et Quantum Startup Foundry) et en France (HEC Challenge+ et Deeptech Founder). Le nombre d'opérations d'investissement et les montants totaux ont connu une forte croissance ces dernières années. En 2012, trois startups avaient réalisé une levée de fonds, pour un montant total de 34 millions de dollars. En 2018, vingt-quatre startups ont levé 128 millions de dollars.

Le programme Deeptech Founder accéléré une grande partie des startups quantiques françaises comme Quandela, Pasqal et Alice&Bob. La figure ci-dessous nous présente un panorama des startups. Le fond français, Quantonation (dirigé par BpiFrance), 100% spécialisé quantique y a contribué aussi. Nous regardons en détail cet écosystème français dans le prochain chapitre.

La figure suivante (Figure 10) nous montre les différentes startups quantiques liés spécifiquement à la cybersécurité.

Tour d'horizon des structures innovantes à l'intersection de l'informatique quantique et de la cybersécurité :

- **l'ordinateur quantique** pour briser les chiffrements (calcul quantique),
- **la cryptographie quantique** pour sécuriser les communications (distribution de clés quantique et le générateur de nombres aléatoires quantique),
- **la protection contre la menace quantique** (cryptographie post-quantique).

Figure 10 – Radar des startups Quantique & Cybersécurité innovantes [85]

Dans le monde des startups, deux modèles s'affrontent. Le modèle américain, décentralisé basé sur l'initiative individuelle et l'investissement privé et le modèle chinois, centralisé, basé sur l'interventionnisme étatique et l'investissement public massif. Les États-Unis et le Canada totalise soixante-quatorze startups, la Chine une dizaine. L'écosystème en Europe compte environ quatre-vingt-dix startups. Avec vingt startups, le Royaume-Uni se classe en 1ère position, suivi de la France avec seize et l'Allemagne avec quatorze.

En 2022, louer un calculateur quantique n'est plus un problème. Treize sociétés offrent ce service sur le Cloud [86]. Le Monde des startups, associés au géants et universités est en pleine effervescence. De surcroît, les États investissent aussi et soutiennent cet écosystème à coût de milliards de dollars.

LES ÉTATS

L'ordinateur quantique avec tous ses dangers, est devenu un enjeu stratégique de souveraineté et de sécurité. Dans cette course mondiale, il y a clairement une domination des Etats-Unis et de la Chine qui se disputent la première place. Comme nous l'avons vu précédemment, ces deux pays peuvent compter sur des mastodontes de la haute technologie (Google, IBM, BTAX [16], Huawei, ZTE...).

A l'heure actuelle, plus d'une dizaine de pays ont adopté des stratégies nationales de recherche et développement, avec des plans nationaux ambitieux (Figure 11) dont les financements qui pour certains se comptent en dizaines de milliards de dollars et ce depuis 2007.

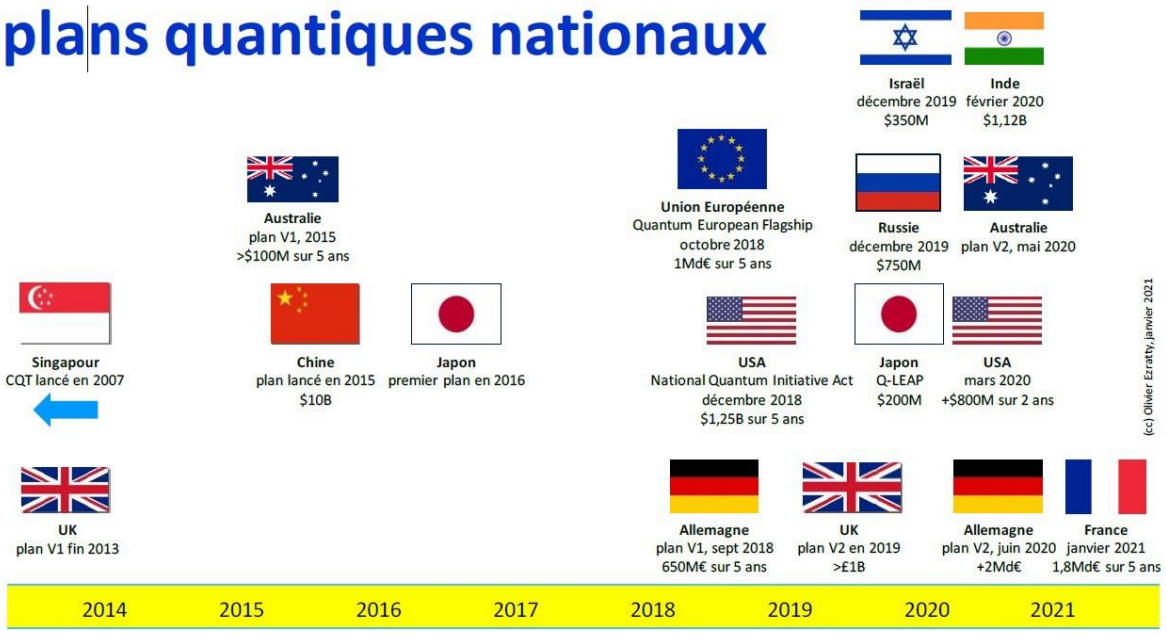

Figure 11 – Plans Quantiques Nationaux [87]

Sur la scène internationale, l'informatique quantique est l'objet d'une véritable course à l'innovation. Avec cette manne financière, la course aux brevets est lancée. La Chine et les États-Unis sont les deux pays qui investissement le plus dans le quantique [88]. La Chine est devenue le leader mondial en termes de brevets (5 161 soit plus de la moitié des 52,1% de brevets mondiaux), devant les USA (2 401, 24,2%) et le Japon (768, 7,8%). Le Royaume-Uni (394, 3,9%) et la Corée du Sud
(379, 3,8%) complètent le TOP5 (Figure 12).

16. BATX : Baidu, Alibaba, Tencent and Xiaomi

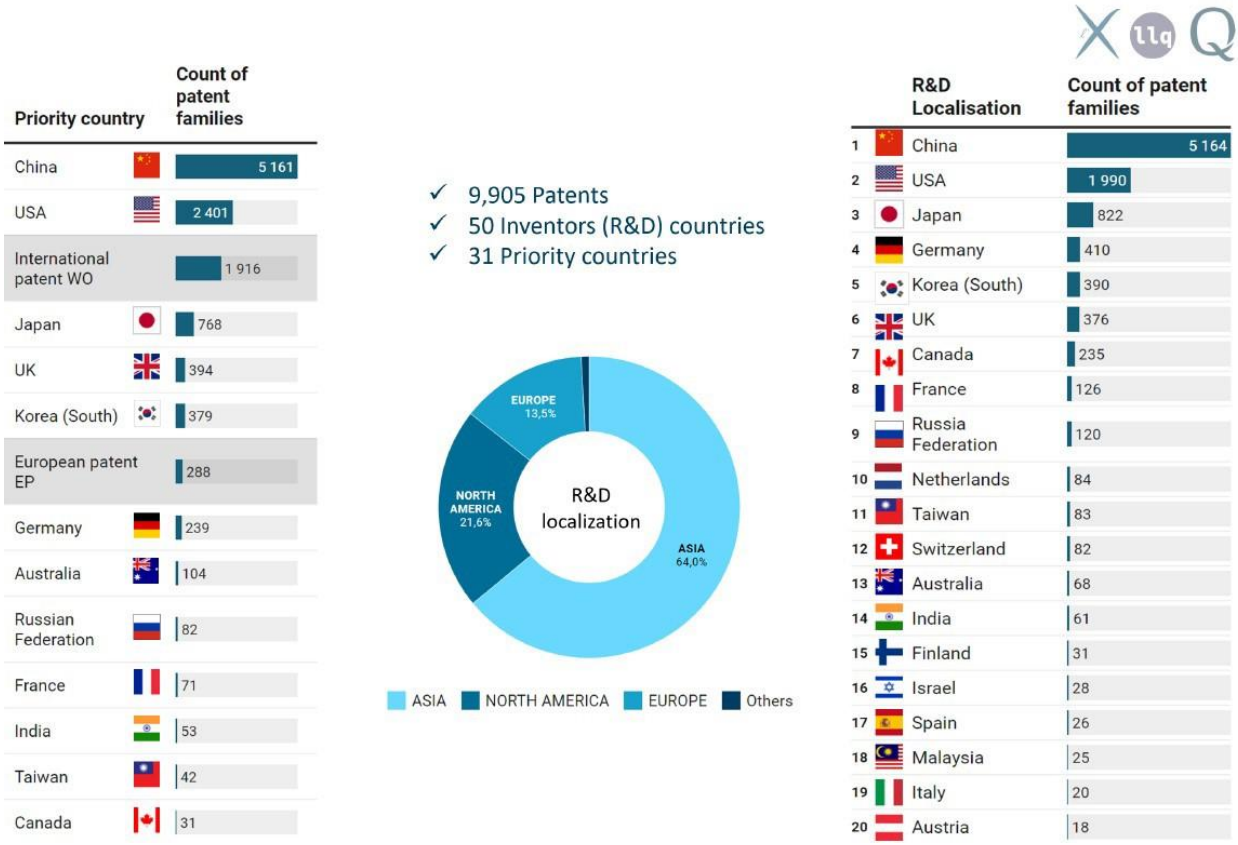

Figure 12 – Brevets déposés dans le domaine du quantique [89]

Panorama des investissements par pays

- **La Chine**

Dès 2006, La Chine a investi plus de 2 milliards de dollars, puis en 2017, elle a lancé la construction du National Laboratory for Quantum Innovation avec un budget estimé à 10 milliards de dollars. Ce dernier a vu le jour en 2019, sous la direction de Pan Jianwei [90], considéré comme le *"père du Quantique"* par le magazine Nature et nommé comme l'une des personnes scientifiques les plus influentes en 2017 [91].

La Chine est le leader incontesté dans le domaine des communications quantiques. Avec le lancement du premier satellite disposant de technologies quantiques, suivi d'un premier test réussi (communication par liaison quantique entre le satellite et une base au sol distants de 1200 kms) [92]. Il s'agit du premier satellite au monde à l'épreuve du piratage.

La Chine continue depuis à développer des technologies sécurisées de communication quantique sécurisées. Ce développement est soutenu au plus haut de l'État chinois. Lors de la 24ème étude sur les perspectives de recherche et d'application de la science et de la technologie quantique le 16 Octobre 2020, Xi Jinping, secrétaire général du Comité central du Parti Communiste Chinois, insistait sur le fait qu'*"Il est nécessaire de bien comprendre l'importance et l'urgence de promouvoir le développement des technologies quantiques, et de renforcer sa planification stratégique"* [93].

En 2021, des chercheurs de l'Université de sciences et technologie de Chine assuraient que leur ordinateur quantique, nommé Zuchongzhi 2, est bien plus puissant que celui de Google : preuves à l'appui, avec une publication dans le journal de la société américaine de physique [94].

- **Les États-Unis**

L'administration américaine a mis en place le National Quantum Initiative Act (NQIA) fin 2018 pour un montant d'1,25 milliards de dollars. Ce pro- gramme gouvernemental vise à encourager la recherche et le développement, ainsi que l'éducation en matière de technologie quantique. En 2021, parmi les financements listés dans le budget de la Maison Blanche pour le quantique (600 millions de dollars), on trouve une ligne à 25 millions de dollars consacrée à la création d'un Internet quantique national. Les États-Unis veulent rattraper et reprendre un longueur d'avance dans le domaine de la communication quantique et de la cybersécurité. Michael Kratsios, US Chief Technology Officer, a souligné que le pays devait être *"gagnant et leader"* non seulement dans la technologie actuelle, mais aussi dans ce qui *"définirait notre avenir"* (dont le Quantique) [95].

- **L'Union Européenne**

L'Union Européenne a quant à elle investi dès 1999, pour un montant de de 550 millions d'euro dans le programme Future Emerging Technologies (FET). A la suite du Quantum Manifesto signé en mai 2016 par de nombreux acteurs académiques mais aussi industriels, elle a accentué sa volonté d'investir dans la technologie quantique. Le "Quantum Flagship", lancé en 2018, est un projet de la commission

européenne sur dix ans et doté d'1 milliard d'euros. A sa création, il a soutenu une vingtaine de projets pour un montant de 135 Millions d'euros.

- **Le Royaume-Uni**

  Le Royaume Uni est le premier pays européen à avoir lancer son programme national quantique en 2013 pour un montant de 370 millions d'euros sur cinq ans, puis il a réinjecté plus de 1 milliard d'euros en 2018. Ce qui explique au- jourd'hui les nombreux programmes universitaires et le relatif grand nombre de startup du pays.

- **La France**

  Fin 2019, le rapport de la mission parlementaire dirigé par la députée Paula Forteza (Rapport Forteza [96]) a été livré. La France, très en retard dans le domaine, a annoncé en janvier 2021 un plan sur le quantique avec un budget de 1,8 milliards sur cinq ans [97]. Nous y reviendrons plus en détail dans le 3ème chapitre sur la réponse française.

- **L'Inde**

  L'Inde est un acteur récent dans le domaine du quantique, il a lancé en 2020 un plan sur cinq ans doté de 1,12 milliards de dollars, principalement dans l'informatique, la communication et la cryptographie quantique.

- **Israël**

  Israël a créé un fond en 2018 pour soutenir sa recherche universitaire dans le quantique. Fin 2019, Israël a lancé un plan plus ambitieux portant sur les domaines de la communication quantique, des capteurs quantiques pour l'industrie et la défense, et du Cloud pour soutenir les besoins en calcul.

- **Le Japon**

  Le Japon a lancé l'initiative Q-LEAP en 2016, renforcé par le plan MEXT Q-LEAP [98] en 2018 sur une période de dix ans, qui investit principalement dans les domaines de la simulation quantique et de l'informatique quantique. L'objectif est de construire un ordinateur de cent qubits à dix ans.

- **La Russie**

  La Russie a créé en 2012 le Russian Quantum Center, dédié à la recherche sur les ordinateurs, les communications et les capteurs quantiques. En 2019, la Russie a annoncé un plan quinquennal sur les technologies quantiques de 750 millions de dollars.

- **Singapore**

  Précurseur dans le domaine, la recherche quantique est centralisée au Centre des Technologies Quantiques (CQT) de l'Université nationale de Singapour (NUS) depuis 2017, avec un financement de 15 millions de dollars annuel. La recherche singapourienne est spécialisée sur les ordinateurs et la cryptographie quantique.

En conclusion, vu le montant des investissements, les attaques à base d'ordinateurs quantiques ne semblent pas actuellement à la portée des organisations cybercriminelles. Pourtant si une telle organisation pouvait acquérir cette puissance de calcul, vos informations personnelles, médicales, bancaires, etc. lui seraient accessibles. Elle aurait aussi accès à des échanges d'information d'ordre militaire ou liés à la sécurité d'un État. L'écosystème mondial se mobilise, des milliards de dollars ont été investis pour protéger les données, surtout celles des États.

Nous avons pu voir que le quantique nous emmène dans un nouveau paradigme dans lequel la cryptographie telle qu'on la connaît sera mis à mal. Mais alors qu'en est-il alors pour les systèmes les plus reconnus, à tort ou à raison, en matière de sécurité et d'immuabilité ?

ATTAQUES SUR LES BLOCKCHAINS

ETAT DES LIEUX

Nous avons vu précédemment l'état de l'art en matière de technologies quantiques ainsi que les principaux principes cryptographiques. Notre postulat de base étant que l'arrivée du quantique pourrait remettre en question les notions de sécurité nous nous sommes naturellement interrogés sur le comportement sur les Blockchains. En effet, les Blockchains ont la réputation, à tort ou à raison, d'être infaillibles. Dans cette partie nous ne traiterons pas des enjeux idéologiques et politiques de la Blockchain mais de l'aspect purement technologique et cryptographique.

Afin de faciliter la lecture de cette partie nous conviendrons que lorsque le terme "Bitcoin" arbore une majuscule nous parlons de la Blockchain. Lorsque la majuscule est absente on parle de son token, en l'occurrence, de la cryptomonnaie bitcoin.

Les Blockchains ne sont pas exemptes d'attaques, on recense quelques centaines d'attaques entre 2017 et 2021.

Type of Attack	Major Attacks	Total
Exchange Exit	14	$ 4.383 billion
Exchange Hack	43	$ 1.702 billion
DeFi Hack	49	$ 1.122 billion
DeFi RugPull	7	$ 124 million
51% Attack	14	$ 24 million in double-spendings

Table 1 – Ransomware Attacks 2017-2021

Le montant des attaques sur le monde des Blockchains (chaines, cryptos, exchanges, investissement, etc.) représente sur la période 2017-2021 environ 7 milliards de dollars. Ce montant est anecdotique si on le rapporte à la capitalisation totale du marché de 3000 milliards de dollars en 2021 [99]. Ce qui nous intéresse dans le cadre de notre mémoire est la partie technologique et on se rend compte que finalement seules les "attaques 51%" et DeFi Hack sont imputables à la technologie Blockchain. En effet, les autres typologies d'attaques ciblent et/ou utilisent des failles existantes dans le monde non-Blockchain telles que les "exchanges exit", "rug pull" et autres qui sont davantage considérées comme des fraudes et arnaques aux investisseurs et clients. Si on analyse l'aspect financier, le montant connu impacté par des "attaques 51%" est de l'ordre de 24 millions de dollars et celui des Defi Hack est valorisé à 1,2 milliards de dollars (dont une attaque de plus 600 millions de dollars). Sur ce der- nier montant il nous est impossible de cibler les montants sur les attaques réalisées sur des failles purement liées à la technologie Blockchain mais nous supposons que cela en représente une grande partie. Finalement, ce montant est-il comparable aux chiffres du secteur bancaire traditionnel ? Selon l'étude [100] menée par le think tank "Club des Juristes" et présidé par Bernard Cazeneuve, "Nombre de rapports inter- nationaux mesurent les coûts directs et indirects des attaques numériques. Ainsi,

en 2017, le coût global a été de 600 milliards de dollars". Nous sommes donc bien loin des niveaux affichés sur les technologies Blockchain sur un espace de cinq ans. Mais ces montants sont-ils la seule justification en matière de cyberrésilience ? Évidemment ce n'est pas le cas. Le secteur est tout d'abord bien plus large sur tous les plans (capitalisations, ressources humaines, adaptation, etc.) mais également plus facilement attaquable. Les hackers en vrais ROIste vont donc chercher à rentabiliser leurs frais et ainsi attaquer ce qui est le plus simple. Nous parlons bien évidemment d'une typologie d'hacker recherchant le gain financier uniquement. Ces attaquants se mettront sur le champs Blockchain dès lors que le marché s'y prêtera.

TYPOLOGIES D'ATTAQUES

Il y a dix principales typologies d'attaques visant les cryptomonnaies :

- "Exchange Hack".
- "DeFi Hack".
- "51% Attack".
- "Phishing".
- "Rug pull/Exit scam".
- "Ransomware".
- "SIM swap".
- "Investment swap".
- "High Profile Doubler Scam".
- "Extortion".

Comme vu précédemment nous ne traiterons que les "Attaques 51%" et les "DeFi hack" car ce sont les deux seules typologies d'attaques qui exploitent des failles dans les technologies Blockchains. Vous pourrez retrouver l'ensemble des définitions dans ce document du Cloud Security Alliance [101].

Une "attaque 51%" est une attaque visant les Blockchains à preuve de travail ou Proof of Work (PoW) en anglais, où des mineurs se coordonnent dans l'objectif de contrôler plus de 50% du hachage minier du réseau. Leurs buts sont alors d'utiliser cette majorité de contrôle pour empêcher la confirmation de nouvelles transactions ou d'annuler des transactions qui ont été effectuées sous leur contrôle, ce qui conduit à une attaque de "double dépense". Concrètement, après une "attaque 51" il n'y a souvent rien d'écrit dans la technologie de la Blockchain qui puisse arrêter l'attaque. L'impact financier sur ce type d'attaque vient finalement par ricochet puisque cela génère une baisse de confiance dans la technologie de la Blockchain attaquée et de fait les investisseurs la déserte. Ce n'est donc pas l'attaque en elle-même qui cause un préjudice financier majeur.

Ce type d'attaque existe mais ne touche que des Blockchains relativement confidentielles. En effet, si on souhaite effectuer ce type d'attaque sur la Blockchain Bitcoin il faudrait contrôler près de 7500 nœuds de confirmations [102]. Selon la même source, Bitcoin aujourd'hui c'est environ 15000 nœuds répartis dans le monde entier, dont 54% aux localisations inconnues. Le nombre de nœuds est donc un premier moyen de se prémunir de ce type d'attaque [17] mais est directement conditionné par le succès et l'engouement suscité par votre Blockchain. Techniquement il est également possible de s'en prémunir en exigeant une profondeur de bloc de confirmation plus importantes. Ceci permettant de

solliciter l'ensemble des nœuds de la chaîne pour valider un bloc. Coté utilisateur les transactions seront plus longues à être enregistrées mais seront plus sûres, car validées par un plus grand nombre de nœuds.

Les attaques de type DeFi [18] quant à elles exploitent le smart contract [19] ou les infrastructures portant ces smart contracts. On peut donc imputer ces attaques à la technologie et sa (mauvaise) mise en place par les développeurs Blockchain/Smart Contract. Par ailleurs, on peut noter que paradoxalement, attaquer une chaîne DeFi n'est absolument pas illégal [105]. Comme le précise l'auteure "les smart contracts n'ont pas d'autorité juridique à eux seuls mais ne sont pas pour autant dépourvus d'assise juridique". Toutefois, l'assise juridique repose ici sur une notion de propriété individuelle, or les smart contracts sont dans la plupart "open source", personne n'en a donc la propriété. En outre, et selon Gernot Fritz et Lukas Treichl conseillers juridiques spécialisés Corporate and M&A, Data regulation and cyber, Intellectual property chez Freshfields Bruckhaus Deringer "Sur le plan juridique, les premières interprétations des contrats intelligents réduisaient le contrat intelligent au seul code, déclarant effectivement le code comme la loi elle-même : autonome, auto-exécuté et auto-appliqué. Toute erreur ou vulnérabilité accidentelle du code devrait être considérée comme faisant également partie du contrat. Cependant, l'application d'une approche à "deux couches" est plus raisonnable, car elle positionne le contrat intelligent dans le système juridique plus large : la couche technique, le code, est limitée à une section de la couche juridique, le contrat. Mais les deux couches doivent être co-ordonnées et combinées pour être efficaces et juridiquement contraignantes ..." [106]. -

17. Toute Blockchain PoW n'a pas nécessairement ce fonctionnement de contrôle par la majorité des noeuds. La Blockchain Cardano, par exemple, effectue ce contrôle sur la capitalisation totale du marché.

18. "L'objectif de la finance décentralisée est de permettre la transmission de valeur et la création d'une finance pour tous et sans intermédiaire comme peuvent l'être les banques ou les plateformes d'échange. La DeFi permet à n'importe qui d'obtenir des prêts. C'est un système totalement décentralisés pour les emprunteurs et il n'est pas possible qu'un prêt vous soit refusé. Il vous suffit d'avoir un accès à internet. Cela permet également aux prêteurs de faire travailler leur argent avec des taux d'intérêts décents !" [103]

19. "Les smart contracts, ou contrats intelligents, sont des programmes informatiques irrévo- cables, le plus souvent déployés sur une Blockchain, qui exécutent un ensemble d'instructions pré-définies" [104]

Étude de cas décrit par le Cloud Security Alliance dans son étude sur les dix principales typologies d'attaques sur les Blockchains [101] :

> Le 10 août, Poly Network a subi un piratage de 612 millions de dollars, le plus important piratage lié aux crypto-monnaies à ce jour. Le piratage typique de DeFi vise des instruments DeFi spécifiques, ce qui entraîne des pertes beau- coup plus faibles. Cette attaque visait l'infrastructure de Poly Network, en se concentrant sur la plateforme DeFi elle-même et en ciblant le contrôle des contrats intelligents de l'échange décentralisé (DEX). En conséquence, le principal contrat inter-chaînes a été entièrement contrôlé par le pirate, ce qui lui a permis de déverrouiller les jetons qui étaient censés être bloqués dans le contrat, de les envoyer à des adresses sous son contrôle, puis de répéter l'attaque sur plusieurs chaînes. Le pirate a restitué la quasi-totalité des fonds dans les jours qui ont suivi le piratage initial. Cependant, au moment de la rédaction de ce rapport, une grande partie des fonds restitués - environ 235 millions de dollars - se trouve toujours dans un portefeuille multisig sous le contrôle de Poly Network et du pirate. Cela signifie que Poly Network ne peut pas sortir les fonds de ce portefeuille sans les clés privées du pirate. Le pirate a jusqu'à présent refusé de divulguer sa clé privée.Ce piratage record illustre l'importance de la sécurité des contrats intelligents et des normes d'audit pour assurer la qualité et réduire les vulnérabilités du code. Comme les pi- ratages et les fraudes de DeFi continuent de croître de manière exponentielle trimestre après trimestre, l'avenir de la criminalité de DeFi semble sombre. Si les crimes de DeFi continuent à devenir plus sophistiqués, les contrats intel- ligents seront probablement de plus en plus la cible d'attaques à plus grande échelle.

A titre informatif, voici quelques attaques connues de 51% :

- Krypton.
- Shift.
- MonaCoin.
- Bitcoin gold.
- Zencash.
- Litecoin Cash.
- Feathercoin.
- Vertcoin.
- Ethereum Classic.
- Verge.
- Bitcoin SV.

Ce que nous révèle ces attaques visant l'écosystème Blockchain c'est que seulement 17% d'entre elles sont imputables à la technologie elle-même et ses surfaces d'attaques potentielles. La majeure partie des attaques sont des typologies d'attaques connues et qui ne sont pas dues au fait de la technologie Blockchain ou de son iplémentation. Par ailleurs, ces attaques ciblent dans la plupart des cas l'élément le plus faillible : l'Homme.

IMPACTS SUR LES BLOCKCHAINS

Comme vu précédemment, on peut affirmer que l'informatique quantique aura la puissance suffisante lui permettant d'attaquer les Blockchains, mais concrètement qu'est-ce que cela veut dire ?

Ce qui pose interrogation en matière de sécurité porte sur les éléments suivants :

- Random Number Generation.
- Hashage.
- Signatures et clés pubiques.

De manière générale, les principes cryptographiques reposent sur la génération aléatoire de nombre (série de chiffres). Dans les faits, l'informatique actuel est "dé- terministe" c'est-à-dire que lorsqu'on soumet un même argument (à une fonction déterministe) elle vous renverra constamment la même résultat. En d'autres termes, il est extrêmement compliqué voire impossible de créer réellement une série de chiffres de manière aléatoire. Cette problématique est d'autant plus intéressante dans le cas de la Blockchain puisque fondamentalement son principe repose sur l'attribution aléatoire de nombres. Le quantique quant à lui est indéterministe par nature, il est donc parfaitement adapté à ce contexte et permets ainsi la génération de nombre réellement aléatoire, cette opération est donc plus sûre grâce à cette technologie.

Le hashage quant à lui est le processus cryptographique qui donne vie à la Blockchain. Son principe est simple, cela permet de transformer une entrée de texte de taille variable en une sortie de longueur fixe. Ainsi la sortie est générée par une approche déterministe à partir de l'entrée. Dès lors, il est possible de recomposer le message en entrée à partie de la valeur de sortie. Certes cela est possible mais uniquement par "brute force" c'est-à-dire en testant unitairement toutes les entrées possibles pour retomber sur une sortie identique, ce qui permet alors de relier entrée et sortie.

Dans une Blockchain on utilise les fonctions de hashage pour garantir l'immuabilité des blocs et pour fournir la preuve de travail que doit compléter un nœud pour intégrer un nouveau bloc. Dans la majeure partie des Blockchains la fonction de hashage la plus répondue est le SHA256, qui génère donc une sortie de 256 bits. Concrètement, cela signifie que pour forcer (Brute Force) cette fonction il faudrait effectuer 2e256=1,16 10e77, opérations pour l'attaquer. Selon le CSA, aujourd'hui aucun ordinateur (même un super ordinateur) n'est en mesure de réaliser ces opé- rations.

La fonction de Hashage est également utilisée pour la validation de la création d'un nouveau bloc. Le principe est le suivant : lorsqu'un nouveau bloc doit être ajouté, ce qu'on appelle "les mineurs" sont en concurrence pour exécuter un calcul sur ce bloc. Le premier à réussir est autorisé à ajouter le bloc. Par ailleurs, la Blockchain va récompenser, généralement par un token [20], le mineur. Dans le cas de la Blockchain Bitcoin, le mineur victorieux reçoit des tokens bitcoins en guise de récompense. Finalement, c'est l'ordinateur ayant la plus grande puissance de calcul, donc plus rapide, qui gagne. Cependant, cette compétition n'est pas réellement terminée dès qu'un mineur est considéré comme victorieux. La Blockchain attend que plusieurs nœuds aient trouvés le même résultat. Dès lors que plus de 50% es nœuds ont trouvés le même résultat la Blockchain va considérer que ce résultat est le bon, c'est ce qu'on appelle "la profondeur de bloc". Ainsi, un ordinateur quantique avec une correcte utilisation de l'algorithme de Grover permettra un calcul beaucoup plus rapide mais

ne permettra pas d'altérer le nouveau bloc. Par extension, on pourrait considérer que si 51% des nœuds sont coordonnés et équipés d'ordinateurs quantiques et pourraient s'entendre sur le contenu du nouveau bloc. Elle est possible sur des jeunes Blockchains avec peu de nœuds. Dans le cas de Bitcoin il existe environ 16000 nœuds actifs au 17/05/2022[102], il faudrait donc pouvoir décider des résultats sur plus de 7500 nœuds au même moment.

La France se classe avec 521 nœuds [21] (3,26% du total), 4ème pays disposant du plus de nœuds Bitcoin derrière les États-Unis et l'Allemagne. La première place est occupée par plus de 54% des nœuds d'origines non communiquées 13.

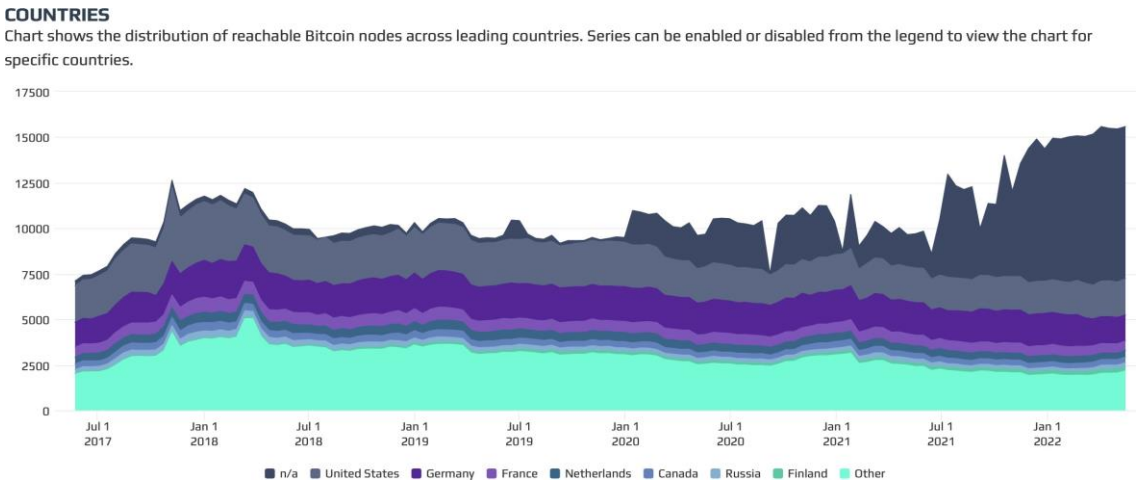

Figure 13 – Noeuds par pays

La cryptographie à clés publiques permet dans le cas des Blockchains d'authentifier les transactions qui y sont réalisées. Cette clé est ainsi utilisée pour soutenir les opé- rations de portefeuilles numériques sur une Blockchain. En d'autres termes, on utilise la clé publique du portefeuille numérique de Madame Michu pour effectuer ses différentes transactions sur une Blockchain. Le portefeuille numérique est donc associé par un hashage effectué sur la clé publique de l'utilisateur. Le portefeuille numérique est donc là pour stocker et sécuriser vos actifs numériques ainsi que les transactions s'y rapportant. Les signatures à clés publiques les plus couramment utilisées sur les Blockchains sont basées sur la Cryptographie à Courbe Elliptique (ECC) qui a la particularité de générer des clés de petite taille. Ce principe a été utilisé car il est facile à mettre en œuvre et répondait à l'assurance de sécurité pré-quantique. Mais le quantique fait voler en éclat l'ECC car associé à l'algorithme de Shor, il permettra de divulguer la clé privé de n'importe quelle clé publique publiée sur la Blockchain. Ceci est catastrophique pour certaines Blockchains, mais pas toutes. En effet, les Blockchains utilisant la preuve de participation (PoS 22) sont principalement visées par cette avancée technologique. Les Blockchains telles que Bitcoin qui reposent sur le PoW seront bien moins impactés puisque la publication des clés publiques ne sont pas nécessairement requises. Par ailleurs la clé publique est issue d'un hashage (SHA256) qu'il faudrait faire évoluer vers des fonctions de hashage post-quantique.

20. Un token est un actif numérique émis et échangeable sur une blockchain [107]
21. Statistiques au 17/05/2022

ANALYSE DE RISQUES SUR LES BLOCKCHAINS PRINCI- PALES

Bien que l'approche cryptographique reste sur des logiques similaires d'une Blockchain à l'autre, les détails d'implémentation sont bien distincts. Dès lors, les menaces liées aux algorithmes post-quantiques peuvent ainsi s'opérer à différents niveaux. Nous allons reprendre les travaux réalisés par le Cloud Security ALliance (CSA) [108].

Bitcoin :

1. Immuabilité : il existe une probabilité d'attaque et d'altération d'un bloc exis- tant puisque l'algorithme de hashage utilisé repose sur 256 bits (SHA 256). Une sécurité basée sur l'algorithme de Grover adossé à du quantique permet- trait de diminuer le nombre d'opérations à réaliser mais resterait quand même sur un niveau de 2e128 opérations ce qui permettrait de le rendre résistant aux attaques quantiques.
2. Adresse public : afin de recevoir des bitcoins, tout destinataire doit générer une paire de clés publiques/privées et calculer une adresse, ou seront stockées les transactions. Cette adresse est un hachage de la clé publique du porte- feuille du destinataire. Dans le cas de Bitcoin, un algorithme asymétrique est utilisé (ECC), qui comme nous l'avons vu précédemment n'est pas quantique- proof. Toutefois, la clé publique est cachée par la fonction de hashage donc elle reste bien protégée tant qu'aucune transaction n'est à réaliser. Cependant, lorsqu'un utilisateur à besoin de dépenser des bitcoins associés à une adresse, alors la clé publique est publiée sur la Blockchain. Cette opération est normale puisque cela permet à la Blockchain de vérifier la transaction. Cependant, et comme le précise le rapport [108], dans une transaction, tous les bitcoins liés à cette adresse doivent être dépensés. Tout "changement" restant est envoyé, en principe, à une nouvelle adresse. Si cette règle est respectée, le seul risque d'un ordinateur quantique est celui d'un adversaire interceptant la transaction, brisant la clé et effectuant une autre transaction, le tout en quelques minutes. Il est assez peu probable qu'un ordinateur quantique soit assez rapide pour le faire à court terme. Ce risque est donc minime. Ce- pendant, par mesure pratique, de nombreux utilisateurs réutilisent la même adresse pour plusieurs transactions. Ce n'est pas la bonne implémentation et peut mettre leurs cryptoactifs en danger lorsque les attaques quantiques arriveront.
3. PoW : comme évoqué précédemment un ordinateur quantique avec le bon algorithme pourra également tirer avantage de la puissance de cette machine et donc valider les blocs potentiellement en premier et ainsi recevoir la ré- compense. Pour altérer la chaîne de bloc il faudrait que plus de 50% des nœuds soient "attaqués". Le risque est donc existant mais minime sur cette ère post-quantique.

Ethereum :

1. Immuabilité : dans la même logique que pour Bitcoin, la chaîne Ethereum est vulnérable au quantique tant qu'elle n'adapte pas ses fonctions de hashage. La seule différence aujourd'hui entre ces Blockchains est dans la technique de hashage utilisée, le Keccak-256 (plus connue sous le nom "SHA3") en l'occurrence.

2. Consensus : le même mécanisme de consensus PoW est utilisé actuellement par Ethereum, les remarques sont donc similaires à celles de Bitcoin. Néan- moins, des travaux sont en cours pour passer sur un mode PoS. Cet Ethe- reum 2.0 devait arriver lors

du 1er semestre 2022 et vient d'être repoussé au dernier trimestre 2022. Cette mise à jour majeure fera passer le réseau Ethe- reum d'une approche PoW à une logique PoS, ce qui permettra notamment de sécuriser la chaîne, notamment face au quantique, d'accélérer l'ensemble des transactions et de baisser la consommation énergétique de 99% (FAQ POS CSA). La partie quantique-resistance sera adressée notamment par « avec des schémas de signature réputés résistants aux attaques quantiques tels que Lamport, XMSS ou SPHINCS comme mentionnés en première par- tie. » [108]. Le schéma de signature de transactions utilisée par Ethereum est l'Elliptic Curve Digital Signature Algorithm (ECDSA) qui est n'est pas considéré comme quantum-résistant.

STANDARDISATION

Les signatures post-quantiques sont en cours de normalisation. Ainsi, des travaux sont en cours dans le cadre du processus du NIST afin de sélectionner des candidats appropriés pour les signatures et les mécanismes d'échange de clés résistants au calcul quantique, qui peuvent être utilisés pour chiffrer les clés privées. Nous ne passerons en revue l'ensemble de ces systèmes de signature mais nous concentrerons sur l'état actuel du processus.

À l'heure actuelle, il y a trois candidats finalistes pour la normalisation des systèmes de signatures par le NIST. Deux sont basés sur les treillis et un sur la cryptographie multivarié. En outre, il y a des candidats alternatifs, basés sur les fonctions de hachage, et à nouveau, les schémas multivariés. De nombreux autres candidats pour le premier et le deuxième tour ont été éliminés. Dans la première partie nous avons décrits le fonctionnement des cryptographies en treillis et multivariés qui restent des pistes intéressantes.

Finalement, que pouvons-nous en conclure ? Les Blockchains seront bien évidemment impactées, et ce, quelles que soient leur taille et capitalisation de marché. Cependant, certains aspects ne seront pas exploités par des attaquants. En effet, le processus de validation communautaire permettra de contrôler l'impact voire l'existence de certaines attaques (sic, "attaques 51%"). Néanmoins, l'ensemble des Blockchains devront revoir leur implémentions et migrer vers des schémas de signa- tures Lamport, XMSS ou SPHINCS et tout autre schéma validé par le NIST.

À la suite d'entretiens effectués le 25.03.2022 avec M. Gérard Dréan, auteur et conférencier sur les sujets liés à l'économie, l'histoire de la pensée économique et des cryptomonnaies, nous indique que le PoW n'est pas plus ou moins résistant au quantique que le PoS, seul compte l'implémentation (la manière de concevoir et architecturer les Blockchains). En d'autres termes, une chaîne de type PoS bien conçue sera plus résistante qu'une chaîne PoW mal conçue. Donc il y a bien le niveau de sécurité intrinsèque d'une chaîne (d'un point de vue technologique) mais également sa conception et utilisation.

22. PoS : Proof of Stake ou Preuve de Participation.

CAS PRATIQUES

Étudions maintenant quelques cas d'usages Blockchain dans différents secteurs. L'idée n'est pas de faire une analysé poussée de chaque secteur mais plutôt de voir si ces initiatives sont globales ou localisées, si elles ne concernent qu'une typologie sectorielle et enfin de savoir le pourquoi ces initiatives. En déterminant ce pourquoi on pourra en déduire des hypothèses que pourraient se faire des attaquants (voir ces canvas en annexe B).
Ces canvas tirés du site de la Cloud Security Alliance [109] nous permettent tout d'abord de constater que l'utilisation de la technologie Blockchain peut se faire dans tous les secteurs. Les canvas proposés nous permet de faire ressortir un certain nombre d'éléments saillants. La plupart de ces cas d'usage permettent de répondre unanimement à des enjeux de réduction des complexités et coûts administratifs, transparences sur la documentation et une vision en temps réelle de données.

On note cependant que certaines des initiatives décrites dans ce document ne sont toujours pas en production depuis la date de rédaction du rapport en 2018. Ceci s'explique non pas par la jeunesse de la technologie mais plutôt par son expérimentation très récente par les différentes entreprises. En effet, une telle technologique présente des coûts financiers et humains élevés. Cette nouvelle approche s'inscrivant davantage dans de la recherche et développement plus que du simple projet informatique a un coût financier bien réel. Le coût humain souvent sous-estimé peut-être également énorme. En effet, si vous simplifiez toute la chaîne de gestion documentaire, processus, charge de la preuve, etc. ce sont des activités qui sont aujourd'hui réalisés manuellement ou semi-manuellement par un humain qui vont être entière- ment automatisées.
Finalement, qu'est-ce qu'un attaquant peut tirer de ces différents cas d'usages ? Dans la plupart des cas le gain financier des entreprises est principalement due à une baisse des coûts, donc si un attaquant opère cela n'est pas forcément dans un vol financier direct. Néanmoins, par ricochet cela lui permets de détenir des secrets de la victime et de le monnayer par la suite. Un attaquant peut également para- lyser le système et donc les processus. Dans le cadre d'un transporteur cela serai catastrophique sur son activité car il pourrait ne plus être en mesure d'opérer. Des plans de continuité d'activité dématérialisé devront être instruits. Sans citer tous les mobiles potentiels on se rend compte que les motifs des attaquants sont les mêmes qu'aujourd'hui (Figure 14). Ce qui va changer sera finalement la dépendance encore accrue des entreprises à leur système d'information.

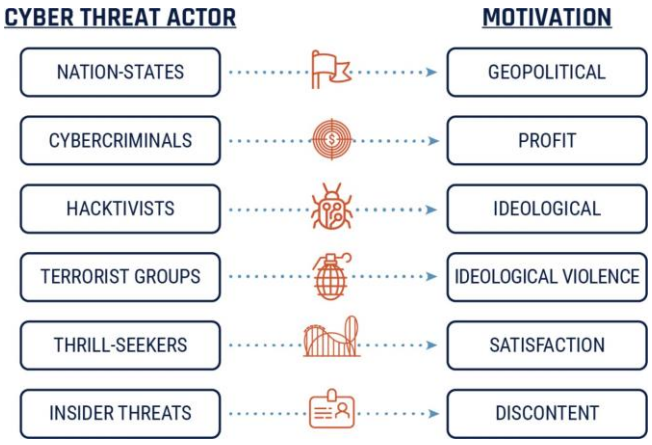

Figure 14 – Typologies d'attaquants

Afin de revenir sur notre problématique de sécurité des Blockchains on peut supposer que lorsque ces applications seront mises en production, et ce de manière massive et multisectorielle, cela poussera les attaquants à se tourner vers ces systèmes. La question que nous pouvons poser est alors : l'informatique quantique permettra-t-il d'attaquer ces systèmes ou bien resteront-ils suffisamment résilients ? Par extension, les attaquants ne vont-ils pas se tourner davantage vers les utilisateurs individuels ?

LA STRATEGIE QUANTIQUE FRANCAISE : UNE POLITIQUE NATIONALE TARDIVE MAIS AMBITIEUSE

La France est entrée dans la bataille de manière officielle le 21 janvier 2021 à travers l'annonce d'un plan quantique à 1,8 milliards d'euros sur cinq ans par le président de la République Emmanuel Macron dans un lieu symbolique que constitue en la matière l'université Paris-Saclay [110].

Ce moment était attendu de longue date par les acteurs du domaine qui commençaient à s'impatienter. Si l'État Français est souvent critiqué pour avoir tendance à vouloir se mêler de tout, ou au contraire d'être totalement absent, il était attendu au tournant dans ce domaine. En effet, les technologies quantiques relèvent d'un investissement à long terme et avec une forte pondération de recherche publique, le tout dans un paysage mondial où tous les États se mènent une lutte sans merci.
En 2019, le premier ministre Edouard Philippe confiait à la députée Paula Forteza une mission parlementaire relative à la stratégie nationale en matière de technologies quantiques. En Janvier 2020, accompagnée de son équipe, elle a remis au gouverne- ment le rapport "Quantique : le virage technologique que la France ne ratera pas" [96].

Le rapport souligne que la technologie quantique est une innovation de rupture, et que seuls les pays qui auront osé prendre des risques trouveront une place dans ce nouveau tournant technologique et pourront donc garantir leur souveraineté. Alors que les États-Unis d'Amérique disposent d'une avancée technologique, l'Alle- magne et le Royaume-Uni ont lancé chacun leur programme national pour 650M€ et 270M£. Le rapport estime que la France accuse aujourd'hui un retard réel en matière de développement technologique et industriel : il y a urgence à agir.
Face aux exploits prometteurs et très attendus de l'informatique quantique, la construction d'une telle machine pose un réel défi en matière de cybersécurité.

La sécurité et la souveraineté nationales par essence ont toujours été étroitement liées aux innovations technologiques, sources de stratégies. Le besoin d'innovation n'a jamais été aussi essentiel dans un monde caractérisé par le retour des États puissance, l'émergence d'acteurs non étatiques, tels que les groupes terroristes, l'évolution des théâtres d'opération dans les champs numériques et spatiaux. Face à l'impérieuse nécessité de l'innovation, l'État Français a mis au cœur de son action l'innovation pour faire face aux défis futurs. Elle se trouve donc au centre des préoccupations du pouvoir politique, des services régaliens, des autorités militaires, des industriels de l'armement et des startups civiles. Elle innerve tout l'écosystème quantique français.

Il y a ainsi en France un écosystème qui est au cœur de la réussite française. Il regroupe les meilleures équipes de recherche fondamentale et technologique, des laboratoires universitaires, les organismes de recherche, les startups et les grands groupes qui travaillent et œuvrent ensemble pour pousser les innovations. Il y a les fleurons de l'industrie qui demain utiliseront ces technologies comme Total, EDF, etc. et qui sont impliqués dans ces recherches parce qu'ils en seront les utilisateurs tout comme l'État sur ses capacités civiles ou militaires.

Devenir une économie de rupture technologique nécessite de faire des choix de secteurs prioritaires, sur lesquels focaliser des soutiens massifs à l'innovation et au développement. Une telle intervention ciblée, orientée sur le long terme, doit per- mettre d'anticiper, de préparer et d'encourager les grandes transitions notamment numérique qui vont venir remodeler notre société à horizon 2030, tout en garantissant le plus important : notre souveraineté nationale.
Si l'essor de l'informatique quantique oblige l'État Français à se mettre en ordre de bataille avec un plan d'actions ambitieux (chapitre 1), il suscite sur le plan stratégique autant de craintes que d'espoirs technologiques (chapitre 2) dont la seule finalité recherchée doit être de garantir notre indépendance dans ce domaine décisif (chapitre 3).

L'ÉTAT FRANCAIS A L'ÉPREUVE DE LA REVOLUTION DE L'INFORMATIQUE QUANTIQUE

Maîtriser l'infiniment petit, c'est disposer d'un avantage décisif dans les supercalculateurs, donc les communications, la défense, la santé, etc. Toutes les grandes puissances le savent et se sont engagés dans une bataille qui a déjà commencé [111].
Comme nous l'avons vu au chapitre précédent, les États-Unis, la Chine, le Royaume- Uni ou encore l'Allemagne et bien d'autres ont tous déjà élaboré des programmes nationaux en matière de technologies quantiques.

Il y a donc urgence pour la France car tout se joue maintenant. L'enjeu est avant tout d'assurer la souveraineté technologique de la France, de garantir la sécurité du pays et de préserver sa compétitivité économique par rapport aux autres pays plus avancés qu'elle en matière d'innovation. Pour ce faire, elle dispose d'atouts majeurs comme des chercheurs et des développeurs pointus en la matière. Elle bénéficie par ailleurs d'une antériorité sur le sujet. En effet, la France a été la pionnière de la re- cherche en physique quantique, dont la première révolution a permis l'invention du transistor, des lasers ou encore du GPS. Elle dispose ainsi de toutes les compétences pour se distinguer sur la scène internationale dans cette technologie de rupture en visant le leadership mondial de l'informatique quantique. Mettre la France dans le trio mondial de tête des technologies quantiques, telle est l'ambition du pouvoir étatique. Un plan d'investissements public-privé de 1,8 milliards d'euros sur cinq ans est annoncé pour permettre de réaliser l'exploit scientifique majeur de se doter d'un prototype complet d'ordinateur quantique. Imaginez des calculs informatiques en trois minutes au lieu de 10 000 ans aujourd'hui, des applications infinies, des possibilités insoupçonnées et un véritable avantage stratégique.

"Le quantique fait partie des quelques clés du futur que la France doit avoir en main", indique le Président Emmanuel Macron lors de la présentation du plan quantique le 21 janvier 2021 à l'université Paris-Saclay.
Pour concrétiser cet objectif, le gouvernement a missionné en avril 2019 la députée de la 2ème circonscription des Français établis hors de France Paula Forteza,
M. Jean-Paul Herteman ex-PDG de Safran et M. Lordanis Kerenidis directeur de recherche du CNRS sur la question des technologies quantiques. Les conclusions rendues le 9 janvier 2020 ont répondu à deux questions essentielles : la France peut-elle jouer un rôle majeur dans la révolution de l'informatique quantique ? Et quelle politique nationale

ambitieuse mettre en place pour y parvenir ?

"Quantique : le virage technologique que la France ne ratera pas" est le titre audacieux du rapport remis aux ministres de l'enseignement supérieur et recherche, des armées et de l'économie directement concernés par cette révolution à venir. Sur cette base, le gouvernement a annoncé la mise en place d'un groupe de travail interministériel pour établir une feuille de route quantique regroupant les trois ministères cités, l'Inria [23], le CEA, le CNRS et les opérateurs financiers Bpifrance et issus du Secrétariat général pour l'investissement (SGPI [112]) . De cette feuille de route a été élaboré la stratégie nationale quantique pour mettre la France au cœur de cette future révolution.

Ainsi sur la base d'une analyse des enjeux du quantique et des préconisations associées (1ère partie), le gouvernement a pu donner un signal politique fort à travers l'élaboration d'un plan quantique ambitieux pour l'avenir (2nd partie).

UNE RÉVOLUTION NUMÉRIQUE A NE PAS RATER

"Le virage est là et c'est maintenant qu'il faut le prendre, nous l'avons compris". C'est par ces mots que le président de la République Française introduit le plan quantique élaboré par le gouvernement sur la base d'un rapport parlementaire exhaustif.
Le rapport "Forteza" souligne que la technologie quantique est une innovation de rupture, et que seuls les pays qui auront osé prendre des risques trouveront une place dans ce nouveau tournant technologique et pourront donc garantir leur souveraineté.

Alors que les États-Unis d'Amérique et la Chine disposent d'une avancée techno- logique, l'Allemagne et le Royaume-Uni ont lancés chacun leur programme national avec un an d'avance. Le rapport estime que la France accuse aujourd'hui un retard réel en matière de développement technologique et industriel et conclut qu'il y a urgence à agir. De nombreux pays sont dans la course (Figure 15).
Pour éclairer le gouvernement, le rapport [96] aborde les axes et les enjeux de la technologie quantique (§1) et formule des recommandations (§2).

23. Inria : Institut national de recherche en sciences et technologies du numérique

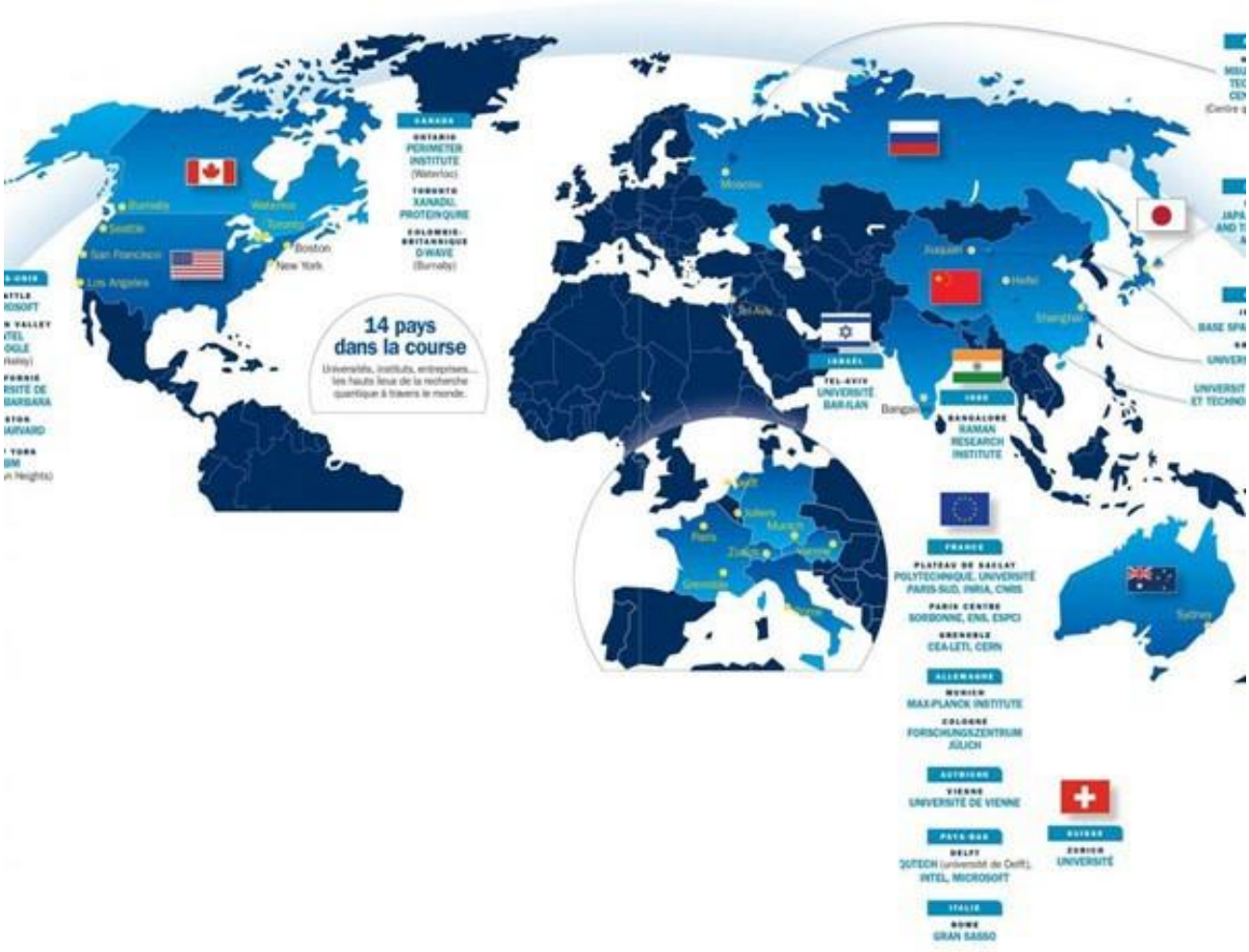

Figure 15 – Radar des startups Quantique & Cybersécurité innovantes

Les axes et enjeux majeurs de la technologie quantique

Dès le préambule du rapport, les ambitions sont clairement affichées. La France doit devenir l'un des leaders mondiaux en matière de calculateurs quantiques tolérants aux défauts Large Scale Quantum (LSQ), devenir le leader européen en matière de calculateurs quantiques bruités de taille intermédiaire Noisy Intermediate Scale Quantum (NISQ) et devenir l'un des leaders mondiaux en matière de logiciels métiers.

Elle doit également jouir d'une large autonomie industrielle sur les technologies habilitantes, jouir d'une large autonomie industrielle sur les capteurs à base d'impuretés dans le diamant et maintenir une indépendance stratégique sur les technologies de cryptographie.

Pour atteindre ces objectifs, le rapport présente trois axes de recherche et développe- ment à emprunter préférentiellement et identifie sept enjeux majeurs pour la France dans le domaine du quantique.

Les axes de recherches et de développement prioritaires

Le 20 janvier 2022, M. Gérard Longuet, sénateur et M. Cédric Villani, député, ont déposé le Rapport n° 377, fait au nom de l'Office Parlementaire d'Évaluation des Choix Scientifiques et Technologiques (OPECST), intitulé "La stratégie quantique française". Cette office vient notamment confirmer la pertinence des trois axes de recherche et développement à emprunter préférentiellement, à savoir le calcul, les communications et

la cryptographie, et les capteurs quantiques [113]. L'objectif de la stratégie est bien d'accélérer dans les secteurs où la France possède déjà un certain avantage.

- Les calculateurs quantiques.
  Les calculateurs quantiques sont essentiellement tournés et financés par le monde de la Défense militaire. Il convient d'ouvrir plus largement le spectre en développant les usages et les marchés civils afin d'assurer la viabilité économique de ce secteur sur le long terme.

- Les communications et la cryptographie.
  La sécurisation des données représente un enjeu stratégique pour les entre- prises, les grands groupes industriels, les banques ou encore l'État dans toutes ses composantes. L'avènement possible de l'ordinateur quantique impose de recourir à des méthodes plus élaborées. La cryptographie quantique et post- quantique offrent des solutions à moyen terme [114]. Ces technologies, qui reposent sur la transmission de qubits générés aléatoirement, assurent l'inviolabilité des échanges et la sécurisation des données en toutes circonstances. Elles doivent faire l'objet d'une veille rigoureuse afin d'anticiper de potentielles failles ou difficultés en matière de sécurité.

- Les capteurs quantiques L'exploitation des propriétés quantiques de certaines particules permet de détecter, de mesurer et de réaliser des images avec une extrême précision. Elles améliorent les capacités de systèmes existants tout en ouvrant la voie à de nouvelles fonctionnalités. Afin de consolider la position de la France, il convient d'orienter la R&D sur les capteurs à atomes froids, sur la prochaine génération de senseurs inertiels, sur les capteurs magnétiques et sur les horloges atomique [115].

Ces trois axes de R&D doivent s'appuyer sur une veille scientifique et technologique de ces technologies et sur les évolutions qui accompagneront leur développement.

Les enjeux technologiques et nationaux
Les rapporteurs ont identifié plusieurs sept enjeux majeurs (trois pour le calcul quantique, deux pour la cryptographie quantique et post-quantique et deux pour les capteurs quantiques) qui doivent guider l'action de l'écosystème quantique français regroupant les chercheurs, les développeurs, les industriels et l'État [116].

S'agissant du calcul quantique, il convient de :

- Diffuser l'usage du calcul quantique dans les secteurs applicatifs prioritaires (chimie, logistique, intelligence artificielle, etc.) afin d'anticiper et d'éviter une rupture technologique.
- Se prémunir d'une trop forte dépendance vis-à-vis d'un acteur ou d'une voie technologique unique.
- Garantir la capacité de développement quantique de la France dans ce domaine et éviter la rétention technologique des autres pays. Sur l'axe des communications et des cryptographies quantiques et post-quantiques, deux enjeux majeurs doivent être appréhendés.
- Garantir la sécurité des systèmes de télécommunication. Dans l'éventualité même lointaine de l'avènement d'un calculateur quantique suffisamment per- formant,

l'intégrité rétroactive sur cinquante ans (au moins) des communications et informations sensibles.
- Garantir la souveraineté des systèmes de télécommunication. En d'autres termes, il faut se prémunir contre l'introduction, dans les infrastructures de communication, de composants de cryptographie quantique maîtrisés unique- ment par les acteurs non européens.

Pour les capteurs quantiques, il y a lieu de :
- S'assurer d'une capacité opérationnelle d'approvisionnement en technologies de capteurs quantiques.
- Garantir la viabilité économique à long terme des technologies de capteurs quantiques développées en France.

Les propositions de la mission parlementaire pour une stratégie nationale

Après avoir reçu mission d'apporter une analyse sur l'avenir quantique de la France, le rapport parlementaire de la députée Paula Forteza élabore plusieurs propositions pour doter la nation d'une force de frappe quantique [117].

Après avoir donné les axes de recherches et de développements et déterminer les enjeux quantiques majeurs de demain, les rapporteurs soumettent au gouverne- ment trente-sept propositions. Une majorité d'entre elles seront reprises dans le plan stratégique quantique de la France énoncé par le président de la République le 21 janvier 2021 à l'université Paris-Saclay.

Ces propositions visent prioritairement à assurer la souveraineté de la nation sous deux angles : technologique et économique.

Des recommandations pour garantir la souveraineté technologique de la France

Les propositions que nous allons observer dans ce paragraphe concernent la création d'une infrastructure de pointe pour la recherche et l'industrie dont le socle s'appuie sur un programme de soutien au développement technologique et au développement des usages. Pour aboutir à cette finalité, vingt-cinq propositions sont formulées. Le rapport étant public, nous ne mettrons que les plus marquantes :

- Héberger, au « Très Grand centre de calcul » (TGCC), une plateforme de calcul quantique diversifiée, évolutive et accessible aux communautés de chercheurs et développeurs académiques et industriels [118].
- Ouvrir un appel à contributions permanent à destination des startups et laboratoires français et européens développant des processeurs d'accélération quantique en vue d'une intégration à l'infrastructure de calcul.
- Déployer une plateforme de test pour différents dispositifs de communications quantiques
- Inciter les laboratoires et entreprises français à répondre aux appels à projets européens "Flagship Quantum Technologies" [119]
- Ambitions sur les calculateurs "Large Scale Quantum" (LSQ), c'est à dire tolérant aux défauts
- Mettre en place, en 2020, un Grand Défi de l'innovation "Noisy Intermediate Scale Quantum" (NISQ), c'est à dire un ordinateur quantique imparfait de taille intermédiaire visant à développer, avant 2023, une pile logicielle métier interopérable pour les secteurs de la chimie, de la logistique et de l'IA

- Renforcer les moyens de recherche en algorithmes et logiciels dans le domaine du calcul quantique
- Élaborer une stratégie d'évaluation des systèmes "Quantum Key Distribution" (QKD) s'appuyant sur un schéma de certification français et européen.
- Diffuser l'usage du calcul quantique, à travers des "challenges" et "hackathons" proposés par les industriels des secteurs applicatifs les plus avancées à l'instar du "Airbus Quantum Computing Challenge" [120].

Des recommandations pour assurer la souveraineté économique de la France

Dans leurs conclusions, les rapporteurs notent des enjeux économiques majeurs liés à la maîtrise des technologies quantiques. Onze propositions visent à préserver la souveraineté de la France. Elles abordent la nécessité d'attirer et de garder les ta- lents à travers une formation et un accompagnement de carrière de qualité, d'investir massivement dans les startups spécialisées et la nomination d'un coordinateur inter- ministériel du plan national. Sur les onze propositions, voici celles qui nous paraissent les plus pertinentes :

- Créer, à Paris, à Saclay ainsi qu'à Grenoble, trois hubs quantiques rassemblant chercheurs en informatique théorique et appliquée, ingénieurs, industriels des filières technologiques, et utilisateurs finaux.
- Concevoir des parcours de formation avec une spécialisation en ingénierie et en informatique quantique et anticiper la croissance du besoin en ingénieurs et techniciens des filières industrielles.
- Sensibiliser les acteurs de l'écosystème aux nouvelles dispositions de la loi PACTE relatives à la mobilité des chercheurs et l'accès aux moyens des laboratoires par les startups.
- Accompagner la création d'une cinquantaine de startups du quantique jus- qu'en 2024.
- Sensibiliser les différents acteurs les plus stratégiques aux risques de pillage technologique et aux outils disponibles permettant d'y faire face.
- Constituer un comité stratégique chargé de prendre les décisions d'orientation des actions de recherche.
- Nommer un coordinateur interministériel du plan national, chargé de veiller à la cohérence globale des actions des différents acteurs publics et privés au niveau national.

Fort de cette analyse et des recommandations éditées dans le rapport Forteza, le gouvernement a élaboré une politique nationale ambitieuse capable de donner à la France un leadership scientifique et industriel dans les technologies quantiques.

UNE VOLONTÉ D'INVESTIR POUR L'AVENIR

Après plusieurs années de longue gestation, rallongée par la pandémie de Covid-19 et un bon nombre d'aléas politiques, le plan quantique national a enfin été lancé le jeudi 21 janvier 2021 par le Président de la République Emmanuel Macron à l'occasion d'une visite au Centre de Nanosciences et de Nanotechnologies (C2N) du CNRS sur le Plateau de Saclay [121].

Inspiré du rapport Forteza et des 37 mesures proposées, la "task force quantique" chargée d'élaborer la stratégie nationale dans ce domaine a bien pris en compte l'excellence de la recherche française mais aussi le retard du pays en termes

d'investissements (le rapport Forteza ayant préconisé de tripler le budget pour la recherche).

Ce déplacement présidentiel s'inscrit dans la lignée de ce qui a déjà été mis en place ces trois dernières années en faveur de la recherche française (le loi de programmation pour la recherche, le programme d'investissement d'avenir [122], le plan de relance [123] et le plan sur l'intelligence artificielle [124]) Similaire au Plan IA présenté en 2018, le plan quantique prévoit des actions en faveur de la recherche (en particulier pour les ordinateurs, capteurs et communications quantiques), de l'industrie et de la formation.
Cet engagement politique et financier sans précédent sur des technologies disruptives permet à la France de rentrer avec force et robustesse dans la course [125]. Certes, elle affiche un certain retard à l'allumage mais elle peut s'appuyer sur un écosystème académique et industriel plus motivé que jamais.

A la différence des plans quantiques de nos voisins, celui de la France a la mérite d'être très détaillé (26 pages). Il expose les différents domaines, instruments et montants d'investissements associés (§1). Un cadre et un suivi pour plus d'efficacité sont également précisés (§2).

Un plan quantique ambitieux et attendu
Lors de l'annonce du plan quantique, le Président Emmanuel Macron annonçait avec un investissement massif de 1,8 milliard d'euros sur cinq ans. La France se hisse ainsi en troisième position des nations qui investissent dans les technologies quantiques [126].

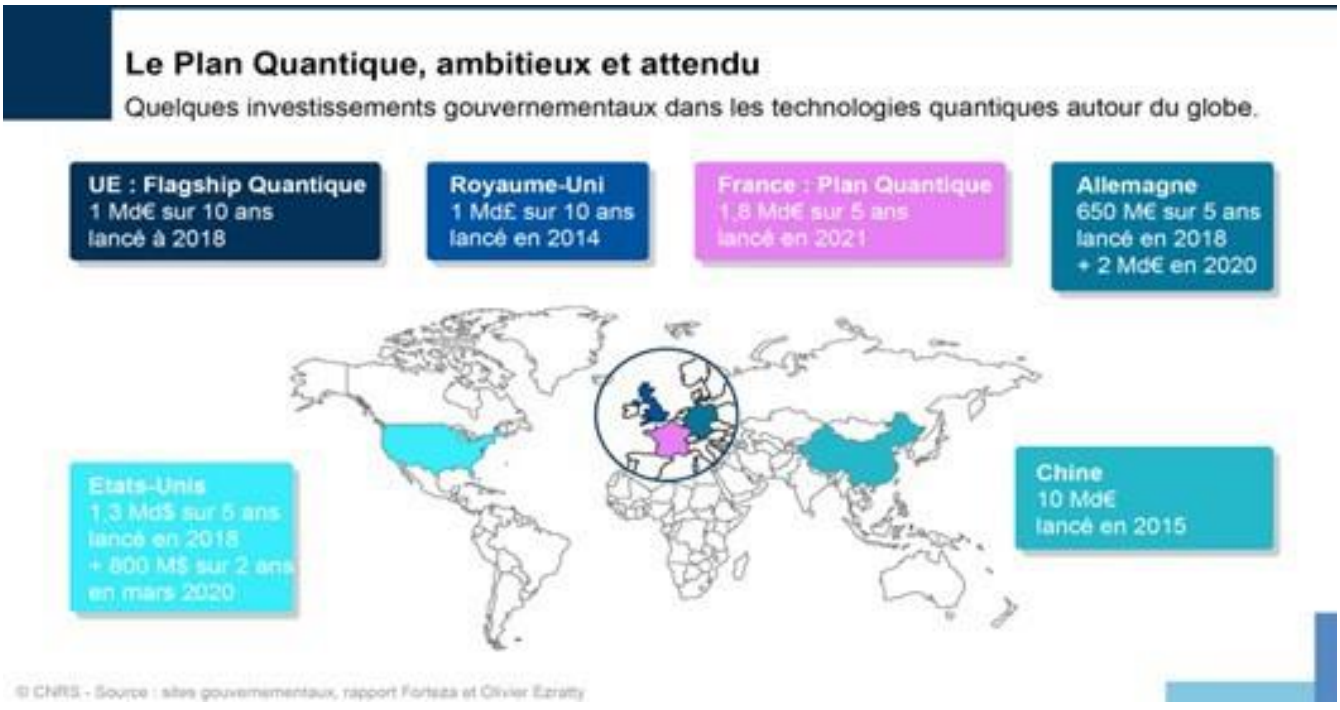

Figure 16 – Plan Quantique

On le comprend, cette stratégie est un enjeu majeur pour la France. Elle dispose de nombreux atouts pour la conduire : de grands laboratoires d'excellence dont certains récompensés par des prix Nobel, une large communauté d'entreprises et d'industriels, ou encore un premier fond dédié aux technologies quantiques [127].

Les axes stratégiques du plan quantique

Définir une stratégie, c'est avoir un objectif et faire des choix. L'objectif affiché est d'enrichir et affirmer les capacités de la France sur les plans scientifique et techno- logique, ainsi que dans les chaînes de valeur industrielles et le développement du capital humain, afin d'assurer notre indépendance dans ce domaine technologique qui participera à façonner le futur. De l'analyse du plan quantique, il ressort certains choix affirmés comme une volonté forte d'investir dans la recherche fondamentale, de favoriser l'émergence d'une filière industrielle complète intégrant notamment les technologies habilitantes, et de faire le pari du silicium pour le LSQ tout en encourageant les autres technologies sur le NISQ .

La stratégie nationale quantique annoncée par le président de la République repose sur 3 axes :

- La mise à disposition de nouveaux moyens pour les chercheurs, y compris sur la formation, mais aussi pour les startups et les industriels
- Le développement de l'informatique quantique
- Des investissements dans toutes les technologies autour du quantique : calculateurs, communications, capteurs et cryptographie notamment. Comme l'indique Cédric O, secrétaire d'Etat chargé du numérique, dans l'entretien Decode Quantum, l'État est moins dirigiste que dans les années 1960/1970 (plan de calcul en 1966 [128]). Il intervient en amont de l'innovation en finançant la recherche publique comme le font tous les autres pays industriels. Il crée les conditions d'un flux optimum allant de la recherche aux entreprises, petites et grandes.

L'État ne fait pas trop de choix sur telle ou telle technologie (quantique) dans la mesure où l'incertitude scientifique reste élevée. Il cofinance avec le secteur privé les startups du secteur et joue le rôle de client là où c'est pertinent, surtout côté centres de calcul et secteurs régaliens.

Un financement conséquent qui permet de rentrer avec force dans la course aux technologies quantiques

Porté par le président de la République, le plan quantique a pour objectif d'élever la France au plus haut niveau mondial des technologies quantiques, appelées à transformer l'informatique et l'industrie, par un engagement public-privé de 1,8 milliard d'euros sur cinq ans . L'État apporte 1,05 milliard d'euros sur la table, le reste provenant de fonds européens (200 millions) et privés (550 millions) [129].

Le plan quantique fait notamment passer les crédits publics à 200 millions d'euros par an, ce qui placerait la France au troisième rang mondial (derrière la Chine et les États-Unis). La France peut ainsi espérer devenir le premier État à se doter d'un prototype complet d'ordinateur quantique généraliste.

Le 1,8 milliard d'euros d'investissement est réparti suivant six grands axes de financement. Cet investissement concerne toutes les technologies quantiques (ordinateur, capteurs, communication et cryptographie) ainsi que l'écosystème associé. Ce plan financier massif positionne la France à un très bon niveau à l'échelle internationale [130].

Axes technologiques de la stratégie nationale						Total 2021-2025 (M Euros)
NSQ	LSQ	Capteur Quantique	Communication Quantique	Cryptographie Post-Quantique	Technologie Capacitante	
352	432	258	325	156	292	1815

Table 2 – Répartition par axe de technologies

Il s'agit d'un effort absolument majeur, qui témoigne avant tout de la volonté du gouvernement et du président de la République, de faire de la France un des acteurs majeurs de ces technologies au niveau européen et international. L'objectif économique également affiché est de créer 16 000 emplois directs à l'horizon 2030, pour une activité qui représentera à terme entre 1 et 2 % des exportations françaises.

Total 2021-2025 M Euros	1815
Recherche	725
Formation	61
Maturation Technologique	171
Innovation de Rupture	114
Soutien au déploiement industriel	224
Politique d'Achat Public	72
Entreprenariat	439
Intelligence Economique	9

Table 3 – Répartition par modalités de soutien

Total 2021-2025 M Euros	1815
PIA 4	594
Subvention aux organismes de recherche	274
Autres contributions nationales	164
Innovation de Rupture	114
Financements Européens	238
Secteur Privé	545

Table 4 – Répartition par origine de financements

Une stratégie quantique cadrée et contrôlée

Un plan d'action ne peut être efficace que s'il est cadré et suivi dans son exécution. Le président de la République français a désigné les principaux piliers du plan quantique à savoir un programme de développement technologique global et intégré ainsi qu'un renforcement de l'écosystème d'innovation français dans le domaine du quantique.

Pour s'assurer du suivi de la stratégie mise en place, un coordonnateur est ainsi créé pour alerter de toutes difficultés rencontrées dans l'application du plan quantique, pour être sûr

que la réactivité est bonne sur les projets de recherche, pour recruter et garder les doctorants et en quelque sorte pour consolider l'écosystème quantique.

Une action qui repose sur deux piliers principaux

Le premier, un programme de développement technologique global et intégré.

Le président de la République, Emmanuel Macron, a beaucoup insisté dans son discours à Saclay sur la nécessité de mettre en place un programme de développement technologique global et intégré allant de la recherche fondamentale jusqu'à l'industrialisation à l'image des grands projets technologiques à long terme de l'aéronautique, de l'espace, de la physique, des hautes énergies [131]. Le but de ce programme est de se donner les moyens de maîtriser les technologies quantiques. Celui-ci doit nécessairement passer par des étapes. Ainsi, pour l'ordinateur quantique, l'objet le plus risqué, le choix stratégique affiché est de procéder en deux phases :

- S'acculturer à l'usage des simulateurs d'ordinateur quantique [132].
- Développer un ordinateur hybride notamment pour la chimie, la logistique et l'intelligence artificielle et ce dès l'horizon 2023 [133].

Avec le grand équipement national de calcul intensif et le CEA, la France hébergera la première structure au monde d'ordinateur quantique hybride. Il faudra enrichir l'écosystème de développeurs dans ce domaine pour anticiper les ruptures futures et que les futures technologies trouvent leur marché. Le Président de la République annonce pour ce faire 350 millions d'euros d'investissement [134].

Mais il faudra aller plus loin et développer l'ordinateur quantique universel et passer à l'échelle industrielle. La France est considéré comme l'un des rares pays capable de relever le défi grâce à l'excellence de la recherche théorique et technologique, grâce à l'industrie micro-électronique. La France pourrait alors devenir le premier état à disposer d'un prototype complet d'ordinateur quantique généraliste. Grâce à l'in- vestissement de la recherche publique et privée, mais aussi grâce à des partenariats industriels comme celui réalisé récemment entre ATOS et la star-up Pasqal. Ce sera un exploit scientifique majeur et le gouvernement va y investir 450 millions d'euros [135].

Le second, le renforcement de l'écosystème d'innovation français.

L'Etat veut donner les moyens aux chercheurs, aux entrepreneurs et industriels de donner le meilleur de leur savoir-faire et de les aider à accélérer. Il faut consolider cette logique d'écosystème qui permet les va et vient entre le fondamental et le technologique, entre le laboratoire de recherches, des grands groupes et les startups / ETI (Entreprises de taille intermédiaire) qui sont en train de se développer.

Il faut jouer sur les complémentarités qui existent dans ce continuum sans forcément faire le choix aujourd'hui d'une technologie quantique clé mais en décidant et en assumant de financer l'ensemble d'entre-elles. Il est assurément trop tôt pour faire un choix définitif. L'État accompagne donc cet écosystème dans une logique d'innovation très ouverte de tests ou de paris qui vont être faits, qu'on va perdre pour certains et gagner pour d'autres. L'État assume cette part d'incertitude.

Création d'un coordinateur interministériel de suivi

Pour conduire cette stratégie et ainsi asseoir durablement la France dans le premier cercle des pays qui maîtrisent ces technologies, M. Neil Abroug, ingénieur INSA et docteur en mathématiques appliquées, est nommé Coordinateur National de "la stratégie

d'accélération pour les technologies quantiques" [136].

Intégré au secrétariat général pour l'investissement, sous l'autorité du Premier ministre, ce coordinateur travaillera en étroite collaboration avec les ministères char- gés de la mise en œuvre de cette stratégie, et en liaison avec l'ensemble des parties prenantes. Il présentera régulièrement les avancées de la stratégie au conseil inter- ministériel de l'innovation.

D'ores et déjà, plusieurs actions sont programmées :

- Un Programme et Équipement Prioritaire de Recherche (PEPR) couvrant la recherche amont tirée par les usages.
- Un programme d'enseignement supérieur aligné avec les attentes du tissu industriel.
- Un grand défi permettant d'offrir un accès au plus important parc de calculateurs quantiques de première génération d'Europe.
- Un programme de développement pour la cryogénie haute performance.
- Un programme d'approvisionnement en matières stratégiques critiques pour le quantique.
- D'autres, comme les programmes de maturation technologique en photonique quantique, suivront d'ici la fin de l'année.

M.Neil Abroug pourra compter sur un appui technique et scientifique de l'OPECST, créé par la loi n° 83-609 du 8 juillet 1983, il a pour mission d'informer le Parlement des conséquences des choix de caractère scientifique et technologique afin d'éclairer ses décisions. A cette fin il recueille des informations, met en œuvre des programmes d'études et procède à des évaluations. A cet effet, l'audition publique du 21octobre 2021 a permis de faire le point sur la mise en place de la Stratégie quantique française quelques mois après les annonces du Président de la République. Les avancées scientifiques et technologiques présentées ont confirmé la place importante de la France dans la course mondiale ainsi que les défis qu'il reste à relever [137].
On l'a vu, c'est une véritable course mondiale aux technologies quantiques qui est en cours, avec des répercussions aussi bien scientifiques que stratégiques, voire géopolitiques. La France a tardé, mais y est désormais engagée via sa stratégie nationale sur les technologies quantiques.

Communications chiffrées, capacités de calcul augmentées, les enjeux stratégiques sont nombreux et obligent l'État français à réfléchir également à la sécurité intérieure comme extérieure du pays eu égard aux menaces et/ou aux opportunités que ces technologies disruptives promettent.

L'INFORMATIQUE QUANTIQUE : MENACE OU OPPORTUNITE POUR LA SECURITE NATIONALE

Depuis plusieurs années, un peu partout dans le monde, les chercheurs et les entre- prises de technologies s'échinent à mettre au point un ordinateur quantique. Face aux exploits prometteurs et très attendus de l'informatique quantique, la construction d'une telle machine pose également un réel défi en matière de cybersécurité.

Il y a donc deux façons d'aborder l'informatique quantique. Soit on privilégie une posture défensive et on le combat, soit au contraire on l'utilise à bon escient pour en faire une force

offensive. Dans la mise en œuvre de la stratégie nationale quantique, la France a décidé de travailler sur ces deux axes en parallèle. Le premier axe relève principalement des services régaliens et en particulier de l'ANSSI qui les représente sur ce sujet et le deuxième est essentiellement traité au sein des armées.

D'aucuns diront que la puissance annoncée de l'informatique quantique présente des risques. Le domaine de la cybersécurité, vital pour les échanges sur Internet qui sont devenus essentiels pour nos sociétés, en est la meilleure illustration. L'une des premières applications de l'ordinateur quantique est le déchiffrement de clés utilisées pour chiffrer les informations. Ce faisant, il met en risque les communications, les systèmes de paiements, la validation des transactions financières ou encore toutes les applications de la Blockchain, comme le Bitcoin. Ces clés sont en effet basées sur la difficulté à factoriser en nombres premiers des très grands nombres, problème qui est justement l'une des capacités fondamentales de l'ordinateur quantique comme nous l'avons vu dans les chapitres précédents.

A l'inverse, l'informatique quantique peut s'avérer être la solution idéale notamment en matière de résolution et de traitements rapides d'opérations complexes. La physique quantique porte également en elle une solution définitive pour sécuriser les échanges : la sensibilité des particules à toute observation permet en effet de détecter à coup sûr si une information a été interceptée sur le chemin entre son émetteur et son récepteur. Et le chemin vers cette solution n'est peut-être pas si long que cela. La Chine l'a prouvé par la mise en place d'une liaison de communication quantique sol-espace pour son satellite Micius dès 2017 [138]. Ces technologies constitueront sans doute l'une des briques de sécurité de l'Internet de demain, affectant fortement le secteur des télécommunications. Les prémices sont déjà visibles, via la solution ID Quantique, qui contribue depuis début 2019 à la sécurisation du réseau 5G de SK Telecom [139], l'un des leaders du marché de téléphonie mobile Sud-Coréen. Dans ce cas, la technologie chiffre les données transmises à l'aide de clés quantiques spéciales qui, selon les lois de la physique quantique, sont impossibles à intercepter ou à voler. Intéressées par les capacités annoncées de l'informatique quantique, les armées françaises se lancent dans la bataille à la recherche de performance inégalée.

Nous l'avons mis en exergue, si l'ordinateur quantique constitue aujourd'hui un risque pour la cybersécurité (1ère partie), il présente de nombreuses opportunités notamment pour les armées. (2nd partie).

UNE STRATEGIE DEFENSIVE POUR LES SERVICES REGA- LIENS : ANTICIPER LES MENACES

La cybersécurité est désormais un enjeu majeur pour les grandes organisations, dont une part croissante des activités dépend de systèmes numériques. La confiance dans ces systèmes est devenue essentielle, mais elle est chaque jour érodée par des incidents majeurs tels que des fuites importantes de données personnelles ou encore des interruptions de services vitaux (souvent liées à des rançongiciels).
L'ordinateur quantique ne vient pas inverser la donne. Au contraire, il rend l'avenir de la sécurité des systèmes de communication encore plus incertain même si à ce jour sa capacité à rendre caduque nos systèmes de chiffrement est assez lointain. On estime une

fenêtre assez large entre 2030 et 2045. Rien n'empêche cependant un attaquant d'acquérir des données aujourd'hui chiffrées et attendre la disponibilité de l'ordinateur quantique pour les déchiffrer. Ainsi des données aujourd'hui protégées ne le seraient plus à court terme [140].
Pour anticiper la menace, l'écosystème quantique et le cybergendarme de la sécurité des systèmes d'information (l'ANSSI) préparent depuis plusieurs années de nouvelles solutions permettant une transition sécurisée vers de nouveaux modèles cryptographiques [141]. Les avancées en informatique quantique poseront de nouveaux défis en matière de cybersécurité (§1). Il convient de se préparer au mieux à cette menace en proposant un plan défensif solide et robuste (§2).

L'INFORMATIQUE QUANTIQUE : UN CYBER- RISQUE MAJEUR

Afin d'anticiper ces défis, il faut au préalable déterminer quels seront les impacts de l'informatique quantique sur les infrastructures françaises numériques actuelles avant d'envisager de proposer des solutions pour s'en prémunir.

Quel impact sur les infrastructures françaises numériques actuelles ?

La sécurité de la majorité des infrastructures numériques repose sur la cryptographie à clé publique, une technologie qui permet de sécuriser les communications entre des entités qui ne partagent aucun secret préétabli. Cette technologie sert deux fonctionnalités principales : l'établissement de canaux protégés (établissement de clés) et l'authentification (signatures numériques). Aujourd'hui, ces techniques reposent essentiellement sur deux problèmes mathématiques dimensionnés pour être pratique- ment impossibles à résoudre avec nos ressources informatiques et nos connaissances mathématiques actuelles : la factorisation des grands nombres (RSA) et le calcul du logarithme discret. Problèmes mathématiques, qu'un ordinateur quantique pourra résoudre. Autre menace, que nous avons évoqué précédemment, celle d'une attaque « stocker maintenant, déchiffrer plus tard ». Celle-ci ne peut être exclue.
On peut aussi penser aux attaques informatiques telles que les attaques par déni de service (DOS ou DDOS) nécessitant d'exploiter de fortes ressources en termes de traitement informatique qui, à l'aide des futurs ordinateurs quantiques, pourraient devenir facilement exécutable.

Quelles solutions envisagées ?

Le NIST, chargé d'établir différents standards technologiques et métrologiques aux Etats-Unis, tente de répondre en désignant des protocoles qui devraient résister à l'ordinateur quantique. L'objectif est d'établir de nouveaux standards. Il a pour cela organisé en 2017, une compétition internationale afin d'atteindre un consensus scientifique autour de la cryptographie post-quantique. Parmi les vingt-six soumissions finalistes basées sur des critères comme la sécurité, les performances et les caractéristiques de l'implémentation, sept sont le résultat des travaux d'équipes projets françaises Inria [142]. Pour cette entité, les données les plus sensibles devront être rechiffrées dès que les algorithmes seront disponibles. Pour traiter l'ensemble des données, le NIST évoque une durée de l'ordre de vingt ans.
Pour l'ANSSI, la cryptographie post-quantique est "la voie la plus prometteuse pour contrecarrer la menace quantique". La cryptographie post-quantique, désigne l'en- semble des méthodes visant à garantir la sécurité de l'information face à un calculateur quantique. Il s'agit d'une famille d'algorithmes cryptographiques qui comprend l'établissement de clés

et de signatures numériques qui assurent une sécurité même contre un attaquant équipé d'ordinateurs quantiques. Ces algorithmes peuvent être exécutés sur des ordinateurs classiques avec des canaux de communications classiques. Ils peuvent donc être déployés par anticipation sur des infrastructures existantes [141].

A ce jour, l'ANSSI n'approuvera aucun remplacement direct des algorithmes actuellement utilisés à court/moyen terme car la cryptographie post-quantique est encore trop immature. Ainsi, elle privilégie de mettre en place des mécanismes hybrides, combinant "des mécanismes asymétriques éprouvés" (vulnérables aux attaques exécutées par un ordinateur quantique) avec "des mécanismes asymétriques" supposément résistants à l'ordinateur quantique. Les développeurs de systèmes devant protéger des informations au-delà de 2030 devraient considérer l'adoption de telles mesures et préparer les moyens d'une migration de leurs mécanismes cryptographiques. Les recommandations de l'ANSSI seront étudiées dans le §2.
Le rôle de l'Agence nationale de la sécurité des systèmes d'information devra être prépondérant pour guider les organisations les plus sensibles (les ministères et les Opérateurs d'importance vitale). Elle a déjà publié un guide de sélection d'algorithmes cryptographiques [143], mais la tâche d'accompagner les acteurs pour sécu- riser leurs informations est considérable.

ELABORER UN PLAN DEFENSIF SOUS L'EGIDE DE L'ANSSI

Bien qu'aucun ordinateur quantique ne soit actuellement assez puissant pour rendre réellement obsolète les mécanismes actuels de protection, il convient de se préparer au mieux à cette menace. Elles préconisent aux développeurs de systèmes devant protéger des données au-delà de 2030 de préparer les moyens d'une migration des mécanismes cryptographiques. Une adaptation des critères de délivrance des visas de sécurité est également envisagée par l'ANSSI.
S'il est encore difficile d'anticiper la date d'arrivée sur le marché d'un ordinateur quantique opérationnel et en capacité d'effectuer de telles opérations, l'ANSSI estime qu'il est plus prudent de travailler dès maintenant à la mise au point et l'adoption de nouveaux protocoles post-quantiques ou résistants à l'ordinateur quantique. Cela permettra aussi d'empêcher des attaques dites rétroactives qui visent à enregistrer les données maintenant pour les déchiffrer plus tard, quand la technologie sera à disposition.

Une feuille de route pour la transition post-quantique

Au niveau national, l'ANSSI recommande de déployer, à court terme (sous 1 à 4 ans) des solutions dites hybrides qui ajoutent une surcouche de protection post- quantique aux méthodes de cryptographie classiques actuelles. Cette solution permet de protéger les données des attaques classiques, de mettre à l'épreuve des méthodes post-quantiques et surtout d'éviter toute régression de sécurité. Elle concerne principalement les données demandant une protection de longue durée, au-delà de 2035.

Ces recommandations affecteront la délivrance des visas de sécurité. L'ANSSI ex- plique qu'elle adaptera ses modalités d'évaluation. La dernière phase, lors de laquelle l'agence délivrera des visas de sécurité revendiquant une assurance de sécurité pré- quantique à long terme avec hybridation facultative, dépend fortement des avancées de la recherche. Les spécificités de cette phase seront adaptées au cours des pro- chaines décennies.

Pour accompagner une transition progressive, l'ANSSI encourage la feuille de route en trois phases [141] (Figure 17) :

- Phase 1 (aujourd'hui) : hybridation pour fournir une défense en profondeur post-quantique supplémentaire à l'assurance de sécurité pré-quantique.
- Phase 2 (au plus tôt en 2025) : hybridation pour fournir une assurance de sécurité post-quantique tout en évitant toute régression de sécurité pré-quantique.
- Phase 3 (probablement pas avant 2030) : cryptographie post-quantique autonome facultative.

Ces recommandations évolueront nécessairement en fonction des avancées mondiales sur la cryptographie post-quantique et de l'avancement de la campagne de normalisation du NIST. Le calendrier estimé de la feuille de route pourrait être avancé ou ralenti en conséquence.

En tant qu'autorité nationale de cybersécurité en France, l'ANSSI a suivi de près les progrès de la cryptographie post-quantique. Elle publie des recommandations générales sur le choix des algorithmes cryptographiques dans les produits de sécurité [143] et délivre des labels de sécurité pour les produits répondant aux exigences générales de sécurité [144]. Elle a donc un double rôle en matière d'utilisation des algorithmes cryptographiques : consultatif et réglementaire. Mais l'ANSSI n'est pas une agence de normalisation, son rôle n'est pas d'élaborer des normes cryptographiques. Elle recommande des mécanismes cryptographiques [145].

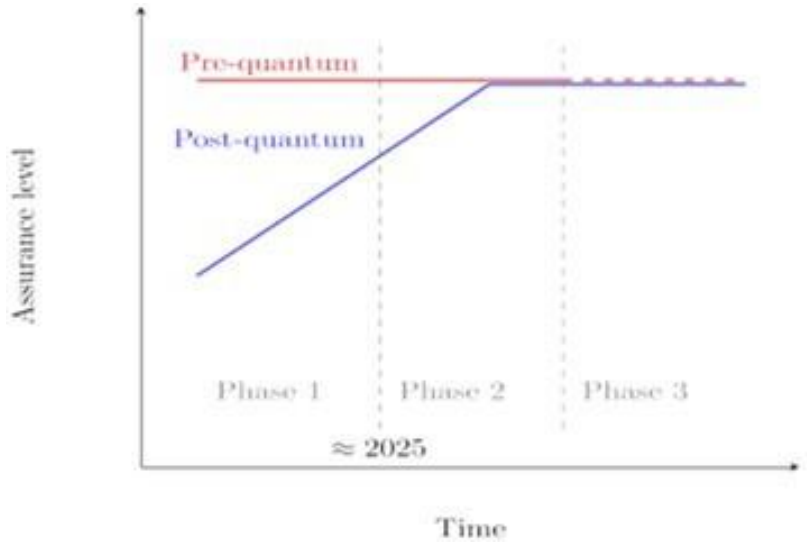

Figure 17 – Feuille de route selon l'ANSSI

Un rapprochement inévitable ANSSI – R&D : le projet "RISQ"

L'ensemble des acteurs de la sécurité est aujourd'hui confronté à de nouveaux défis en vue de standardiser ces nouveaux algorithmes post-quantiques. A l'initiative de l'ANSSI, le projet RISQ[25] est un projet national à visée industrielle dont l'objectif est de préparer l'industrie Française au basculement post-quantique [146]. Ce projet a pour but de faire de la France un acteur international majeur de la transition post-quantique. Un des objectifs de RISQ est de renforcer la présence de la filière française de la sécurité numérique au sein des organismes de standardisation en rassemblant les acteurs nationaux aux compétences reconnues internationalement, incluant de grands groupes industriels, des PME/ETI, des services étatiques, et des laboratoires académiques, afin de concerter leurs actions de

propositions de standards et d'évaluation des candidatures. En interaction avec ce processus, le projet définit une feuille de route pour la commercialisation de gammes de produits de sécurité post-quantique, librairies de calculs cryptographiques logicielles et matérielles, serveurs d'archivage, d'horodatage, etc. allant de la conception des briques théoriques par les laboratoires partenaires au développement de démonstrateurs et leur validation.

La présence de grands groupes au sein du consortium est garante de l'adaptabilité des solutions développées aux systèmes déployés à l'heure actuelle.

Le projet RISQ rassemble au sein d'un consortium de quinze partenaires : les acteurs majeurs de la recherche académique, du monde industriel et des partenaires institutionnels [146]. On y retrouve entre autres Airbus Group, l'Agence Nationale de la Sécurité des Systèmes d'Information, le Commissariat à l'énergie atomique et aux énergies alternatives, CryptoExperts, C&S Communication & Systèmes, l'Ecole Normale Supérieure, Gemalto, Inria Paris, Inria Rhônes Alpes, le Laboratoire IRISA, LIP – ENS de Lyon, Orange, Paris Center for Quantum Computing, Secure-IC, Thales Communications & Security, l'Université de Versailles-Saint-Quentin-en-Yvelines. Ainsi le projet RISQ prévoit que les acteurs français, en regroupant leurs compétences fortes, prennent part à l'élaboration des normes, développent en amont la technologie et la propriété intellectuelle nécessaires, évaluent et mettent en place des processus de migration, de sorte que l'industrie française soit réactive face à ce changement technologique. Actant le caractère capital que revêt le projet, plusieurs grands industriels ont souhaité y prendre part même sur fonds propres. Si les technologies quantiques font peser des menaces certaines sur notre sécurité, elles amènent également de nombreuses opportunités pour la renforcer et la rendre plus offensive. C'est le choix opéré par les armées françaises.

-

24. RISQ : Rassemblement de l'Industrie française pour la Sécurité post-Quantique

UNE STRATEGIE OFFENSIVE POUR LES ARMEES : EXPLOITER LE POTENTIEL

Comme l'a rappelé le Président de la République Emmanuel Macron à l'occasion de son discours sur la stratégie de défense et de dissuasion à l'École militaire, le 7 février 2020 : *"l'émergence de nouvelles technologies, comme les applications de la physique quantique, est porteuse de nombreuses opportunités, mais également source de futures instabilités"* [147]. Même si les principes quantiques font déjà l'objet d'applications très utiles comme la communication, la détection ou de calcul, les progrès de la recherche ces dernières années laissent entrevoir une nouvelle génération d'applications disruptives qui donneront à ceux qui la maîtriseront un avantage certain notamment dans le domaine militaire. Dans ce domaine, les ruptures technologiques en matière de détection, de communication et de calcul sont, d'ores et déjà, une certitude. Seule subsiste une incertitude sur le calendrier. La physique quantique recèle ainsi le potentiel pour fournir la supériorité opérationnelle dont toutes les armées modernes sont en quête permanente. Conscientes de cette réalité, les grandes puissances engagent des moyens considérables dans la recherche (France 1,8 milliard sur cinq ans [148] / Israël 1,25 milliard de shekels sur cinq ans [149] / Chine 50 milliards de dollars [150] / USA 2,2 milliards de dollars [151]) . L'Europe s'efforce de suivre le tempo car attendre placidement n'est pas une option. Dans ce cadre, la France s'est dotée d'une feuille de route quantique interministérielle [152]. Il appartient au ministère des Armées de développer son propre plan d'action « technologies quantiques » pour permettre aux armées de faire leur révolution quantique à l'horizon 2040.

On le comprend assez vite, les technologies quantiques sont un intérêt stratégique et vital pour les armées françaises. Le 4 janvier 2022, la ministre des Armées Florence Parly participait au lancement d'une nouvelle plateforme nationale de calcul quantique installée au sein du CEA (direction des applications militaires).
Pour la ministère des Armées, la technologie quantique est *"la mère"* de toutes les ruptures technologiques. Elles *"présentent un intérêt absolument stratégique pour la protection des Français"* [153].
Parce que les armées doivent envisager l'avenir en s'appropriant ces technologies disruptives (§1), elles investissent massivement aux côtés de startups pour devenir leader sur la scène internationale dans le domaine militaire (§2).

PROSPECTIVE : QUELLES PRIORITES STRATEGIQUES POUR LES ARMEES ?

Considérant le potentiel des technologies quantiques et l'engouement des États pour s'en doter, nul doute que la nature disruptive de ces technologies conférera un avantage stratégique à ceux qui les maîtriseront, ce qui induit d'indéniables enjeux d'autonomie et de souveraineté notamment. Dans le domaine de la sécurité et de la défense, elles sont de nature à générer de nouveaux modes d'actions, ou bien elles amélioreront des modes d'actions existants. Dans les deux cas, elles confèreront une avance significative et un avantage opérationnel décisif. Les applications quantiques recèlent le potentiel pour donner une supériorité opérationnelle décisive à une force militaire. L'utilisation des propriétés quantiques provoquera un bouleversement des méthodes et des capacités militaires dans des domaines aussi variés que les communications et la détection.

Depuis 2020, le quantique est une des priorités de la stratégie française d'innovation de

défense. Trois domaines à fort enjeu pour les armées sont identifiés : les capteurs quantiques, les communications et le calcul quantique [153].
Si les deux premiers vont être abordés dans cette partie du mémoire, le calcul quantique sera traité dans le cadre des investissements portés par les armées dans ce domaine bien particulier.

La communication quantique pour lutter contre les cyberguerres étatiques
Les cyberattaques soutenues par les États sont de plus en plus nombreuses et joueront un rôle important dans les conflits internationaux. Pourquoi un ennemi utiliserait-il seulement des armées humaines alors qu'il peut nuire à l'infrastructure critique d'une nation avec un ordinateur ou des millions d'ordinateurs lors d'une attaque coordonnée ? Ces cyberguerres obligent les armées à réfléchir aux armes disruptives de demain.
L'un des premiers thèmes qui cristallise l'attention est la communication dite quantique. Ainsi, le ministère des Armées a développé des équipements de très haut niveau de sécurité pour protéger, pendant plusieurs dizaines d'années, des données stockées ou échangées. Les algorithmes de chiffrement utilisés aujourd'hui apportent un premier niveau de sécurité contre la menace que représenterait l'apparition d'un ordinateur quantique mais cela ne sera pas suffisant tant l'évolution de la technologie est incommensurable.

L'intérêt des communications quantiques réside dans le fait qu'elles pourraient per- mettre de communiquer des données de manière ultra-sécurisée, voire totalement impossible à pirater.
La première application des communications quantiques est la distribution quantique de clés (QKD), qui consiste à échanger des clés cryptographiques par l'intermédiaire de particules quantiques. L'information elle-même est transmise via l'infrastructure de communication habituelle et sous la forme de bits traditionnels, mais les clés cryptographiques nécessaires pour la déchiffrer sont transmises séparément et au moyen de particules quantiques [154].

Une révolution dans la détection : les capteurs quantiques
La détection quantique fait référence à la capacité d'utiliser la mécanique quantique pour construire des capteurs extrêmement précis. Il s'agit de l'application de la technologie quantique considérée comme ayant le potentiel opérationnel à plus court terme.
Les capteurs quantiques sont des applications prometteuses dans le domaine de la défense : navigation, interception, détection, sismographie, etc. Les capteurs quantiques sont sur le point de fournir des niveaux de précisions inégalées. Ils permettront par exemple, d'améliorer considérablement les performances de détection des systèmes d'armes ou encore de pouvoir disposer de systèmes de navigation de très haute précision. Concrètement, pour l'utilisateur, cela reviendrait à un GPS qui ne dépendrait plus des signaux en provenance des satellites. Un GPS capable de déterminer où les bâtiments de la marine se trouvent, même pendant des missions de très longue durée, et qui se repérerait non pas à l'aide des signaux envoyés par les satellites, mais en mesurant par exemple les infimes variations de la gravité terrestre. A cet effet, la marine française pourrait devenir la première marine au monde à être équipée de systèmes opérationnels basés sur une technologie quantique. Elle sera dotée à l'horizon 2026/2027 du système GIRAFE [26] développé par la société française ONERA [155].

Grâce aux technologies quantiques capables de mesurer des variations infimes de la gravité terrestre, les sous-marins de la dissuasion nucléaire pourraient s'affranchir à l'avenir des

signaux satellitaires GPS pour se localiser [156].
D'autres applications de détection sont également envisagées, à plus court terme. On parle d'antennes RF (Radio Fréquence) miniaturisées pour la réception, mais aussi des systèmes d'imagerie 3D qui pourraient être utiles pour la cartographie des fonds marins, mais aussi d'installations souterraines. Les systèmes envisagés per- mettraient une détection y compris par temps de brouillard ou en zone poussiéreuse ou encore dans des environnements complexes, comme les jungles. La détection de tirs par procédé photo acoustique pourrait également être beaucoup plus précise.

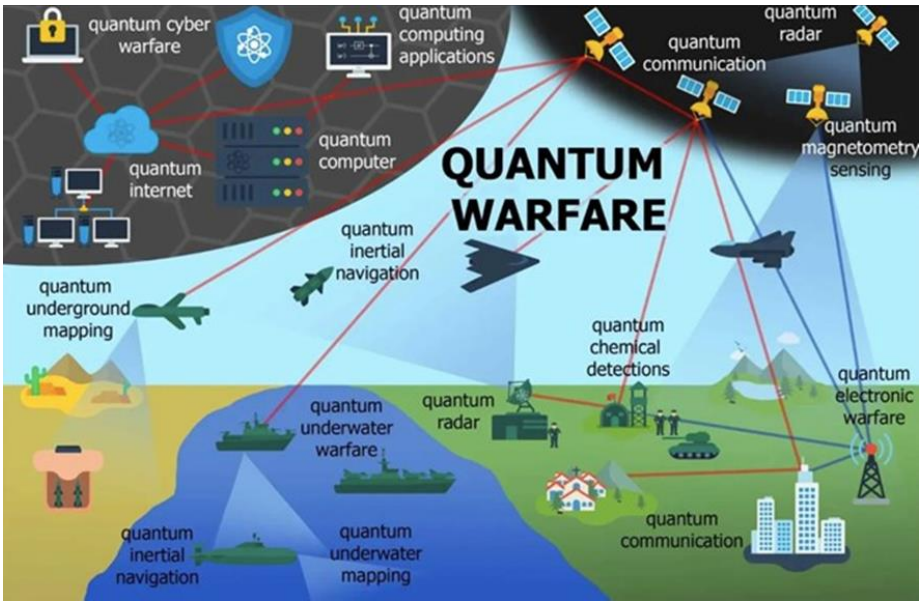

Figure 18 – La guerre quantique

INNOVER : L'INVESTISSEMENT DES ARMEES DANS DES APPLICATIONS DE DEFENSE HAUTEMENT STRATEGIQUES

Beaucoup d'espoirs sont placés dans ces technologies de calcul quantique. En théorie, elles devraient permettre de réaliser des calculs aujourd'hui inaccessibles pour des processeurs classiques. Pour le ministère des Armées, cette capacité de calcul phénoménale serait un véritable atout pour prolonger les travaux extrêmement sensibles menés dans le domaine de la dissuasion par la direction des applications mi- litaires du CEA, mais aussi dans les combats de demain. Elle pourrait traiter en un temps record des milliards de données, par exemple à des fins de renseignement. Elle permettrait également d'améliorer l'efficacité des systèmes composés de milliers de véhicules ou de satellites, en optimisant l'ensemble des trajectoires tout en tenant compte de leurs dynamiques individuelles [153].
C'est pourquoi les armées se sont pleinement engagés dans la création d'une plateforme nationale de calcul quantique. Cette plateforme hébergera des ordinateurs quantiques qui seront mis à la disposition d'une très large communauté de chercheurs, de scientifiques et de startups. A travers cette plateforme c'est la construction d'une filière quantique souveraine qui se dessine. La supériorité opérationnelle des armées, c'est-à-dire la capacité à garder l'avantage sur le terrain, dépend étroitement de la souveraineté technologique française [157].

Une plateforme nationale de calcul quantique pour une indépendance et une supériorité stratégiques

Cette plateforme nationale de calcul quantique s'inscrit dans la stratégie nationale. Il est à noter que cette plateforme est installée dans un site militaire au Très Grand Centre de Calcul du CEA - direction des applications militaires [158]. Le ministère des Armée y a investi 50 millions d'euros pour développer les technologies quantiques sur la période de la loi de programmation militaire (LPM) 2019-2025.

Cette technologie est vitale et décisive pour les armées car elle permet une capacité de calcul phénoménale, qui est un véritable atout par exemple pour poursuivre les travaux extrêmement sensibles menés dans le domaine de la dissuasion militaire.

A pleine maturité, il permettra d'effectuer des calculs jusqu'à 1 milliard de fois plus vite qu'une technologie de calcul classique, ce qui ouvre la voie à la résolution de problèmes actuellement non solubles dans un temps humain. Avec un premier investissement de 70 millions d'euros pour un objectif total de 170 millions cette plateforme interconnectera systèmes classiques et ordinateurs quantiques [157].

De manière très simplifiée, les calculs actuels fonctionnent actuellement sur une base de bits élémentaires, capables de se trouver dans deux états distincts : 1 ou 0. Avec la physique quantique, les opérations sont cette fois basées sur des qubits, qui pourront adopter plusieurs états à la fois. C'est cette superposition d'états, et donc de possibilités, qui devrait permettre une puissance de calcul démultipliée. Appliquée à des cas concrets, la technologie quantique permettra de développer des algorithmes aux possibilités inédites.

Des investissements militaires dans la French Tech quantique

La startup française Pasqal qui est en train de développer un ordinateur quantique a levé 25 millions d'euros en 2021 auprès du fonds d'investissement spécialisé dans le quantique Quantonation et du nouveau fonds d'investissement du ministère des Armées français. C'est le premier investissement du ministère des armées pour sou- tenir des technologies cruciales pour la souveraineté française. Dotée d'une équipe de chercheurs des plus renommées au monde, Pasqal comptera à l'avenir parmi les leaders des calculateurs quantiques. Cette technologie permet de réaliser des calculs d'une puissance inédite et pourrait révolutionner les capacités opérationnelles des armées. Les applications pour la défense sont multiples et hautement stratégiques. Les ordinateurs quantiques reposent sur l'exploitation de propriétés surprenantes et parfois contre-intuitives de la matière au niveau de l'infiniment petit, atomes, photons, ou électrons. Leurs capacités théoriques sont immenses pour certains types de calculs (l'objectif est d'atteindre 1000 qubits dans les années à venir), et pourraient révolutionner l'informatique, mais pour l'instant, la technologie est encore balbutiante.

Bien qu'il s'agisse du premier investissement de ce nouveau fonds, le ministère des Armées s'est distingué ces derniers mois par plusieurs rapprochements avec des star- tups. Earthcube [159] (technologie de renseignement) et Unseenlabs [160] (lutte contre la délinquance en mer) bénéficient d'un soutien financier et technologique du ministère. Par ailleurs, celui-ci a débloqué une enveloppe de 10 millions d'euros pour dénicher les solutions les plus prometteuses face à a crise sanitaire, qui avait profité à une trentaine de projets.

25. GIRAFE : Gravimètres Interférométriques de Recherche à Atomes Froids Embarquables

De toutes les vagues technologiques, l'informatique quantique pourrait bien se révéler la plus puissante. Et comme pour l'intelligence artificielle, les Américains et les Chinois ont pris de l'avance. Face à eux, il faut que la France maîtrise aussi cette technologie de rupture pour rester dans la course, développer un écosystème fort et préserver sa souveraineté.

CREATION D'UN FUTUR ECOSYSTEME EUROPEEN QUANTIQUE : QUELLES PERSPECTIVES ?

Au niveau européen, et bien que l'engouement international soit encore très localisé outre-Atlantique, de nombreux travaux de recherche ont été initiés, comme "Open- SuperQ" qui réunit des équipes de chercheurs et de développeurs d'Allemagne, d'Es- pagne, de Suède, de Suisse et de Finlande [161]. Plusieurs fonds d'investissement ont été débloqués à cette fin. La collaboration d'institutions d'au moins trois pays différents est par exemple une des conditions d'accès aux financements du programme européen "Flagship Quantique" [162].
Quid de la France sur cette thématique ? Côté français, la recherche est active et de qualité. A titre d'exemple, le projet de recherche "Quantum Silicon" à Grenoble réunit les chercheurs de trois laboratoires français (CEA-IRIG [163], CNRS-Institut Néel [164] et CEA-Leti [165]) autour de la composition de processeurs quantiques basés sur du silicium.
A ce jour, la France occupe la troisième place mondiale des nations les plus performantes et compte cinq établissements parmi les cent premiers [166]. Elle reflète ainsi une tradition française d'excellence.
Rappelons que le Président de la République Emmanuel Macron, a émis le souhait à travers le plan quantique d'organiser les forces industrielles et de recherche du pays pour faire de la France un acteur majeur des technologies quantiques.
Il n'est pas trop tard. La France a une carte à jouer. La technologie est encore embryonnaire et elle dispose d'une recherche à la point en la matière. Elle doit pour se faire développer un écosystème riche et divers de laboratoire de recherche, grands groupes, startups et fonds d'investissement pour décoller et faire émerger des solutions opérationnelles (1ère partie). La France doit également maîtriser la technologie et sortir des premières applications industrielles concrètes (2nd partie).

UN ECOSYSTEME JEUNE MAIS DEJA RICHE …

Comme toutes les technologies récentes, l'informatique quantique nécessite la mobilisation d'un écosystème riche et divers : recherche, développement, financement, commercialisation, tous les acteurs doivent être mobilisés pour faire émerger des solutions opérationnelles, avec un véritable impact global. La technologie étant encore en phase de recherche et développement, les laboratoires et universités sont des acteurs clés de l'écosystème quantique.
Pour relever ce défi, le plan quantique permet de structurer les forces vives du pays sur le domaine des technologies quantiques et des technologies dites "habilitantes" nécessaires à la mise en œuvre des futurs systèmes quantiques (notamment matériaux de pointe). Les technologies quantiques sont encore à ce stade une question de recherche fondamentale. C'est pourquoi l'État a fait le choix de s'entourer des trois grands opérateurs de recherche français concernés. Un véritable groupe de travail composé entre autres du CNRS, du CEA

et de l'Inria [152] pour définir la stratégie quantique française. Grâce à ce tissu de laboratoires qui maille le territoire national et à son approche pluridisciplinaire alliant recherche fondamentale, innovation et transfert technologique, cet écosystème est en passe de représenter un atout français majeur pour répondre efficacement aux défis des technologies quantiques et positionner la France au plus haut niveau de compétition internationale.
Challengée par une technologie disruptive, la R&D veut créer une communauté quantique forte et robuste (§1) en vue de promouvoir le savoir-faire français et de préserver la souveraineté nationale (§2).

CREER UNE COMMUNAUTE DE R&D QUANTIQUES FORTE ET ROBUSTE

La fonction R&D développe des innovations. A ce titre, elle regroupe l'ensemble des processus qui, partant de la recherche fondamentale ou d'une invention, assurent sa faisabilité industrielle.
La R&D englobe ainsi les trois champs classiques de la recherche : recherche fondamentale, recherche appliquée et développement expérimental. Elle nécessite pour se faire de très nombreux capitaux. Le plan quantique est venu préciser les fonds dédiés et la répartition entre fonds publics et fonds privés (cf. Chapitre 1). Pour remplir ses fonctions, la R&D s'appuie sur des réseaux technologiques, scientifiques et académiques.

Les laboratoires et centres de recherches

La France compte plusieurs dizaines de laboratoires dans le quantique (Figure 19), presque tous des UMR du CNRS (Unités Mixtes de Recherche associées à des Universités) ou des laboratoires du CEA et de l'Inria. Un état des lieux des compétences en technologies quantiques a été cartographié [167].

Dans ces centres de recherches, on trouve les doctorants, post-doctorants, chercheurs et enseignants-chercheurs. La majorité d'entre eux planchent sur la physique quantique fondamentale et expérimentale. Certains se rapprochent de l'informatique quantique dans ses grandes branches : calcul et simulation, télécommunications et cryptographie et enfin, métrologie.

Figure 19 – La recherche quantique en France

Pour relever les grands défis présents et à venir, ces acteurs clés de la recherche et de l'innovation se mettent en ordre de bataille pour permettre à la France de rayonner à l'international et se hisser sur les podiums des challenges que le monde offre. Excellence, liberté de recherche, transdisciplinarité et valorisation des résultats sont autant de valeurs portés par ces chercheurs et développeurs.

Les réseaux académiques

L'université Paris-Saclay, lieu de savoir et de science, comporte un centre en sciences et technologies quantiques appelé "Quantum". Cette université regroupe près de 13% de la recherche française. Elle s'est hissée au 13ème rang du classement de Shan- ghai ranking 2021, a gravi la toute première marche du podium en mathématiques [166]. Elle regroupe 275 laboratoires avec les organismes de recherche, 48000 étudiant et 9000 enseignants / chercheurs. Elle joue un rôle majeur dans le domaine des sciences et technologies quantiques en France et dans le monde. Plus de 80 équipes de recherches contribuent au meilleur niveau international, aussi bien dans les laboratoires académiques que chez les industriels du campus, dans tous les domaines stratégiques et technologies quantiques [27].

Ces chercheurs sont impliqués dans des enseignements de haut niveau aussi bien en physique quantique qu'en ingénierie. Paris-Saclay a développé un partenariat académie-industrie très fructueux de longue date et a vu naître plusieurs des star- tups de la seconde révolution quantique.

Aux côtés de ce mastodonte académique, on retrouve le projet SIRTEQ financé par la région Ile-de-France. Porté par le CNRS, le projet "Sciences et ingénierie en Région pour les technologies quantiques" (SIRTEQ) a été labellisé Domaine d'Intérêt Ma- jeur (DIM) en 2018. SIRTEQ a pour objectif de développer de nouveaux moyens de traiter l'information ou de faire des mesures ultraprécises, en utilisant de nouveaux supports physiques – des supports quantiques, et non plus classiques. Il poursuit quatre axes dont celui du calcul

et informatiques quantiques. SIRTEQ regroupe 349 chercheurs et enseignants chercheurs, 270 doctorants, 109 post-doctorants, 106 équipes de recherche, 32 laboratoires, 5 communautés d'universités et établissements (Paris Sciences et Lettres, Sorbonne Universités, Université Paris Saclay, U. Paris Seine, U. Sorbonne Paris Cité), 728 chercheurs permanents et non permanents ré- partis dans 105 équipes qui couvrent les grandes thématiques de recherche en technologies quantiques.

PROMOUVOIR LE SAVOIR-FAIRE FRANCAIS ET PRESERVER LA SOUVERAINETE NATIONALE

Dans la présentation du plan quantique, le président de la République a donné les grands axes. Un des objectifs annoncé comme essentiel par l'autorité est de donner un grand coup d'accélérateur aux formations, aux recherches scientifiques et aux expérimentations technologiques, tout en renforçant les chaînes de valeur industrielles.
Ainsi, la stratégie des universités doit résider dans la promotion des formations en physique quantique de la licence au doctorat. L'attractivité des talents est également centrale dans la vision étatique.

Valoriser les acquis et fidéliser les talents

En plus de l'augmentation significatives des offres de formations liées au quantique, la qualité des enseignements doit faire l'objet d'investissement car il s'agit là d'un atout indéniable pour attirer les volontaires et les talents.
A ce titre, l'Etat continue à investir massivement dans les formations en insistant sur l'interdisciplinarité et en créant de nouvelles formations. Il est ainsi envisagé dans le plan quantique cent bourses de thèses, cinquante post-docs et dix bourses de jeunes talents en plus par an et ce pendant cinq ans au moins.

Côté formation initiale, les sites académiques s'organisent également. L'université de Grenoble Alpes lance un nouveau master 2 international "Quantum information
- quantum engineering" (QuEnG) dont la première promotion a fait sa rentrée en septembre 2022 [168]. L'idée est de préparer la prochaine génération de jeunes chercheurs et chercheuses déjà formés à l'interdisciplinarité actuellement développée au niveau du doctorat. L'année de recherche en technologies quantiques "Arteq", ouverte par l'Université Paris-Saclay et l'ENS Paris-Saclay depuis 2020 est passé de dix étudiants pour la première promotion à trente pour la seconde [169].
La France est le deuxième pays le plus touché au monde par la fuite des cerveaux (Figure 20). Elle a ainsi un solde négatif de 130 000, alors que les Allemands ont un solde positif de 374 000 [170]. Cela crée donc un paradoxe que le Président de la République Française dans son discours sur la stratégie quantique veut voir inverser.

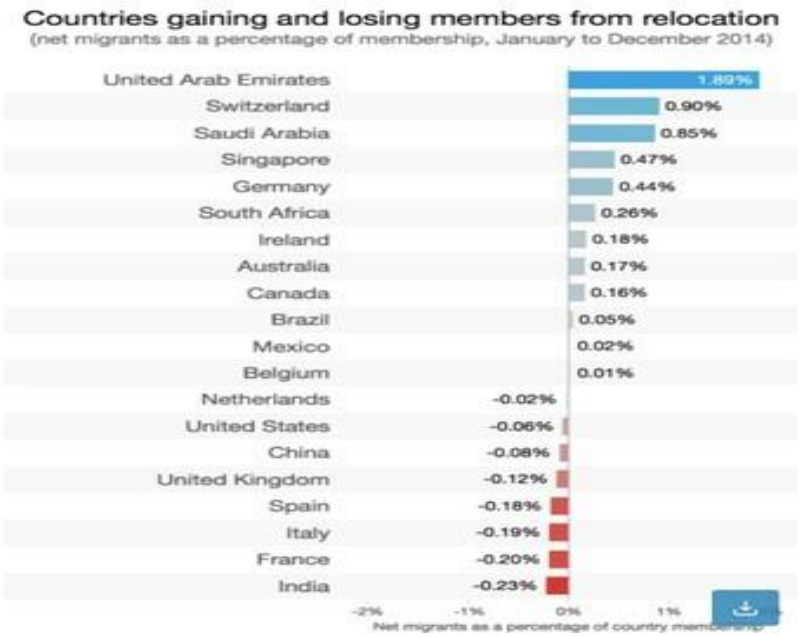

Figure 20 – Fuite des cerveaux

26. Font partis du Quantum Paris-Saclay : L'Université de Paris-Saclay, le CNRS, le CEA, IN- RIA, ONERA, Institut polytechnique de Paris, UVSQ, Faculté des sciences d'Orsay, Centrale SUPELEC, Ecole normale SUP et Institut d'optique Paris TECH.

L'État fait face à des enjeux majeurs technologiques et scientifiques. Il doit alors pour les résoudre s'entourer de talents capables d'avoir des approches transsectorielles et/ou transdisciplinaires. Dès lors, il ne fait guère de doute qu'il doit se doter des compétences nécessaires afin de relever ces défis de taille.
Pour être attractif, l'écosystème académique quantique doit valoriser les potentiels et la carrière, laisser libre cours à la recherche, à l'innovation, former, challenger et accompagner les talents sur le long terme. Lors de son discours à Paris-Saclay en Janvier 2021, le président Emmanuel Macron a déclaré que la France allait *"continuer d'y investir. Nous formons des femmes et des hommes de talent qui font vivre notre système de recherche et d'innovation quantique"* [171].

Préserver la souveraineté nationale dans le domaine du quantique
Le plan quantique entend assurer la souveraineté nationale face notamment aux États-Unis et à la Chine qui investissent massivement, mais aussi face aux géants du numérique (comme Google ou IBM) dont les efforts de recherche se multiplient avec des budgets conséquents et des premiers résultats.
La stratégie quantique réside dans la mise en place par le gouvernement d'une sécurisation de toute la chaîne : en matière de recherches, en matière technologique et en matière industrielle. Il faut garder les talents, garder certaines technologies pour ne pas dépendre des deux grandes puissances internationales qui concurrencent la France. Il faut ainsi préserver et jalousement garder chaque maillon de cette chaîne.
Qu'il s'agisse de la recherche fondamentale, de la recherche technologique appliquée au secteur privée, il faudra également accompagner cette stratégie d'une forme de veille, d'une volonté d'investir pour accompagner et maîtriser cette chaîne de valeur. C'est la clé pour garder une recherche libre en permanence et pour la souveraineté de la France en matière de savoirs et d'application industrielle [96].

Les technologies quantiques seront clés dans les secteurs régaliens de la défense et de la sécurité. La maîtrise des ordinateurs et des communications quantiques seront des ressources majeures pour bâtir des infrastructures sécurisées et se doter de puissances de calculs sans précédent. Il faudra pour cela se mettre en capacité de maîtriser toute la chaîne de valeur : les matériaux, la construction des composants, les applications. L'enjeu est donc colossale mais ô combien essentiel pour ne pas dépendre des États-Unis ou de la Chine à travers le moindre composant.

UN FORT ENGAGEMENT DES INDUSTRIELS

Comme nous l'avons présenter dans le chapitre précédent, le marché de l'informatique quantique est bien là et est évalué à 1000 milliards de dollars d'ici 2035. La course industrielle est donc bel et bien lancée. D'ici 2030, il existera entre deux milles et cinq milles ordinateurs quantiques dans le monde [72]. Plusieurs entrepreneurs spécialisés dans la technologie se sont ainsi en- gagés avec pour objectif de concevoir le premier ordinateur quantique évidemment le plus puissant au monde. Cette ruée vers un futur disruptif est portée depuis quelques années par un écosystème industriel constitué de grands groupes et de startups. L'industrie française est actuellement dans la course sur plusieurs applications liées au quantique.
C'est une véritable effervescence qui se crée autour des possibilités de découvertes et d'applications de l'informatique quantique dans des secteurs variés comme la finance, la cryptographie et même le développement des objets connectés. On y retrouve par exemple

les simulateurs quantiques de la société "Atos" dont la plateforme a permis dès 2016 de transformer les développeurs informatiques à des langages et des algorithmes radicalement nouveaux. La France est également très bien positionnée sur la cryptographie post-quantique. Les appels à projets Américains le prouvent : un quart d'entre eux implique l'Inria. Et surtout, nous constatons un écosystème de startups en cours de structuration grâce à l'appui de du fond Quantonation. La France compte à ce jour une trentaine de startups spécialisés dont les plus connus sont Quandela, Pasqal, Cryptonext, Very Cloud, Alice & Bob.
Force est de constater que la R&D peut s'appuyer sur des industriels catalyseurs de projet (§2) et sur une croissance exponentielle de startups spécialisées en informatique quantique (§2)

DES INDUSTRIELS CATALYSEURS DE PROJET

L'appui des industriels est indispensable pour progresser sur les questions de recherche qui sont au cœur des technologies quantiques. Les grands groupes industriels jouent ainsi un grand rôle dans le développement du quantique. Très engagés et particulièrement challengé sur le sujet, plusieurs n'ont pas attendu pour mettre en place leurs propres équipes de recherche ou financer des projets de recherche quantique appliquée en collaboration avec des laboratoires ou des startups [172].

Des engagements concrets qui n'ont pas attendu le plan quantique pour se mettre en ordre de bataille

Certains secteurs économiques, en particulier celui des transports, de l'aviation, des télécommunications et des énergies, sont plus sensibles à la recherche sur l'informa- tique quantique. Ainsi dès 2015, la société Airbus a missionné une équipe dédiée au sein de la Airbus Defense & Space Unit. Le géant de l'aéronautique collabore avec QC Ware (USA), startup du logiciel quantique. L'objectif est d'utiliser l'ordinateur quantique pour de l'optimisation, et la simulation quantique pour créer des matériaux ultradurables [173].
Atos, acteur de pointe sur le développement de l'informatique quantique a lancé en 2016, le programme "Atos Quantum". En juillet 2018, la compagnie a rendu public l'émulateur Atos Quantum Learning Machine (QLM), premier système industrialisé et prêt à l'emploi capable d'émuler jusqu'à quarante et un qubits sur des processeurs Intel classiques [174].
Thales n'est pas en reste et mise pour sa part sur la recherche pour prévenir la "crypto-apocalypse" [175].
Dans le secteur de l'énergie, Total collabore avec Atos (QLM), pour combattre le changement climatique grâce aux algorithmes quantiques [176]. De la même manière, EDF a lancé en 2018 un projet dédié. Le projet PASQuanS, qui vise à développer un simulateur quantique (hardware et software), et qui fait partie des projets soutenus par le Flagship européen, s'assure de l'application concrète de la technologie développée par l'intermédiaire d'un comité de l'utilisateur final où siègent Airbus, Bosch, EDF, Siemens et Total [177].

Un investissement massif pour participer au rayonnement de la France

Comme indiqué dans son discours de Paris-Saclay, l'action de l'État sera complétée par le cofinancement des industriels. Leur implication sera déterminante pour le succès de la France en la matière.
La compétition internationale très rude, dans le domaine quantique, avec des concurrents tels que les géants Américains Amazon, IBM ou Google oblige les startups Françaises à mettre la barre très haute concernant les résultats expérimentaux à atteindre, et donc à recruter

des théoriciens et des ingénieurs de niveau très élevé ainsi que du matériel quasiment conçu sur-mesure et des consommables très onéreux.
L'année 2022 a été annoncée comme exceptionnelle en termes de levée de fonds par les startups Françaises. Dans le domaine des innovations quantiques, Alice & Bob a levé 27 millions d'euros en 2022, un record après celui de Pasqal de 25 millions d'euros en 2021.
L'écosystème de l'entrepreneuriat Français lié à l'univers quantique démontre des caractéristiques spécifiques, en particulier au niveau des montants requis des investissements très importants. S'ajoutent aux levés de fonds, les fonds privés issus de Venture Capitalists comme Bpifrance et Quantonation ainsi que les Business Angels. Ces derniers sont des particuliers, anciens chefs d'entreprise à la tête d'un patrimoine important et dotés d'une grande expérience entrepreneuriale.

Sur l'enveloppe de 1,8 milliard du plan quantique, 350 millions iront au développe- ment de simulateurs quantiques et 430 millions à celui de l'ordinateur quantique. Le solde financera les travaux autour des capteurs, des communications et de la cybersécurité à l'ère de cette technologie.

UNE FRENCH TECH QUANTIQUE EN EBULLITION QUI FAIT DES ENVIEUX

L'année 2021 a été annoncée comme exceptionnelle en termes de levée de fonds par les startups Françaises. La compétition internationale très rude dans le domaine quantique oblige les startups Françaises à mettre la barre très haut concernant les résultats expérimentaux à atteindre.
Alice & Bob a par exemple déclaré que les fonds levés en 2022 (27 millions d'euros) allait servir à recruter les meilleurs chercheurs et ingénieurs au monde, à acheter le meilleur matériel présent sur le marché et à développer des partenariats concernant l'utilisation de son futur ordinateur quantique. La stratégie nationale d'accélération quantique favorise l'émergence de startups prometteuses. Cet écosystème de la French Tech quantique commence à peine à se structurer mais affiche une ambition commune : booster les applications industrielles en lien avec la recherche. Plébiscitée pour son réseau académique et ses politiques publiques en matière quantique, la France attire les startups étrangères en la matière dont les intérêts doivent être rigoureusement contrôlés.

Une cartographie restreinte mais de qualité

Entre la conception de nouvelles machines et la découverte d'applications inédites, la concrétisation des ordinateurs quantiques provoque une véritable effervescence dans la recherche. Plusieurs startups, principalement issues de laboratoires CNRS, se positionnent pour participer à cette révolution (capteurs et systèmes de communication quantiques). Quatre startups se distinguent en particulier :

- La société Quandela qui travaille à l'émergence de nouveaux ordinateurs et de nouveaux réseaux de communication.
- La société Pasqal s'attaque quant à elle aux simulateurs quantiques programmables à l'aide d'atomes froids ayant la capacité de résoudre des problèmes complexes sur lesquels buttent les ordinateurs classiques haute performance.
- La startup Alice & Bob vise la mise au point en cinq ans d'un calculateur quantique universel opérationnel.
- La startup C12 développe quant à elle des processeurs quantiques fiables pour accélérer des calculs très complexes.

D'autres startups cherchent à se faire une place sur ce marché et espèrent également

produire l'ordinateur du futur. A ce jour, une trentaine de PME et startups parient donc sur cet avenir quantique. A leur façon, elles participent à la souveraineté nationale et à l'indépendance en matière quantique. En ce sens, le système étendu d'aides à l'amorçage de ces startups, entamées sous l'étiquette "Deep Tech", est en véritable atout.

Au résultat, la France dispose du plus grand nombre de startups en Europe. Et le plan national quantique prévoit d'en avoir une centaine dans cinq ans.

Des startups étrangères attirées par l'excellence française

En moins de trois ans, six startups étrangères spécialistes des technologies quantiques se sont installées en France [178]. Volonté d'espionnage ou recherche d'excellence, quels sont les intérêts de ces entreprises qui s'installent sur le territoire national.

Ce chiffre s'explique autant par l'excellence académique que par les politiques publiques initiées notamment depuis 2021.

La dernière startup étrangère a s'être installée sur Paris est la société IQM d'origine Finlandaise mi-décembre 2021 . La première est la société californienne QC-Ware en 2019. Quatre autres startups provenant des Etats-Unis, du Royaume-Uni (Kets quantum et PQShield), des Pays-Bas et d'Espagne (Multiverse computing) lui ont succédée.

Ce succès est en partie dû à la densité académique de la France sur le sujet quantique. La liste des établissements reconnus est longue, tout comme celle des laboratoires prestigieux qui leur sont affiliés. Cependant, cet accès leur permet certes de se for- mer à la française mais aussi de recruter parmi les talents français pour travailler sur leurs propres intérêts. Participant à l'économie du lieu d'installation, à travers des investissements, des infrastructures et des emplois, ces entreprises se fondent dans le paysage quantique français. Il n'y a guère que leur nom qui nous rappelle à leur origine.

Il existe un revers de la médaille à ce dynamisme étranger. En effet, les startups françaises du quantique devront désormais faire avec leurs concurrents étrangers sur tous les fronts, tant sur le recrutement que la participation aux grands projets nationaux.

CONCLUSION ET OUVERTURE

Un bruit extrêmement important entoure l'informatique quantique, et la course à la pseudo innovation soutenue par l'hyperliquidité des marchés financiers et des finan- cements publiques engendre une sur-communication conduisant à la création de la nébuleuse quantique. Nous avons donc tenté d'adresser les différents éléments affé- rents à l'informatique quantique. Nous avons essayé de rétablir les éléments factuels concernant la technologie, la cryptographie, la Blockchain et les impacts sociétaux. Nous avons aussi abordé la position française face au quantique, élément clé de la problématique.

Nous allons donc procéder de façon synthétique [179] :

- Mythe 1 : l'informatique quantique signifiera la fin de l'informatique "normale" (classique).
    - Fait 1 : Les ordinateurs quantiques ne vont pas effacer l'informatique classique. Il y a peu de problèmes complexes dans l'histoire des mathématiques modernes qui nécessiteraient un ordinateur quantique pour être résolus, en revanche certain problèmes pourraient être traités différemment.

- Mythe 2 : L'informatique quantique peut exécuter des codes de programma- tion similaires à ceux des ordinateurs classiques.
    - Fait 2 : L'informatique quantique ne peut pas exécuter les mêmes programmes que les ordinateurs classiques. L'informatique quantique ne peut résoudre que les problèmes qui lui sont spécifiquement destinés, où elle dispose de l'algorithme pour résoudre les calculs. Encore aujourd'hui peu d'ordinateurs quantiques sont programmables à grande échelle.

- Mythe 3 : l'informatique quantique détruira la cybersécurité.
  Fait 3 : Dans l'état actuel des choses, les algorithmes quantiques de Shor et Grover viennent mettre à mal les normes de sécurisation actuelles. En effet, l'informatique quantique peut détruire la sécurité d'internet si une attaque quantique est déclenchée. Les ordinateurs quantiques seront théoriquement capables de briser les algorithmes PKC [28] les plus robustes. Cela met en danger l'ensemble des réseaux de communication et des données. Cependant, les algo- rithmes de cryptographie post-quantique offrent une cybersécurité renforcée, même en cas d'attaque quantique à grande échelle. L'implémentation de cette stratégie est bien la cible de mondiale de tous les pays embarqués dans cette trajectoire en termes de conduite de changement.

- Mythe 4 : Les ordinateurs quantiques pourraient atteindre la conscience et se transformer en "esprit quantique".
    - Fait 4 : L'esprit quantique ou la conscience n'est qu'une hypothèse très loin d'avoir été prouvée. Ce mythe s'apparente plus à de la science fiction et sup-

pose que la conscience a elle-même une forme quantique ce qui touche plus à l'ésotérisme.

- ❖ Mythe 5 : l'informatique quantique sera commercialisée à grande échelle dans les 15 ans à venir.

    - Fait 5 : Il sera même difficile pour l'informatique quantique de remplacer entièrement l'informatique classique. En réalité, les ordinateurs se diversifient, et l'avenir semble plus appartenir aux machines hybrides puisque les ordinateurs classiques restent puissants. Les machines hybrides sont le seul moyen d'accroître l'importance de l'informatique quantique dans le secteur commercial. Élément confirmé par Philippe Duluc, le CTO du groupe ATOS.

- ❖ Mythe 6 : La cryptographie post-quantique correspond à une nouvelle tech- nologie encore plus puissante que l'ordinateur quantique.

    - Fait 6 : La cryptographie post-quantique se base sur des approches résistantes à l'utilisation d'ordinateurs quantiques pour le déchiffrement, et ne s'apparente pas à une technologie.

- ❖ Mythe 7 : La Blockchain est infaillible, même à l'utilisation d'ordinateur quantique.

    Fait 7 : Aujourd'hui les apports de la Blockchain sont indéniables en termes d'intégrité de l'information, et les applications sociétales sont extrêmement intéressantes, que celles-ci soient en finance, dans le domaine du transport, de l'immobilier, de la santé, dans le secteur pharmaceutique, agro-alimentaire, ou de l'éducation, etc. Cependant, le chiffrement des blocs est déjà à risque, ou même cassable. Mais le fonctionnement communautaire rend l'intérêt limité pour les attaquants car résulte soit en un "fork" soit dans une nécessité de continuité d'action (piratage permanent). Cette mise en risque pourrait être problématique pour les jeunes Blokchains et les cas d'usages entreprise, mais beaucoup moins inquiétante pour les Blockchains déjà matures.

27. Public-key Cryptography

- Mythe 8 : La France est en retard par rapport aux autres pays quant à la technologie quantique.

    - Fait 8 : La France s'est en effet lancée dans l'aventure quantique à un niveau institutionnel quelques années après d'autres pays tels que le Royaume-Uni, les États-Unis, l'Allemagne ou la Chine. Cependant, sa stratégie choisie est une approche holistique. En effet, pour la France l'objectif n'est pas seulement technologique mais aussi applicatif, et cela à grande échelle. Par ailleurs, la France bénéficie d'un niveau académique sur le sujet qui n'a rien à envier aux autres. En d'autres termes, la France s'est peut-être lancée après ces concurrents, mais a potentiellement pris un chemin plus fructueux. Par ailleurs, l'investissement français dans le domaine ne va faire que croître dans les an- nées à venir.

Dans ce rapport, nous avons donc tenté d'apporter un certain nombre d'éclairages quant à la nébuleuse quantique. Nous avons essayé de traiter les impacts potentiels sur la société mais aussi les opportunités quant aux innovations, en cours ou futures, que celles-ci soient cryptographiques, liées à la Blockchain, ou plus largement pour la société française. En réalité, les bénéfices de l'ordinateur quantique sont bien plus profonds et ne se limitent pas à des menaces potentielles dirigés vers la société. En effet, les apports dans des environnements à comportement particulaire, peuvent être réellement intéressants car le changement de paradigme sous-jacent permettrait de redéfinir notre perception de certains sujets et problématiques, et de proposer des solutions potentiellement bien plus spectaculaires.
La France a pris la mesure des enjeux, et sa réponse institutionnelle indique des velléités de suprématie quantique mondiale. Cependant l'approche holistique, semble indiquer que notre pays ne cherche pas à seulement à ajouter une corde à son arc, mais réellement de changer d'arc. La problématique qui semblait technologique initialement, a pris une dimension géopolitique majeure.

Références

[1] Cracking 256-bit rsa keys – surprisingly simple !, 2015. URL https://www.doyler.net/security-not-included/cracking-256-bit-rsa-keys. Consulté le 2022/05/17.

[2] Nouvelle taille de clé rsa minimale pour les certificats de signature de code. ssl.com, Permanent. URL https://www.ssl.com/fr/les-blogs/nouvelle-taille-de-cl%C3%A9-rsa-minimale-pour-les-certificats- de-signature-de-code/. Consulté le 2022/04/15.

[3] Challenge richelieu dgse. GitHub, 2019. URL https://github.com/gw3l/ richelieu. Consulté le 2022/04/23.

[4] MW Johnson, P Bunyk, F Maibaum, E Tolkacheva, AJ Berkley, EM Chapple, R Harris, J Johansson, T Lanting, I Perminov, et al. A scalable control system for a superconducting adiabatic quantum optimization processor. *Supercon- ductor Science and Technology*, 23(6) :065004, 2010.

[5] Quantum computers are not as powerful as you might think... Medium, 2022. URL https://bootcamp.uxdesign.cc/quantum-computers-are-not- as-powerful-as-you-might-think-af80ae838025. Consulté le 2022/04/23.

[6] Will quantum computing ever live up to its hype ? Scientific Ameri- can, 2021. URL https://www.scientificamerican.com/article/will- quantum-computing-ever-live-up-to-its-hype/. Consulté le 2022/04/23.

[7] What europe can learn from france when it comes to quantum computing. Sifted by FT, 2021. URL https://sifted.eu/articles/france-quantum- computing-investment/. Consulté le 2022/04/12.

[8] Paul Benioff. The computer as a physical system : A microscopic quantum me- chanical hamiltonian model of computers as represented by turing machines. *Journal of statistical physics*, 22(5) :563–591, 1980.

[9] David Mermin. Breaking rsa encryption with a quantum computer : Shor's factoring algorithm. *Lecture notes on Quantum computation*, pages 481–681, 2006.

[10] Elizabeth Gibney. Hello quantum world ! google publishes landmark quantum supremacy claim. *Nature*, 574(7779) :461–463, 2019.

[11] Richard P Feynman. Quantum mechanical computers. *Optics news*, 11(2) : 11–20, 1985.

[12] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. *Phys. Today*, 54(2) :60, 2001.

[13] Tadashi Kadowaki and Hidetoshi Nishimori. Quantum annealing in the trans- verse ising model. *Physical Review E*, 58(5) :5355, 1998.

[14] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[15] John Clarke and Frank K Wilhelm. Superconducting quantum bits. *Nature*, 453(7198) :1031–1042, 2008.

[16] Nicolai Friis, Oliver Marty, Christine Maier, Cornelius Hempel, Milan Holzäp- fel, Petar Jurcevic, Martin B Plenio, Marcus Huber, Christian Roos, Rainer Blatt, et al. Observation of entangled states of a fully controlled 20-qubit system. *Physical Review X*, 8(2) :021012, 2018.

[17] Mohammadsadegh Khazali and Klaus Mølmer. Fast multiqubit gates by adia- batic evolution in interacting excited-state manifolds of rydberg atoms and superconducting circuits. *Physical Review X*, 10(2) :021054, 2020.

[18] A Imamog, David D Awschalom, Guido Burkard, David P DiVincenzo, Da- niel Loss, M Sherwin, A Small, et al. Quantum information processing using quantum dot spins and cavity qed. *Physical review letters*, 83(20) :4204, 1999.

[19] Leonid Fedichkin, Maxim Yanchenko, and KA Valiev. Novel coherent quantum bit using spatial quantization levels in semiconductor quantum dot. *arXiv preprint quant-ph/0006097*, 2000.

[20] Viktor Ivády, Joel Davidsson, Nazar Delegan, Abram L Falk, Paul V Klimov, Samuel J Whiteley, Stephan O Hruszkewycz, Martin V Holt, F Joseph He- remans, Nguyen Tien Son, et al. Stabilization of point-defect spin qubits by quantum wells. *Nature communications*, 10(1) :1–8, 2019.

[21] A Bertoni, Paolo Bordone, Rossella Brunetti, Carlo Jacoboni, and S Reggiani. Quantum logic gates based on coherent electron transport in quantum wires. *Physical Review Letters*, 84(25) :5912, 2000.

[22] Neil Gershenfeld and Isaac L Chuang. Quantum computing with molecules. *Scientific American*, 278(6) :66–71, 1998.

[23] Bruce E Kane. A silicon-based nuclear spin quantum computer. *nature*, 393 (6681) :133–137, 1998.

[24] Eduardo Berrios, Martin Gruebele, Dmytro Shyshlov, Lei Wang, and Dmitri Babikov. High fidelity quantum gates with vibrational qubits. *The Journal of Physical Chemistry A*, 116(46) :11347–11354, 2012.

[25] PM Platzman and MI Dykman. Quantum computing with electrons floating on liquid helium. *Science*, 284(5422) :1967–1969, 1999.

[26] Herbert Walther, Benjamin TH Varcoe, Berthold-Georg Englert, and Thomas Becker. Cavity quantum electrodynamics. *Reports on Progress in Physics*, 69 (5) :1325, 2006.

[27] Michael N Leuenberger and Daniel Loss. Quantum computing in molecular magnets. *Nature*, 410(6830) :789–793, 2001.

[28] Wolfgang Harneit. Fullerene-based electron-spin quantum computer. *Physical Review A*, 65(3) :032322, 2002.

[29] Isaac L Chuang and Yoshihisa Yamamoto. Simple quantum computer. *Phy- sical Review A*, 52(5) :3489, 1995.

[30] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816) :46–52, 2001.

[31] AP Nizovtsev, S Ya Kilin, F Jelezko, T Gaebal, Iulian Popa, A Gruber, and Jorg Wrachtrup. A quantum computer based on nv centers in diamond : optically detected nutations of single electron and nuclear spins. *Optics and spectroscopy*, 99(2) :233–244, 2005.

[32] Marco Anderlini, Patricia J Lee, Benjamin L Brown, Jennifer Sebby-Strabley, William D Phillips, and James V Porto. Controlled exchange interaction bet- ween pairs of neutral atoms in an optical lattice. *Nature*, 448(7152) :452–456, 2007.

[33] Nicklas Ohlsson, R Krishna Mohan, and Stefan Kröll. Quantum computer hardware based on rare-earth-ion-doped inorganic crystals. *Optics communi- cations*, 201(1-3) :71–77, 2002.

[34] Bálint Náfrádi, Mohammad Choucair, Klaus-Peter Dinse, and László Forró. Room temperature manipulation of long lifetime spins in metallic-like carbon nanospheres. *Nature communications*, 7(1) :1–8, 2016.

[35] Paul G Kwiat and Harald Weinfurter. Embedded bell-state analysis. *Physical Review A*, 58(4) :R2623, 1998.

[36] A Das. Quantum annealing and analog quantum computation lecture notes in physics 679, ed das a and chakrabarti bk, 2005.

[37] Chetan Nayak, Steven H Simon, Ady Stern, Michael Freedman, and San- kar Das Sarma. Non-abelian anyons and topological quantum computation. *Reviews of Modern Physics*, 80(3) :1083, 2008.

[38] Difference between classical computing and quantum computing. Me- dium, 2020. URL https://faun.pub/classical-computing-c1a126a7bd73. Consulté le 2022/05/17.

[39] Guillermo Algaze. The end of prehistory and the uruk period. *The Sumerian World*, (C), 2013.

[40] Nigel P Smart. The enigma machine. In *Cryptography Made Simple*, pages 133–161. Springer, 2016.

[41] Post-quantum cryptography for long-term security pqcrypto ict-645622, 2015. URL https://pqcrypto.eu.org/. Consulté le 2022/05/17.

[42] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations : A survey. *ACM Computing Surveys (CSUR)*, 51(6) :1–41, 2019.

[43] Prasanna Ravi, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. Lattice-based key-sharing schemes : A survey. *ACM Computing Surveys (CSUR)*, 54(1) :1–39, 2021.

[44] Chithralekha Balamurugan, Kalpana Singh, Ganeshvani Ganesan, and Muttukrishnan Rajarajan. Post-quantum and code-based cryptography—some prospective research directions. *Cryptography*, 5(4) :38, 2021.

[45] Sawan Bhattacharyya and Amlan Chakrabarti. Post-quantum cryptography. *Data Management, Analytics and Innovation*, pages 375–405, 2022.

[46] Sattar B Sadkhan. Elliptic curve cryptography-status, challenges and future trends. In *2021 7th International Engineering Conference "Research & Inno- vation amid Global Pandemic"(IEC)*, pages 167–171. IEEE, 2021.

[47] Ray A Perlner and David A Cooper. Quantum resistant public key crypto- graphy : a survey. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, pages 85–93, 2009.

[48] La deuxième révolution quantique : états des lieux. Techno-Science.net, 2021. URL https://www.techno-science.net/actualite/deuxieme- revolution-quantique-etat-lieux-N20850.html. Consulté le 2022/05/03.

[49] Le marche du quantique en pleine croissance. datacenter-magazine.fr, 2021. URL https://datacenter-magazine.fr/le-marche-du-quantique- en-pleine-croissance/. Consulté le 2022/05/03.

[50] Le national quantum initiativ act. congress.gov, 2017. URL https://www-congress-gov.translate.goog/bill/115th-congress/house-bill/6227?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc. Consulté le 2022/05/03.

[51] Conflit sino-americain :le quantique, nerf des guerres de demain. france24.com, 2021. URL https://www.france24.com/fr/%C3%A9co-tech/20211125- conflit-sino-am%C3%A9ricain-le-quantique-nerf-des-guerres-de- demain. Consulté le 2022/05/03.

[52] Course-internationale-autour-physique-quantique. letemps.ch, 2022. URL https://www.letemps.ch/sciences/course-internationale-autour- physique-quantique. Consulté le 2022/05/05.

[53] Le prototype d'ordinateur quantique chinois jiuzhang est leader mondial en matière de capacités de calcul. french.peopledaily.com, 2020. URL http://french.peopledaily.com.cn/n3/2020/1218/c31357-9800654.html. Consulté le 2022/05/02.

[54] Anssi views on the post quantum cryptography transition. ssi.gouv.fr, 2022. URL https://www.ssi.gouv.fr/en/publication/anssi-views-on- the-post-quantum-cryptography-transition/. Consulté le 2022/05/03.

[55] Rsa panel covers cryptography trends, elections and more. TechTarget, 2017. URL https://www.techtarget.com/searchsecurity/news/450413012/ RSA-panel-covers-cryptography-trends-elections-and-more. Consulté le 2022/04/23.

[56] L'ordinateur quantique, un rêve prochain. La Croix, 2016. URL https://www.la-croix.com/Sciences/Numerique/L-ordinateur- quantique-reve-prochain-2016-05-06-1200758376. Consulté le 2022/04/02.

[57] Pourquoi l'informatique quantique n'est pas une menace pour la sécurité. Le Soir, 2021. URL https://geeko.lesoir.be/2021/10/21/pourquoi-linformatique-quantique-nest-pas-une-menace-pour-la-securite/. Consulté le 2022/04/02.

[58] Cybersécurité : qu'est-ce que l'apocalypse quantique et devons-nous avoir peur ? BBC, 2022. URL https://www.bbc.com/afrique/monde-60154391. Consulté le 2022/04/02.

[59] Claus Peter Schnorr. Fast factoring integers by svp algorithms, corrected. Cryptology ePrint Archive, Report 2021/933, 2021. https://ia.cr/2021/933.

[60] Cryptographie sur les courbes elliptiques. Wikipédia, 2022. URL https://fr.wikipedia.org/wiki/Cryptographie_sur_les_courbes_elliptiques. Consulté le 2022/03/17.

[61] Cryptographie post-quantique. Wikipédia, 2022. URL https://fr.wikipedia.org/wiki/Cryptographie_post-quantique. Consulté le 2022/03/17.

[62] Cyberattaque : l'ukraine accuse la russie et dit avoir des « preuves ». Le Monde, 2022. URL https://www.lemonde.fr/pixels/article/2022/01/16/microsoft-a-detecte-une-attaque-visant-a-saboter-des-systemes-informatiques-de-l-etat-ukrainien_6109709_4408996.html. Consulté le 2022/03/17.

[63] Quantum compution : Progress and prospects. National Acede- mies, 2019. URL https://nap.nationalacademies.org/catalog/25196/ quantum-computing-progress-and-prospects. Consulté le 2022/05/14.

[64] Nathan Babcock. Paysage des brevets & publications sur les technologies quantiques. Technical report, Institute for Quantum Science and Technology, 2022. URL https://www.iqst.ca/events/csqic05/talks/nathan%20b.pdf. Consulté le 2022/05/14.

[65] Chien-Hsing Wu, Yan-Chr Tsai, and Hwa-Long Tsai. Quantum circuits for sta- bilizer codes. In *2005 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2333–2336 Vol. 3, 2005. doi : 10.1109/ISCAS.2005.1465092.

[66] The most connected and powerful quantum computer build for business. D- Wave, 2022. URL https://www.dwavesys.com/solutions-and-products/ systems/. Consulté le 2022/05/14.

[67] Mosca's inequality and its effect on quantum cryptography. analy- ticsindiamag.com, 2019. URL https://analyticsindiamag.com/moscas-inequality-and-its-effect-on-quantum-cryptography/. Consulté le 2022/04/05.

[68] Michele Mosca. Cybersecurity in an era with quantum computers : Will we be ready ? *IEEE Secutity Privacy*, 16(5) :38–41, 2018.

[69] Lewis Adam, Ferigato Carlo, Travagnin Martino, and Florescu Elisabeta. The impact of quantum technologies on the eu's future policies : Part 3 perspectives for quantum computing. 2018. URL https://www.semanticscholar.org/ paper/The-Impact-of-quantum-technologies-on-the-EU's-Part-Adam-Carlo/41955ade75354831bdd9754eafdb3201922cae0b. Consulté le 2022/05/13.

[70] Dozens of companies budget $1m+ for quantum computing as tech race intensifies. Sifted, 2022. URL https://sifted.eu/articles/companies- spending-quantum-computing. Consulté le 2022/03/03.

[71] Quantum computing grows. IDC, 2021. URL https://www.idc.com/ getdoc.jsp?containerId=prUS47696021. Consulté le 2022/03/03.

[72] L'informatique quantique pèsera 1000 milliards de dollars en 2035, selon mckinsey. usine-digitale.fr, 2020. URL https://www.usine-digitale.fr/ editorial/l-informatique-quantique-pesera-1000-milliards-de- dollars-en-2035-selon-mckinsey.N937863. Consulté le 2022/05/04.

[73] Quantum ai hardware. Google Quantum AI, 2022. URL https:// quantumai.google/hardware?hl=fr. Consulté le 2022/03/23.

[74] Google cirq software (2022). Google Quantum AI, 2022. URL https:// quantumai.google/software?hl=fr. Consulté le 2022/03/23.

[75] Ryan Babbush Frank Arute, Kunal Arya and al. Quantum supremacy using a programmable superconducting processor. *Nature*, (574) :509–510, 2019. doi : https://doi.org/10.1038/s41586-019-1666-5.

[76] Azure quantum newsletter. Microsoft Quantum Newsletter (2022), 2022. URL https://azure.microsoft.com/en-us/solutions/quantum-computing/ quantum-computing-newsletter-signup/. Consulté le 2022/03/23.

[77] Behind in quantum computer race, germany gets boost from ibm. Ya- hoo ! News, 2021. URL https://news.yahoo.com/behind-quantum-compute- race-germany-132453704. Consulté le 2022/03/23.

[78] Qu'est-ce que l'informatique quantique ? IBM, Permanent. URL https:// www.ibm.com/frfr/topics/quantum-computing. Consulté le 2022/03/23.

[79] Ibm quantum breaks the 100 qubit processor barrier. IBM Research Blog, 2021. URL https://research.ibm.com/blog/127-qubit-quantum- processor-eagle. Consulté le 2022/03/23.

[80] Ibm's roadmap for scaling quantum technology, 2021. IBM Research Blog, 2021. URL https://research.ibm.com/blog/ibm-quantum-roadmap. Consulté le 2022/03/23.

[81] Ibm quantum system one. IBM Research Blog, 2022. URL https:// research.ibm.com/interactive/system-one/. Consulté le 2022/03/23.

[82] Open source quantum development. Qiskit.org, 2022. URL https:// qiskit.org/. Consulté le 2022/03/23.

[83] Blog. IBM Research Blog, 2022. URL https://research.ibm.com/blog?tag= quantum-computing. Consulté le 2022/05/11.

[84] Leilei Huang, Kai Feng, and Chongjin Xie. Quantum random number cloud platform. 2021. doi : https://doi.org/10.1038/s41534-021-00442-x.

[85] Informatique quantique et cybersécurité, garants de l'autonomie technologique européenne. WAVESTONE, 2020. URL https: //www.wavestone.com/fr/insight/informatique-quantique-et-cybersecurite_francedigitale_wavestone/. Consulté le 2022/03/23.

[86] 13 companies offering quantum cloud computing services in 2022. The Quan- tum Insider, 2022. URL https://thequantuminsider.com/2022/05/03/ 13-companies-offering-quantum-cloud-computing-services-in-2022/. Consulté le 2022/03/23.

[87] Olivier Ezratty. Understanding quantum technologies 2021. Technical report, Opinions Libres - Olivier Ezratty, 2022. URL https://www.oezratty.net/ wordpress/2021/understanding-quantum-technologies-2021/. Consulté le 2022/04/06.

[88] Assessment-of-the-future-economic-impact-of-quantum-information-science. IDA.org, 2022. URL https://www.ida.org/-/media/feature/ publications/a/as/assessment-of-the-future-economicimpact-of-quantum-information-science/p-8567.ashx. Consulté le 2022/03/23.

[89] Michel KUREK. Paysage des brevets & publications sur les technolo- gies quantiques. Technical report, Le Lab Quantique, Ecole Polytechnique, 2020. URL https://lelabquantique.com/wp-content/uploads/2020/07/ Rapport-Kurek-FINAL.pdf. Consulté le 2022/03/23.

[90] Pan jianwei. Wikipedia, Permanent. URL https://en.wikipedia.org/wiki/Pan_Jianwei. Consulté le 2022/03/23.

[91] Nature's 10. Wikipedia, Permanent. URL https://en.wikipedia.org/wiki/Nature%27s_10#2017. Consulté le 2022/03/23.

[92] Real-world intercontinental quantum communications enabled by the mi- cius satellite. Phys.org, 2018. URL https://phys.org/news/2018-01- real-world-intercontinental-quantum-enabled-micius.html. Consulté le 2022/04/13.

[93] Xi jinping presided over the 24th collective study of the political bureau of the central committee and delivered a speech. Chinese Government, 2018. URL http://www.gov.cn/xinwen/2020-10/17/content_5552011.htm. Consulté le 2022/05/13.

[94] Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xia- wei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, Ming Gong, Cheng Guo, Chu Guo, Shaojun Guo, Lianchen Han, Linyin Hong, He-Liang Huang, Yong-Heng Huo, Liping Li, Na Li, Shaowei Li, Yuan Li, Futian Liang, Chun Lin, Jin Lin, Haoran Qian, Dan Qiao, Hao Rong, Hong Su, Lihua Sun, Liangyuan Wang, Shiyu Wang, Dachao Wu, Yu Xu, Kai Yan, Weifeng Yang, Yang Yang, Yangsen Ye, Jianghan Yin, Chong Ying, Jiale Yu, Chen Zha, Cha Zhang, Haibin Zhang, Kaili Zhang, Yiming Zhang, Han Zhao, Youwei Zhao, Liang Zhou, Qingling Zhu, Chao-Yang Lu, Cheng-Zhi Peng, Xiaobo Zhu, and Jian-Wei Pan. Strong quantum computational ad- vantage using a superconducting quantum processor. *Phys. Rev. Lett.*, 127 : 180501, Oct 2021. doi : 10.1103/PhysRevLett.127.180501. URL https: //link.aps.org/doi/10.1103/PhysRevLett.127.180501.

[95] White house budget proposes to hike ai and quantum funding by 30 percent to stay ahead of china. The Brighter Side Of News, 2020. URL https://www.thebrighterside.news/post/white-house-budget-proposes-to-hike-ai-and-quantum-funding-by-30-percent-to-stay- ahead-of-china. Consulté le 2022/05/13.

[96] Paula Forteza, Jean-Paul Herteman, and Iordanis Kerenidis. Quantique : Le virage technologique que la france ne ratera pas. Technical report, Gouvernement Français, 2019. URL https://www.entreprises.gouv.fr/files/files/01-nouveau-portail/etudes-statistiques/etudes/rapport- mission-quantique.pdf. Consulté le 2022/03/23.

[97] 1,8 m € en faveur des technologies quantiques. Gouvernement Français, 2021. URL https://www.gouvernement.fr/actualite/18-m-eu-en-faveur-des- technologies-quantiques. Consulté le 2022/05/13.

[98] Mext - quantum leap flagship program(mext q-leap). Japan Science and Technology Agency, 2021. URL https://www.jst.go.jp/stpp/q-leap/en/index.html. Consulté le 2022/05/09.

[99] Les smart contracts : contrats non identifiés ? Statista, 2021. URL https://fr.statista.com/infographie/23555/capitalisation- boursiere-cryptomonnaies-bitcoin-ethereum-binance-solana/. Consulté le 2022/05/20.

[100] Le droit pénal à l'épreuve des cyberattaques. Club des Juristes, 2022. URL https://journalducoin.com/lexique/smart-contract/. Consulté le 2022/05/20.

[101] Top 10 blockchain attacks, vulnerabilities & weaknesses. Cloud Security Alliance, 2021. URL https://cloudsecurityalliance.org/artifacts/ top-10-blockchain-attacks-vulnerabilities-weaknesses/. Consulté le 2022/05/20.

[102] Reachable bitcoin nodes. Bitnodes, 2021. URL https://bitnodes.io. Consulté le 2022/05/17.

[103] Qu'est-ce que la defi ou finance décentralisée ? Cryptoast, 2019. URL https://cryptoast.fr/defi-finance-decentralisee/. Consulté le 2022/05/20.

[104] Qu'est-ce que la defi ou finance décentralisée ? Journal du Coin, 2021. URL https://www.leclubdesjuristes.com/wp-content/uploads/2021/04/rapport_cyberattaques_DEF2_WEB.pdf. Consulté le 2022/05/20.

[105] Les smart contracts : contrats non identifiés ? Village Justice, 2018. URL https://www.village-justice.com/articles/les-smart- contracts-contrats-non-identifies,28893.html. Consulté le 2022/05/20.

[106] What's in a smart contract ? SmartContractLaw, unknown. URL https://www.freshfields.com/en-gb/our-thinking/campaigns/ technology-quotient/fintech/whats-in/whats-in-a-smart-contract/. Consulté le 2022/05/20.

[107] Définition de token. BlockchainFrance, 2018. URL https://blockchainfrance.net/2018/05/22/comprendre-les-tokens/. Consulté le 2022/05/21.

[108] Blockchain in the quantum era. Cloud Security Alliance, 2021. URL https://cloudsecurityalliance.org/artifacts/blockchains-in- the-quantum-era/. Consulté le 2022/05/20.

[109] Beyond cryptocurrency : 9 relevant blockchain and distributed led- ger technology use cases. Cloud Security Alliance, 2018. URL https://cloudsecurityalliance.org/blog/2019/07/31/use-cases-for-blockchain-beyond-cryptocurrency/. Consulté le 2022/05/20.

[110] Strategie nationale sur les technologies quantiques : faire dela france un acteur majeur deces technologies au niveau européen et international. enseignementsup-recherche.gouv.fr, 2021. URL https://www.enseignementsup-recherche.gouv.fr/fr/strategie- nationale-sur-les-technologies-quantiques-faire-de-la-france-un-acteur-majeur-de-ces-49233. Consulté le 2022/05/03.

[111] La maîtrise du quantique le graal geopolitique mondial. challenges.fr, 2021. URL https://www.challenges.fr/high-tech/la-maitrise- du-quantique-le-graal-geopolitique-mondial_764554. Consulté le 2022/04/21.

[112] Quantique : le gouvernement lance une task force interministérielle pour ne pas rater le virage. 01net.fr, 2020. URL https://www.01net.com/actualites/quantique-le-gouvernement-lance-une-task-force-interministerielle-pour-ne-pas-rater-le-virage-1837924.html. Consulté le 2022/05/02.

[113] La cryptographie et la communication quantiques. senat.fr, 2019. URL http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2019_0024_note_technologies_quantiques.pdf. Consulté le 2022/04/21.

[114] Les technologies quantiques. cea.fr, 2021. URL https://www.cea.fr/comprendre/Pages/nouvelles-technologies/essentiel-sur- cryptographie-et-communication-quantiques.aspx. Consulté le 2022/04/21.

[115] Informatique quantique un enjeu économique et de souveraineté selon le rapport forteza. cea.fr, 2022. URL https://www.cea.fr/presse/Pages/actualites-communiques/ntic/capteurs-quantiques-instruments-de-mesure-haute-precision.aspx. Consulté le 2022/04/17.

[116] Quels sont les enjeux de r&d autour des capteurs quantiques. lemon-deinformatique.fr, 2020. URL https://www.lemondeinformatique.fr/actualites/lire-informatique-quantique-un-enjeu-economique-et- de-souverainete-selon-le-rapport-forteza-77668.html. Consulté le 2022/04/12.

[117] Pourquoi la france peut réussir dans les technologies quantiques. challenges.fr, 2020. URL https://www.challenges.fr/high-tech/pourquoi-la-france- peut-reussir-dans-les-technologies-quantiques_692984. Consulté le 2022/04/17.

[118] Trés grand centre de calcul du cea. hpc.cea.fr, 2021. URL http://www-hpc.cea.fr/fr/complexe/tgcc.htm. Consulté le 2022/04/10.

[119] L'avenir est quantique. Quantum Flagship, 2022. URL https://qt-eu.translate.goog/?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc. Consulté le 2022/04/10.

[120] Airbus quantum computing challenge. airbus.com, 2020. URL https://www.airbus.com/en/innovation/disruptive-concepts/quantum-technologies/airbus-quantum-computing-challenge. Consulté le 2022/04/13.

[121] Stratégie nationale sur les technologies quantiques. c2n.universite-paris-saclay.fr, 2020. URL https://www.c2n.universite-paris-saclay.fr/fr/ visite-m-macron/. Consulté le 2022/04/13.

[122] Le programme d'investissement d'avenir. gouvernement.fr, 2018. URL https: //www.gouvernement.fr/le-programme-d-investissements-d-avenir. Consulté le 2022/03/11.

[123] Plan de relance. economie.gouv.fr, 2022. URL https:// www.economie.gouv.fr/plan-de-relance. Consulté le 2022/03/18.

[124] Investissements d'avenir / nouvelle phase de la stratégie nationale d'intelligence artificielle : le gouvernement fait le pari des talents. gouvernement.gouv.fr, 2021. URL https://www.gouvernement.fr/investissements- d-avenir-nouvelle-phase-de-la-strategie-nationale-d- intelligence-artificielle-le#:~:text=Les%20Programmes% 20d'investissements%20d,%E2%82%AC%20%C3%A0%20l'horizon%202025. Consulté le 2022/02/18.

[125] Décoder l'annonce du plan quantique français. frenchweb.fr, 2021. URL https://www.frenchweb.fr/decoder-lannonce-du-plan-quantique-francais/414007. Consulté le 2022/04/18.

[126] Stratégie nationale pour technologies quantiques. entreprises.gouv.fr, 2021. URL https://www.entreprises.gouv.fr/fr/numerique/politique-numerique/strategie-nationale-pour-technologies-quantiques. Consulté le 2022/05/03.

[127] Audacia prévoit de lancer un nouveau fonds d'investissement en 2022. usine.digitale.fr, 2021. URL https://www.usine-digitale.fr/ article/quantique-audacia-prevoit-de-lancer-un-nouveau-fonds-d-investissement-en-2022.N1149522. Consulté le 2022/04/30.

[128] Cedric o décode le plan quantique du gouvernement. frenchweb.fr, 2021. URL https://www.frenchweb.fr/decode-quantum-speciale-avec-cedric-o- pour-decoder-le-plan-quantique-du-gouvernement/413501. Consulté le 2022/04/27.

[129] 1,8 milliard d'euros en faveur des technologies quantiques. gouverne- ment.fr, 2021. URL https://www.gouvernement.fr/actualite/18-m-eu- en-faveur-des-technologies-quantiques. Consulté le 2022/04/21.

[130] Stratégie nationale pour les technologies quantiques. entreprises.gouv.fr, 2021. URL https://www.entreprises.gouv.fr/fr/numerique/politique-

numerique/strategie-nationale-pour-technologies-quantiques.
Consulté le 2022/04/17.

[131] Stratégie nationale quantique : 10 projets et deux équipex+ retenus dans le cadre du programme et éuipement prioritaire de recherche (pepr). cnrs.fr, 2022. URL https://www.cnrs.fr/fr/strategie-nationale-quantique-10- projets-et-deux-equipex-retenus-dans-le-cadre-du-programme-et. Consulté le 2022/03/17.

[132] Présentation de la stratégie nationale sur les technologies quantiques. elysee.fr, 2021. URL https://www.elysee.fr/emmanuel-macron/2021/01/21/presentation-de-la-strategie-nationale-sur-les-technologies-quantiques. Consulté le 2022/04/17.

[133] Les détails du plan quantique : 1,8 milliard d'euros, "un ordina- teur hybride" à l'horizon 2023. nextinpact.com, 2021. URL https://www.nextinpact.com/article/43406/les-details-plan-quantique-18-milliard-d'euros-ordinateur-hybride-a-lhorizon-2023. Consulté le 2022/04/08.

[134] La france va consacrer 1,8 milliard d'euros aux technologies quantiques. lesechos.fr, 2021. URL https://www.lesechos.fr/tech-medias/hightech/ la-france-va-consacrer-18-milliard-deuros-aux-technologies- quantiques-1282929. Consulté le 2022/04/05.

[135] La france se dote d'un plan stratégique ambitieux de presque 2 milliards d'euros. itsocial.fr, 2021. URL https://itsocial.fr/enjeux-it/enjeux-innovation/informatique-quantique/informatique-quantique-la- france-se-dote-dun-plan-strategique-ambitieux-de-presque-2- milliards-deuros/. Consulté le 2022/05/02.

[136] Nomination du coordinateur national pour la stratégie quantique. gouvernement.fr, 2021. URL https://www.gouvernement.fr/communique-nomination-du-coordinateur-national-pour-la-strategie-quantique. Consulté le 2022/05/02.

[137] Office parlementaire d'évaluation des choix scientifiques et technologiques. assemblee-nationale.fr, 2021. URL https://www.gouvernement.fr/communique-nomination-du-coordinateur-national-pour-la- strategie-quantique. Consulté le 2022/04/02.

[138] Satellite de communication quantique micius. aerospace-technology.com, Permanent. URL https://www.aerospace-technology.com/projects/micius-quantum-communication-satellite/. Consulté le 2022/04/12.

[139] Id quantique and sk telecom join forces to form the global lea- der in quantum communications and quantum sensing technologies. quantum-computing.ibm.com, 2018. URL https://www.idquantique.com/ id-quantique-sk-telecom-join-forces/. Consulté le 2022/02/28.

[140] Informatique quantique : une question de sécurité. institutmontaigne.org, 2021. URL https://www.institutmontaigne.org/blog/informatique- quantique-une-question-de-securite. Consulté le 2022/03/28.

[141] ANSSI. https ://www.ssi.gouv.fr/uploads/2022/04/anssi-avis-migration-vers- la-cryptographie-post-quantique.pdf. Technical report, ANSSI, 2022. URL https://www.entreprises.gouv.fr/files/files/01-nouveau-portail/ etudes-statistiques/etudes/rapport-mission-quantique.pdf. Consulté le 2022/05/03.

[142] Cryptographie post-quantique : forte présence d'inria au nist. inria.fr, 2019. URL https://www.inria.fr/fr/inria-au-nist. Consulté le 2022/04/03.

[143] ANSSI. Guide de sÉlection d'algorithmes cryptographiques. Technical report, ANSSI, 2022. URL https://www.ssi.gouv.fr/uploads/2021/03/ anssi-guide-selection_crypto-1.0.pdf. Consulté le 2022/05/03.

[144] Anssi - labels. ssi.gouv.fr, 2020. URL https://www.ssi.gouv.fr/en/ products/labels/. Consulté le 2022/05/01.

[145] ANSSI. Guide des mÉcanismes cryptographiques. Technical report, ANSSI, 2020. URL https://www.ssi.gouv.fr/uploads/2021/03/anssi- guide-mecanismes_crypto-2.04.pdf. Consulté le 2022/05/03.

[146] Risq les enjeux du post quantique. risq.fr, 2018. URL https://risq.fr/ events-conf.html. Consulté le 2022/03/22.

[147] Discours du président de la république emmanuel macron sur la stratégie de défense et de dissuasion devant les stagiaires de la 27ème promotion de l'école de guerre. elysee.fr, 2020. URL https://www.elysee.fr/emmanuel-macron/2020/02/07/discours-du-president-emmanuel-macron-sur-la-strategie-de-defense-et-de-dissuasion-devant-les-stagiaires-de- la-27eme-promotion-de-lecole-de-guerre#:~:text=Mesdames%20et%20Messieurs%2C,ici%20depuis%20Charles%20de%20Gaulle. Consulté le 2022/03/18.

[148] La france va consacrer 1,8 milliard d'euros aux technologies quantiques. les echos.fr, 2021. URL https://www.lesechos.fr/tech-medias/hightech/ la-france-va-consacrer-18-milliard-deuros-aux-technologies- quantiques-1282929. Consulté le 2022/05/02.

[149] Israel est devenu une puissance dans le domaine des technologies quantiques. israelvalley.com, 2021. URL https://israelvalley.com/2021/12/07/israel-est-devenu-une-puissance-dans-le-domaine-des-technologies-quantiques/. Consulté le 2022/03/19.

[150] Conflit sino-américain : le quantique, nerf des guerres de demain ? france24.com, 2021. URL https://www.france24.com/fr/éco-tech/20211125-conflit-sino-américain-le-quantique-nerf-des-guerres- de-demain. Consulté le 2022/03/28.

[151] Etats-unis : le budget de l'informatique quantique et de l'ia augmenté de 30% pour 2021. siecledigital.fr, 2020. URL https://siecledigital.fr/2020/08/19/informatique-quantique-etats-unis-budget-2021/. Consulté le 2022/04/14.

[152] Quantique : le gouvernement lance une task force interministérielle pour ne pas rater le virage. 01net.com, 2020. URL https://www.01net.com/actualites/quantique-le-gouvernement-lance-une-task-force-interministerielle-pour-ne-pas-rater-le-virage-1837924.html. Consulté le 2022/04/23.

[153] Discours de florence parly sur la plateforme nationale de calcul quantique. vie-publique.fr, 2022. URL https://www.vie-publique.fr/discours/283167-florence-parly-04012022-plateforme-de-calcul-quantique. Consulté le 2022/05/03.

[154] La chine développe la cryptographie quantique par satellite. cieles-pace.fr, 2020. URL https://www.cieletespace.fr/actualites/la-chine-developpe-la-cryptographie-quantique-par-satellite. Consulté le 2022/04/25.

[155] L'onera dans la deuxième révolution quantique ! onera.fr, 2021. URL https://www.onera.fr/fr/actualites/onera-dans-la-deuxieme- revolution-quantique. Consulté le 2022/04/21.

[156] La marine française pourrait être la première au monde à utiliser cette technologie révolutionnaire. capital.fr, 2022. URL https://www.capital.fr/economie-politique/la-marine-francaise-pourrait-etre-la- premiere-au-monde-a-utiliser-cette-technologie-revolutionnaire- 1429014. Consulté le 2022/04/22.

[157] Nouvelle plateforme de calcul quantique pour des applications multiples. gouvernement.fr, 2022. URL https://www.gouvernement.fr/actualite/nouvelle-plateforme-de-calcul-quantique-pour-des-applications-multiples. Consulté le 2022/04/11.

[158] Direction des applications militaires. dam.cea.fr, 2022. URL http://www-dam.cea.fr/. Consulté le 2022/04/18.

[159] Earthcube convainc les armées et octave klaba de soutenir sa tech-nologie de renseignement. maddyness.com, 2020. URL https://www.maddyness.com/2020/11/19/earthcube-preligens-levee-armees-octave-klaba-renseignement/. Consulté le 2022/04/19.

[160] Unseenlabs renforce son lien avec les armées pour lutter contre la délin- quance en mer. maddyness.com, 2021. URL https://www.maddyness.com/2021/04/27/unseenlabs-satellites-levee-bateaux-armees/. Consulté le 2022/04/16.

[161] An open superconducting quantum computer. QT.eu, Permanent. URL https://qt.eu/about-quantum-flagship/projects/opensuperq/. Consulté le 2022/04/15.

[162] Initiative phare des technologies quantiques. Commission Européenne, 2022. URL https://digital-strategy.ec.europa.eu/fr/policies/quantum- technologies-flagship. Consulté le 2022/03/23.

[163] Institut de recherche interdisciplinaire de grenoble. CEA, Permanent. URL https://www.cea.fr/drf/IRIG/. Consulté le 2022/04/15.

[164] Centre national de la recherche scientifique. neel.cnrs.fr, Permanent. URL https://neel.cnrs.fr. Consulté le 2022/04/12.

[165] Cea-leti : 50 ans de technologies de miniaturisation novatrices. leti- cea.fr, 2022. URL https://www.leti-cea.fr/cea-tech/leti/Pages/Leti/ a-propos-du-Leti/mission-organisation.aspx. Consulté le 2022/04/08.

[166] 2021 academic ranking of world universities. shanghairanking, Permanent. URL https://www.shanghairanking.com/rankings/arwu/2021. Consulté le 2022/04/15.

[167] Le développement des compétences en technologies quantique. oezratty.net, 2020. URL https://www.oezratty.net/wordpress/2020/developpement- competences-technologies-quantiques/. Consulté le 2022/04/21.

[168] Quantum engineering (queng). univ-grenoble-alpes.fr, 2022. URL https: //www.univ-grenoble-alpes.fr/les-cross-disciplinary-programs- cdp-/quantum-engineering-queng--654167.kjsp?RH=1594993584068. Consulté le 2022/03/23.

[169] Diplôme technologies quantique (arteq). ens-paris-saclay.fr, 2022. URL https://ens-paris-saclay.fr/formations/autres-diplomes/diplome-technologies-quantiques-arteq. Consulté le 2022/04/27.

[170] La france, 2ème pays le plus touché au monde par la fuite des cerveaux. helloworkplace.fr, 2017. URL https://www.helloworkplace.fr/france-fuite-cerveaux/. Consulté le 2022/05/04.

[171] Emmanuel Macron. Présentation de la stratégie nationale sur les techno- logies quantiques. Technical report, gouvernement.fr, 2020. URL https: //www.elysee.fr/front/pdf/elysee-module-17093-fr.pdf. Consulté le 2022/05/03.

[172] L'université paris-saclay est le lieu d'un partenariat académie-industrie intense sur les enjeux du quantique. universite-paris-saclay.fr, Permanent. URL https://www.universite-paris-saclay.fr/recherche/thematiques-et-structures/axes-et-grands-projets/quantum-centre-en-sciences-et-technologies-quantiques/un-lieu-dinterface-intense-academie-industrie. Consulté le 2022/05/04.

[173] Use case airbus : Aerospace optimization. qcware.com, Permanent. URL https://www.qcware.com/customers/airbus. Consulté le 2022/05/04.

[174] Quantum computing leaps into the future. atos.net, Permanent. URL https://atos.net/en/insights-and-innovation/quantum-computing. Consulté le 2022/05/04.

[175] Ordinateur quantique : Thales mise sur la recherche pour prÉvenir la "crypto-apocalypse". thalesgroup.com, Permanent. URL https://www.thalesgroup.com/fr/monde/groupe/magazine/ordinateur-quantique-thales-mise-recherche-prevenir-crypto-apocalypse. Consulté le 2022/05/04.

[176] Atos s'associe à total pour combattre le changement climatique grâce aux algorithmes quantiques. atos.net, 2020. URLhttps://atos.net/fr/2020/communiques-de-presse_2020_07_07/atos- sassocie-a-total-pour-combattre-le-changement-climatique-grace- aux-algorithmes-quantiques. Consulté le 2022/05/04.

[177] Les activitÉs d'edf sur les technologies quantiques. universite-paris-saclay.fr, Permanent. URL https://www.universite-paris-saclay.fr/ les-activites-dedf-sur-les-technologies-quantiques. Consulté le 2022/05/04.

[178] Pourquoi tant de start-up étrangères du quantique s'installent en Île-de-france. usinenouvelle.com, 2022. URL https://www.usinenouvelle.com/editorial/pourquoi-tant-de-start-up-etrangeres-du-quantique-s-installent-en-ile-de-france.N1774857. Consulté le 2022/05/04.

[179] Myths vs. reality of quantum computing. hitechnectar.com, 2022. URL https://www.hitechnectar.com/blogs/myths-vs-reality-quantum- computing/. Consulté le 2022/04/05.

A ANNEXE : RSA BREAKER

RSA Breaker is a command line tool to break RSA keys. It is written in Java and uses Wiener's attack.

RSA consists in finding a public key (*n, e*) and a private key (*n, d*) such that
$n = p.q$
and
$e.d = 1 mod (p-1)(q-1)$
Given (*n, e*) this tool can find *d*, i.e. the private key (*n, d*). The algorithm is based on Wiener's attack and is applicable if $d < n^{(1/4)}$.

INSTALLATION

1) from compiled jar :

$wget https ://github.com/Fengtan/rsa-breaker/raw/master/dist/RSABreaker.jar execution :
$java -jar RSABreaker.jar

2) from sources :

$git clone https ://github.com/Fengtan/rsa-breaker.git rsa-breaker
$cd rsa-breaker/
$javac src/*.java -d class/
$jar cvfm dist/RSABreaker.jar MANIFEST.MF -C class/ .

execution :
$java -jar dist/RSABreaker.jar or :
$java -cp class/ RSABreaker

TEST CASES

Test files are in /test
They can be edited with any hex editor, for instance XVI32

**using input numbers in files :
$java -jar RSABreaker.jar -e=test/e1 -n=test/n1

**using input numbers on CLI :
$java -jar RSABreaker.jar -e=2621 -n=8927

**output in a file :
$java -jar RSABreaker.jar -e=2621 -n=8927 -out=./out

**verbose mode :
$java -jar RSABreaker.jar -e=2621 -n=8927 -v LICENSE

MIT License : www.opensource.org/licenses/mit-license.php

https://github.com/fengtan/rsa-breaker

B ANNEXE : LES DIFFÉRENTS CANVAS

Figure 21 – Canva ASSURANCE

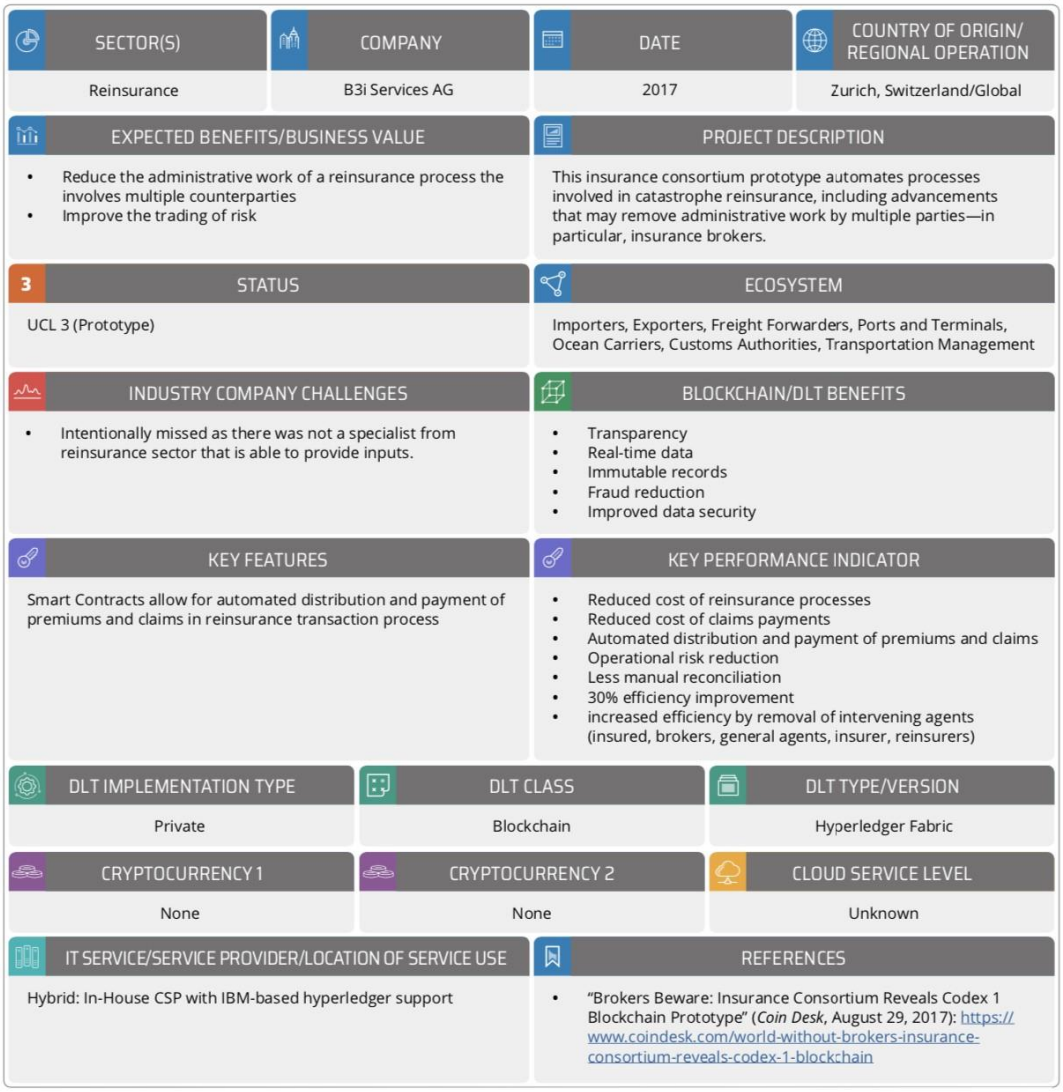

Figure 22 – Canva EDUCATION

EDUCATION

Verification of Identity and Academic Credentials

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Education, Public	University of Melbourne, Australia	October 2017	Australia

EXPECTED BENEFITS/BUSINESS VALUE

- Reduction in use of false certifications and fraudulent credentials

PROJECT DESCRIPTION

A public university in Australia is attempting to issue recipient-owned academic credentials that remain private and unchangeable via blockchain technology in order to provide reliability and security for both recipients and verifiers.

3 STATUS

UCL 3 (Prototype)

ECOSYSTEM

Learning Machine Technologies, MIT Media Lab

INDUSTRY COMPANY CHALLENGES

- Prevention of academic credential fraud

BLOCKCHAIN/DLT BENEFITS

- Ledger stores single confirmation point of academic credentials via distributable "tickets" containing certificate data

KEY FEATURES

- When certificate is issued, data is compressed into hash and logged on blockchain
- Issuer provides a link to their credentials in the certificate
- Verifier validates signature of issuer and certificate data; also ensures certificate status has not expired or been revoked.
- A wallet (IOS- and Android-based) contains issued certificate and evidence required to verify

KEY PERFORMANCE INDICATOR

None yet available

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Public	Blockchain	Bitcoin with Roadmap to Ethereum

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
None	None	N/A

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE

Learning Machine Technologies in partnership with MIT Media Lab/Australia

REFERENCES

- "University of Melbourne to issue recipient-owned blockchain records" (University of Melbourne Newsroom, October 9, 2017): http://newsroom.melbourne.edu/news/university-melbourne-issue-recipient-owned-blockchain-records?_ga=2.100100759.802664920.1507651467-1328473086.1507651452
- "Australian University Tests Blockchain In Bid To Back Up Academic Credentials" (*Coin Desk*, October 10, 2017): https://www.coindesk.com/australian-university-tests-blockchain-bid-back-academic-credentials/
- Blockcerts: The Open Standard for Blockchain Credentials: https://www.blockcerts.org/

Figure 23 – Canva FINANCE

FINANCE

Nostro Bank Account Reconciliations

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Banking	SWIFT	January 2017	Belgium/Global

EXPECTED BENEFITS/BUSINESS VALUE

- Reduced administrative costs
- Improved security of data processing
- Improved security of data storage

PROJECT DESCRIPTION

As part of SWIFT's global payments innovation initiative, which seeks to deliver a new standard in cross-border payments, the company is exploring whether blockchain or DLT can be used by banks to improve reconciliation of their nostro databases in real time.

STATUS

UCL 2 (Proof of Concept)

ECOSYSTEM

Corporate Financial Institutions, SWIFT

INDUSTRY COMPANY CHALLENGES

- Gaps in data and problems with data correlation
- Lack of data centralization and integration
- Cost of exceptions and investigations

BLOCKCHAIN/DLT BENEFITS

- Liquidity savings
- Optimized real-time position management
- Real-time visibility of account entries
- Monitoring intraday expected and available balances
- Operational savings through increased efficiency for Nostro reconciliation

KEY FEATURES

Real-time visibility of end-to-end information for account owners and account servicing institutions utilizing nostro accounts

KEY PERFORMANCE INDICATOR

- Liquidity savings
- Operational cost savings

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Private	Blockchain	Hyperledger Fabric/1.0

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
None	None	IaaS

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE

CSP/IBM/Belgium

REFERENCES

- "SWIFT launches Blockchain Proof of Concept In Hyperledger" (*Blockchain News*, January 12, 2017): http://www.the-blockchain.com/2017/01/12/swift-launches-blockchain-proof-of-concept-in-hyperledger/
- "Swift launches blockchain proof of concept" (*Fintech Futures*, April 25, 2017): http://www.bankingtech.com/698881/swift-launches-blockchain-proof-of-concept/
- "IBM launches blockchain ecosystem on Hyperledger Fabric" (*Fintech Futures*, December 7, 2017): http://www.bankingtech.com/667661/ibm-launches-blockchain-ecosystem-on-hyperledger-fabric/

Figure 24 – Canva ALIMENTATION

FOOD SAFETY

End-to-End Safety and Reliability

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Grocery stores, Supermarket chains and Hypermarkets	Consortium of leading global food supply chain companies in partnership with IBM	August 2017	USA/Global

EXPECTED BENEFITS/BUSINESS VALUE

- Reduction in product losses
- Improved food safety for end users
- Preservation of brand loyalty

PROJECT DESCRIPTION

A group of food retailers are working with IBM to discover how blockchain technology can make the global food supply safer by improving food traceability.

STATUS

UCL 1 (Concept)

ECOSYSTEM

Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Co., McLane Co., Nestlé, Tyson Foods, Unilever, Walmart

INDUSTRY COMPANY CHALLENGES

- Strengthen consumer confidence
- Improve food traceability by providing reliable information about origin and condition of food products (For example, it took more than two months to identify the farm source of contamination in a recent incidence of salmonella in papayas)
- Tracking and addressing food safety problems and distributing information about safety issues

BLOCKCHAIN/DLT BENEFITS

- All players along supply chain, from growers/producers to retailers have access to reliable information about origin, location and condition of food products
- Food contamination issues can be traced quickly; and removed and recalled efficiently
- Information about food contamination can be distributed efficiently, with supporting supply chain data

KEY FEATURES

Database accessible at all points of distribution chain, including producers, wholesalers, transporters, retailers, etc.

KEY PERFORMANCE INDICATOR

Reduction of time identifying origin of food contamination.

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Federated/Consortium (Permissioned)	Non-blockchain	Hyperledger/Fabric

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
None	None	SaaS

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE

Chronicled, a San Francisco-based company, that created the blockchain tools for MediLedgerUSA

REFERENCES

- "IBM Announces Major Blockchain Collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide" (*IBM News Release*, August 22, 2017): http://www-03.ibm.com/press/us/en/pressrelease/53013.wss

Figure 25 – Canva PHARMACEUTIQUE

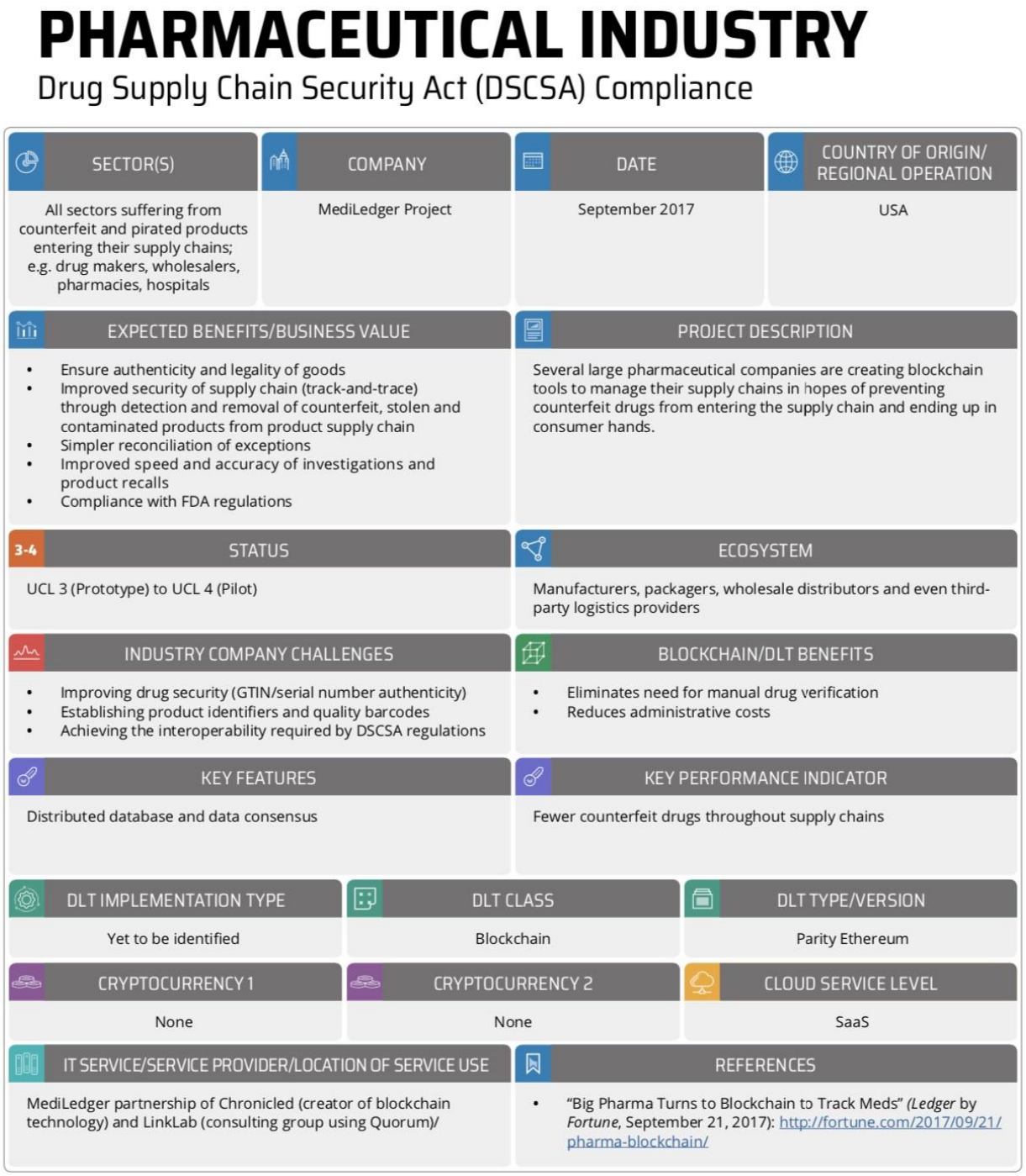

Figure 26 – Canva IMMOBILIER

REAL ESTATE

Transaction Recording

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Real Estate	Cartório de Registro de Imóveis (Real Estate Registry Office of Brazil)	April 2015	Based in USA with partners and advisors worldwide

EXPECTED BENEFITS/BUSINESS VALUE	PROJECT DESCRIPTION
• Improved transparency • Easier contract management • Expedited transactions • Improved storage and access to land title records	This pilot program of a US-based startup and a Brazilian real estate registry aims to efficiently record detailed information about properties and owners that will not be susceptible to fraud, corruption and damage.

4 STATUS	ECOSYSTEM
UCL 4 (Pilot)	Ubiquitous

INDUSTRY COMPANY CHALLENGES	BLOCKCHAIN/DLT BENEFITS
• Simplify and optimize the sale process and the expedient exchange between the parties • Information sharing in a safe and clear fashion	• Greater accuracy and immutability of property ownership data

KEY FEATURES	KEY PERFORMANCE INDICATOR
Detailed records of real estate information, including property addresses, owners and zoning classifications	Efficient transition from paper-based records to immutable computer-based data

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Public	Blockchain	Ubitquity Platform Blockchain/Version 1.1, Colu's API (alpha)

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
None	None	SaaS (Ubitquity)

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE	REFERENCES
CSP using Ubitquity API	• "Blockchain Land Registry Tech Gets Test in Brazil" (*Coin Desk*, April 5, 2017): https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil/

Figure 27 – Canva LOGISTIQUE

SHIPPING

End-to-End Supply Chain Visibility

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Transportation	Maersk *(world's largest container shipping company)*	January 2018	Denmark/Global

EXPECTED BENEFITS/BUSINESS VALUE

- Reduced cost of processing transactions
- End-to-end visibility and reporting
- Reduced documentation workload
- End-to-end documentation
- Faster document processing
- Increased accuracy of document processing

PROJECT DESCRIPTION

In partnership with IBM, Maersk envisions a digitized and paperless shipping solution in which all parties can view cargo and approve its movement throughout transport.

3-4 STATUS

UCL 3 (Prototype) to UCL 4 (Pilot)

ECOSYSTEM

Importers, Exporters, Freight Forwarders, Ports and Terminals, Ocean Carriers, Customs Authorities, Transportation Management

INDUSTRY COMPANY CHALLENGES

- Inconsistent information across organizational boundaries and "blind spots" throughout supply chain hinder efficient flow of goods
- Complex, cumbersome, and costly peer-to-peer messaging
- Manual, time-consuming, paper-based processes
- High air courier expense
- Air courier delays
- Risk assessments lacking sufficient information; clearance processes subject to fraud
- The administrative cost of handling a container shipment is on par with the cost of its transport.

BLOCKCHAIN/DLT BENEFITS

- Fast access to end-to-end information
- Proven data security
- Single information source
- Verifiable authenticity
- Immutability of digital documents
- Efficient, cross-organizational workflows
- Improved risk assessment due to complete data
- Fewer manual interventions
- Lower administrative costs

KEY FEATURES

Smart Contracts

KEY PERFORMANCE INDICATOR

- Reduced administrative costs
- Fewer interventions due to lost/missing information
- Increased speed to problem resolution

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Permissioned	Blockchain	Hyperledger Fabric/1.0

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
None	None	SaaS

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE

CSP/IBM/Denmark

REFERENCES

- "Maersk, IBM create world's first blockchain-based, electronic shipping platform" (*Computer World*, January 16, 2018): https://www.computerworld.com/article/3247758/emerging-technology/maersk-ibm-create-worlds-first-blockchain-based-electronic-shipping-platform.html
- "Digitizing Global Trade with Maersk and IBM" (*IBM Announcements*, January 16, 2018): https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/

Figure 28 – Canva TICKETING

TICKETING

Automated Airline Ticket Sales

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Transportation, potentially Entertainment	S7 Airlines (PJSC Siberia Airlines)	July 2017	Russia/Eastern Europe

EXPECTED BENEFITS/BUSINESS VALUE

- Reduced documentation
- Faster document processing
- Improved accuracy of document processing
- Timely payment
- Fair ticket distribution (reduced scalping)
- Elimination/Reduction of counterfeit tickets

PROJECT DESCRIPTION

With financial support from one of the largest private banks in Russia, a Russian airline will sell tickets using blockchain technology. The airline is exploring the use of cryptocurrency for flight tickets, as well.

5 STATUS

UCL 5 (Pilot Production)

ECOSYSTEM

Customer, S7 Ticket Agents, S7 Airline, Alfa Bank JSC

INDUSTRY COMPANY CHALLENGES

- Inefficient document handling
- Slow payment processing time, with average settlements taking two weeks
- Excessive receivables investment

BLOCKCHAIN/DLT BENEFITS

- Automated document handling
- Automated contract fulfillment
- Reduction of documentation errors
- Increased transaction settlement time
- Reductions in costs and investments

KEY FEATURES

Smart Contracts

KEY PERFORMANCE INDICATOR

Pilot phase resulted in average payment settlement time reduced from 14 days to 23 seconds

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Private	Blockchain	Ethereum

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
Ether	None	IaaS

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE

CSP/IT-Grad/Russia

REFERENCES

- "Russian Airline S7 Now Uses the Ethereum Blockchain for Flight Tickets" (*Crypto Coins News*, July 25, 2017): https://www.cryptocoinsnews.com/russian-airline-s7-now-uses-ethereum-blockchain-flight-tickets/
- "Russian Airline At Home in the Cloud" (*Computer Weekly*, March 29, 2017): http://www.computerweekly.com/news/450415777/Russian-Airline-at-home-in-the-cloud

Figure 29 – Canva CHAÎNE D'APPROVISIONNEMENT

SUPPLY CHAIN

Logistics Management for Buyers and Sellers

SECTOR(S)	COMPANY	DATE	COUNTRY OF ORIGIN/ REGIONAL OPERATION
Supply Chains	Skuchain in partnership with NTT Data	January 2018	USA and Japan/USA

EXPECTED BENEFITS/BUSINESS VALUE

- Trackable flow of goods
- Bank-grade traceability of physical assets

PROJECT DESCRIPTION

Aiming to empower collaboration across all partners in individual global supply chains, Skuchain connects buyers and sellers in real time via blockchain technology and internet ofthings (IoT) innovations, while also ensuring data privacy and security.

STATUS

UCL 2: Proof of Concept

ECOSYSTEM

Skuchain, NTT Data

INDUSTRY COMPANY CHALLENGES

- Managing the complexity of global supply chain logistics
- Reliable traceability at all nodes along transport
- Improve supply chain efficiency and quality control

BLOCKCHAIN/DLT BENEFITS

- End-to-End Track and Trace technology to monitor goods at all nodes on supply chain
- Reliable tracking of invoicing, financing, records management, etc.
- Collaboration among multiple parties
- Reduction of stock wastage
- Increased efficiency and control cver movement and sale of products

KEY FEATURES

Smart Contracts

KEY PERFORMANCE INDICATOR

None yet available

DLT IMPLEMENTATION TYPE	DLT CLASS	DLT TYPE/VERSION
Federated/Consortium (Permissioned)	Blockchain	Hyperledger Fabric/1.0

CRYPTOCURRENCY 1	CRYPTOCURRENCY 2	CLOUD SERVICE LEVEL
None	None	SaaS

IT SERVICE/SERVICE PROVIDER/LOCATION OF SERVICE USE

CSP/ Skuchain /USA

REFERENCES

- "Skuchain uses blockchain and IoT for new supply chain platform" (Global Trade Review, January 24, 2018): https://www.gtreview.com/news/fintech/skuchain-uses-blockchain-and-iot-to-launch-supply-chain-platform/