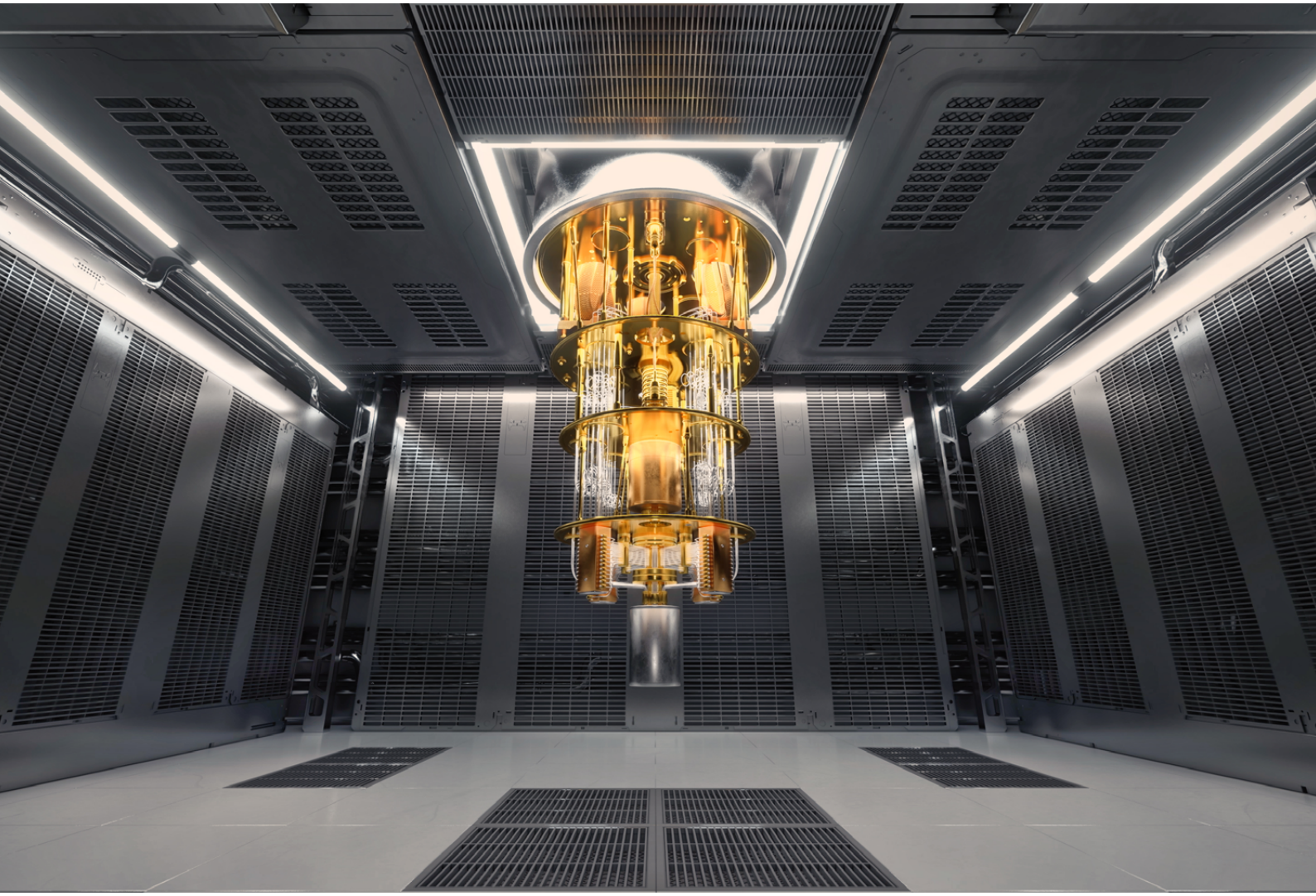
Les opportunités des technologies quantiques pour les entreprises

Livre blanc



orange™

Préface

Le quantique s’impose désormais comme un domaine stratégique, porteur de ruptures technologiques majeures pour les entreprises. Communications ultra-sécurisées, cryptographie post-quantique, nouveaux paradigmes de calcul : les promesses sont nombreuses, mais exigent dès aujourd’hui un positionnement clair, une acculturation active, et une stratégie structurée. Pour Orange, acteur numérique by design, les technologies quantiques représentent à la fois un enjeu scientifique, une opportunité industrielle et un impératif de souveraineté.

Dans un paysage mondial en recomposition, la France tire son épingle du jeu. Portée par un écosystème de start-ups de pointe et par une excellence scientifique reconnue, elle se positionne comme l’un des pôles les plus dynamiques du quantique. Orange, avec ses équipes de recherche, ses projets en coopération avec des laboratoires prestigieux et plus d’une dizaine de thèses dédiées au quantique, participe activement à cet élan. Cette dynamique ne se limite pas à l’expérimentation : elle s’incarne dans des démonstrateurs concrets.

Trois champs structurent aujourd’hui l’approche du quantique : la cybersécurité, les communications, et le calcul. Orange est présent sur chacun de ces volets. Sur la cybersécurité, l’enjeu est immédiat : les solutions de cryptographie post-quantiques deviennent nécessaires pour anticiper l’obsolescence des protocoles actuels face aux capacités des futurs calculateurs quantiques. Sur les réseaux, Orange s’investit dans la construction d’infrastructures capables de supporter des échanges protégés par les lois de la physique. Et sur le calcul, l’entreprise développe les capacités d’intégration, de simulation et de projection pour exploiter les futurs gains algorithmiques au bénéfice de ses clients.

L’année 2025 marque un tournant. Non pas une rupture brutale, mais une phase d’ancrage industriel. Le quantique commence à irriguer les stratégies technologiques des grandes entreprises. Il entre dans le champ des décisions de DSI, de directions de la sécurité, de responsables innovation. Se préparer aujourd’hui, c’est comprendre ses implications, auditer son exposition aux risques, identifier les cas d’usage pertinents et évaluer les investissements nécessaires.

C’est dans cet esprit qu’Orange agit. Ses équipes accompagnent les entreprises avec une ambition claire : aider à décrypter, structurer et anticiper l’intégration du quantique dans les feuilles de route technologiques. Tant que possible en favorisant les pépites françaises. Notre ambition est de vous permettre de comprendre ce changement de paradigme et de devenir « quantum ready ».

Lyse Brillouet,
Executive Vice President Research
ORANGE

Sommaire

Aux origines
de la physique quantique

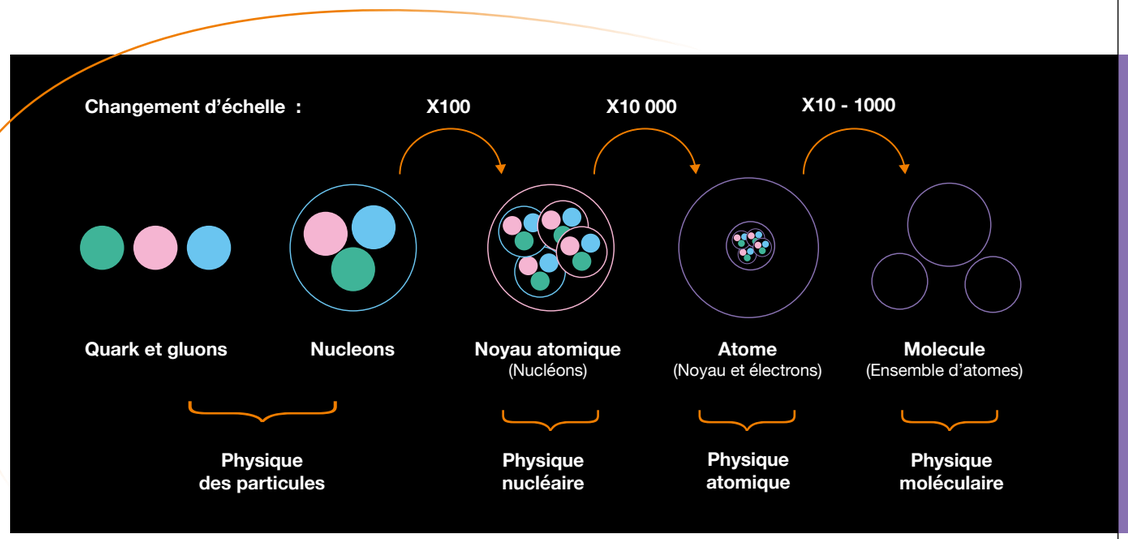
Si, la physique quantique est à l'origine de nombreuses découvertes techniques, la maturité des applications quantiques est encore en devenir. Les technologies quantiques sont aujourd'hui au centre d'une dynamique de recherche internationale inédite. Retour sur les fondements de cette physique et sur plus de 100 ans de découvertes.

De la physique quantique de Planck ...

Au début du XXe siècle, Max Planck pose les bases d'une conception nouvelle de la physique pour décrire le **comportement de la matière à l'échelle atomique**. Pour Planck l'énergie ne se propage pas de manière continue, mais par petits paquets discrets qu'il appelle **quanta**. L'hypothèse de Planck permet d'expliquer le rayonnement de corps noir, un problème majeur de la physique que les lois classiques ne parvenaient pas à résoudre. Einstein, Schrödinger ou Heisenberg poseront les bases de cette nouvelle physique. Les transistors, lasers, horloges atomiques et l'IRM seront créés sur la base de ces théories.

Les quantas

Un quanta est la plus petite quantité indivisible d'une grandeur physique pouvant être échangée, émise ou absorbée.

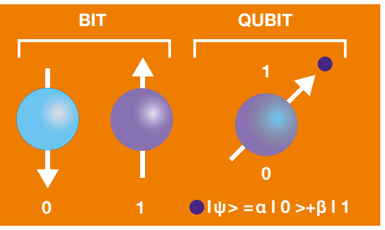


... À l'ordinateur quantique de Benioff

Dans les années 1980 Paul Benioff propose le concept d'ordinateur quantique. Son ambition : démontrer que les machines de Turing peuvent fonctionner avec les lois de la mécanique quantique. Si les ordinateurs classiques traitent l'information à l'aide de bits (0 ou 1), les ordinateurs quantiques utilisent des **qubits**. Ils ont la capacité de représenter simultanément plusieurs états grâce à la superposition. Cette spécificité permet de réaliser des **calculs parallèles**, ce qui ouvre la voie à une puissance de traitement inédite. Il faudra attendre 10 ans pour que les travaux de Benioff soient pleinement reconnus par la communauté scientifique internationale.

les qubits

Un qubit est l'unité de base de l'information quantique : contrairement à un bit classique qui vaut 0 ou 1, un qubit peut être simultanément dans une superposition des deux états. Ceci peut se représenter sous la forme de la sphère de Bloch :



Le paradigme du gap technologique

Paul Benioff subit le principe de la vallée de la mort. Ce concept illustre en théorie de l'innovation le point ou une idée n'est pas concrétisée faute de moyens technologiques pour être mise en œuvre. Benioff ouvre une nouvelle voie. Son travail inspire des chercheurs comme Richard Feynman et David Deutsch, qui poursuivent le développement du domaine. Aujourd'hui, la recherche bat son plein.

Le défi de la décohérence quantique

Les ordinateurs quantiques sont encore instables en raison de la fragilité extrême des qubits. La principale cause d'instabilité est la décohérence quantique. Lorsqu'un qubit interagit avec son environnement (lumière, chaleur, vibrations), il perd ses propriétés quantiques et se comporte comme un bit classique. Ce qui interrompt le calcul et détruit l'information. Les erreurs de manipulation sont également un facteur clé de perturbation quantique.
Pour réduire ces effets et optimiser leur capacité de calcul, la plupart des ordinateurs quantiques doivent être maintenus à des températures proches du zéro absolu, ce qui complique leur fonctionnement. Pour surmonter ces difficultés, les chercheurs tentent de développer des qubits logiques construits à partir de plusieurs qubits physiques, et utilisent des techniques de correction d'erreurs.

Les principes fondamentaux de la physique quantique

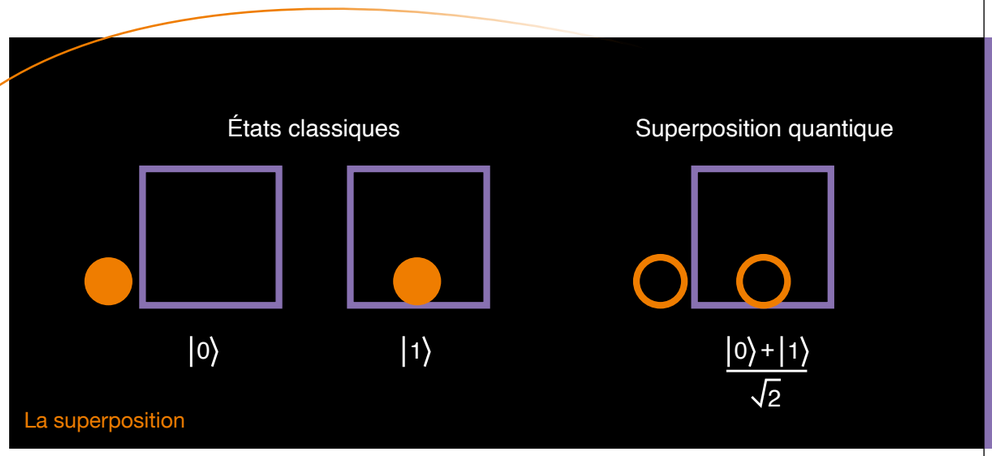
Superposition, intrication, dualité onde-particule, quantification : ces quatre piliers de la physique quantique défient notre intuition classique et constituent la base des technologies quantiques actuelles, ouvrant la voie à de nouvelles architectures de calcul, de communication et de mesure.

La superposition

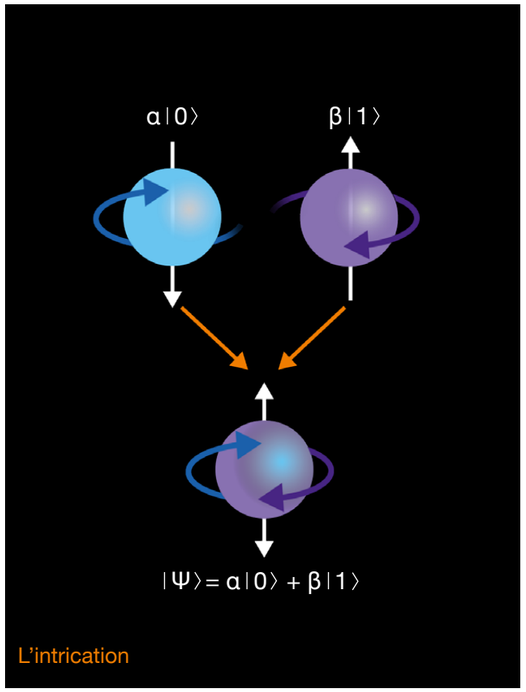
La superposition est un principe non intuitif selon lequel une particule quantique peut exister dans **plusieurs états simultanément**. Cette propriété permet à un qubit d'être à la fois 0 et 1, ouvrant la voie à une capacité de calcul exponentielle. Cette propriété est extrêmement fragile, les quanta tout comme les qubits sont instables, la moindre interférence externe peut faire varier leur état. Cette fragilité est appelée décohérence. Bruit thermique, rayonnements, vibrations, etc. dès qu'un qubit interagit avec son environnement, il perd sa superposition.

L'intrication

Deux particules intriquées voient leurs **états corrélés** instantanément, quelle que soit la distance qui les sépare. Autrement dit, dans un système intriqué, les états individuels ne peuvent plus être décrits indépendamment : la connaissance de l'état d'un qubit informe instantanément sur l'état de l'autre. L'intrication est un principe théorique de la physique quantique défini par Einstein et confirmé expérimentalement quelques années plus tard.



La superposition



L'intrication

La quantification

La quantification postule que certaines grandeurs physiques — l'énergie, la lumière, ou encore le moment cinétique d'une particule — existent uniquement sous forme de valeurs précises et **discrètes**. Contrairement à ce que l'on observe en physique classique, où une valeur peut varier de manière continue (par exemple, la vitesse d'une voiture qui peut passer progressivement de 10 à 11 km/h), la quantification impose des paliers, telles des « marches d'escalier » que l'on ne peut pas franchir partiellement.

L'incertitude

Le principe d'incertitude d'**Heisenberg** stipule que l'on ne peut jamais connaître avec une précision absolue (1) la **position** d'une particule (où elle se trouve) ; et (2) sa quantité de **mouvement** (c'est-à-dire sa vitesse et sa direction). Ce n'est pas un problème d'instrument ou de technologie : c'est une limite imposée par la nature même de la réalité quantique. Ce principe bouleverse la vision classique du monde, où l'on imagine pouvoir tout mesurer avec une précision infinie si l'on dispose des bons instruments. En mécanique quantique, l'observateur fait partie du système observé, et **chaque mesure influence inévitablement ce que l'on observe**.

Le chat de Schrödinger

Cette expérience de pensée est formulée en 1935 par le physicien autrichien Erwin Schrödinger. Elle illustre les implications de la superposition quantique et les limites de son application aux objets macroscopiques. Un chat est enfermé dans une boite dans laquelle se trouvent un poison mortel, un marteau et un atome. Si l'atome se désintègre, le marteau est actionné, il casse le flacon contenant le poison, celui-ci se libère et le chat meurt, si non, celui-ci survit. Tant que la boite est fermée, le chat est à la fois vivant et mort. Les quantas ont théoriquement la propriété d'être de ne pas être figés dans un état. Cependant, dès qu'un observateur externe ouvre la boite, le chat sera soit mort, soit vivant. Cette représentation permet de comprendre plusieurs choses. (1) Un quanta est dans le monde quantique susceptible d'avoir deux valeurs, être ou ne pas être. Ce qui est n'est pas envisageable dans le monde macroscopique. (2) Toute mesure d'un état quantique fige la superposition des quantas.

Les quatre principales familles de technologies quantiques

Amorcée dans les années 2000, la seconde révolution quantique entend contrôler les qubits. Communication, cryptographie, métrologie, calcul ... en l'espace de 20 ans, les progrès sont là. De nombreuses applications de ces technologies fonctionnent avec succès en France et à l'international.

La communication quantique

La communication quantique concerne le **transport ou l'échange d'informations** encodés dans un système quantique. Si les réseaux classiques utilisent des signaux électriques ou optiques pour véhiculer des données binaires, les réseaux quantiques reposent sur la transmission de qubits via des photons pour transmettre l'information. La communication quantique est centrale en ce qu'elle permet l'interconnexion de différents composants d'un écosystème quantique, qu'il s'agisse d'ordinateurs quantiques, de capteurs ou de dispositifs cryptographiques. Les développements actuels se concentrent sur la création de réseaux capables de transporter des qubits à longue distance avec une atténuation minimale. Si la recherche avance, les défis techniques restent considérables.

La communication classique versus la communication quantique

Communication classique	Communication quantique
■ Un usage de signaux électriques (filaire) ou d'ondes électromagnétiques (radio) ■ Permet le transfert de données numériques	■ Transmission de données via des états quantiques (ex : photons uniques) au lieu de signaux classiques ■ Permet la distribution de clés quantiques. ■ Une sécurisation basée sur les lois physiques de la nature

Les principaux cas d'application de la communication quantique

1. **Défense / diplomatie :** Confidentialité absolue, résistance aux interceptions
2. **Cloud souverain :** Échanges entre data centers critiques
3. **Santé et souveraineté sanitaire :** Échange sécurisé de données patients (inter-hôpitaux, biobanques)
4. **Transmission inter-bancaire sécurisée**, synchronisation des marchés
5. **Sécurisation des transferts de propriété intellectuelle** et résistance à l'espionnage industriel

La cryptographie post-quantique

La cryptographie post-quantique est l'une des applications technologiques les plus prometteuses, notamment du fait du développement exponentiel des enjeux de cybercriminalité. Son principe repose sur le protocole BB84 développé par Charles Bennett et Gilles Brassard en 1984. Premier protocole de d**istribution quantique de clés (QKD, pour Quantum Key Distribution)**, le BB84 repose sur deux principes fondamentaux de la mécanique quantique : (1) Le **principe d'incertitude de Heisenberg**, qui empêche toute mesure d'un état quantique sans le perturber et (2) le **théorème de non-clonage**, qui stipule qu'il est impossible de copier un état quantique inconnu sans le modifier. **La cryptographie post-quantique ne repose pas sur la difficulté calculatoire, mais sur les lois fondamentales de la physique, ce qui en fait un outil de sécurité intrinsèquement inviolable**. Aujourd'hui, la cryptographie post-quantique, bien que toujours en phase de maturité technologique, connaît des premiers succès opérationnels.

Alice, Bob et Eve

En cryptographie post-quantique, le scénario classique met en scène trois personnages : Alice, Bob et Eve. Alice souhaite envoyer à Bob une clé secrète à l'aide de la distribution quantique de clés (QKD). Pour ce faire, elle encode des bits sous forme d'états quantiques et les transmet à Bob. Ce dernier mesure ces états dans des bases aléatoires. Alice et Bob comparent publiquement les bases utilisées pour ne conserver que les bits correspondant à des bases identiques, formant ainsi une clé commune. Eve, une éventuelle espionne, tente d'intercepter la communication. Toutefois, en raison du principe d'incertitude de Heisenberg et du théorème de non-clonage, toute tentative d'interception perturbe les états quantiques et introduit des erreurs détectables par Alice et Bob.

La cryptographie classique versus la cryptographie post-quantique

Cryptographie classique	Cryptographie post-quantique
■ Un chiffrement basé sur des algorithmes mathématiques : RSA, AES, ECC ■ Fiabilité corrélée à la capacité de résoudre des problèmes mathématiques complexes ■ Peut être brisée par des calculateurs suffisamment puissants	■ Utilisation d'algorithmes spécialement conçus pour résister aux attaques des ordinateurs quantiques ■ Diversification algorithmique : Adoption d'approches variées afin de limiter les risques en cas d'échec d'une méthode spécifique ■ Interopérabilité et évolutivité : Conception flexible permettant une transition progressive

Les principaux cas d'application de la cryptographie post quantique

1. **Communications gouvernementales et militaires :** sécurisation des données sensibles via la transmission de message exploitant la distribution quantique de clés (QKD).
2. **Réseaux de communication quantique :** à destination des entreprises exploitant de futurs réseaux quantiques ou des infrastructures hybrides (infrastructures quantiques et classiques).
3. **Secteurs industriels à haute sécurité :** dans le secteur de l'énergie notamment pour la sécurisation des communications entre équipements critiques.
4. **Banque et finance :** utilisation de protocoles QKD dans la sécurisation des échanges bancaires.

Le calcul quantique

Avec la superposition d'état des qubits, les calculateurs quantiques ouvrent la voie à une forme de **calcul parallèle** radicalement nouvelle. Les perspectives sont majeures pour la modélisation des systèmes moléculaires complexes, la résolution des problèmes d'optimisation combinatoire ou encore en intelligence artificielle, en cryptographie post-quantique et en simulation de phénomènes physiques. Reste un frein majeur, la décohérence. **La mise au point d'un système tolérant aux fautes, capable de corriger les erreurs sans compromettre l'intégrité des calculs, est donc un enjeu clé**. Ainsi, plusieurs architectures matérielles se concurrencent actuellement : supraconducteurs, ions piégés, atomes neutres, photons intriqués, spin/silicium et qubits topologiques.

Les technologies en développement pour maîtriser les qubits

L'implémentation physique des qubits constitue un enjeu central du développement de l'informatique quantique. Plusieurs technologies coexistent, chacune avec ses avantages, ses limites techniques et son niveau de maturité. La diversité technologique actuelle reflète l'absence d'un consensus sur l'architecture optimale. Chaque technologie permet de traiter des usages spécifiques tels que la simulation, l'optimisation, la communication.

Les ordinateurs classiques versus les ordinateurs quantiques

Informatique classique	Informatique quantique
■ Stocke les informations sous forme de bits avec un nombre discrets d'états possibles 0/1. ■ Traite les données de manière logique et séquentielle.	■ Stocke les informations sous forme de qubits sous forme de 0/1 ou d'une superposition de 0/1. ■ Traite des données avec une logique quantum sur des instances parallèles

Les principaux cas d'application du calcul quantique

1. **Chimie et pharmacie :** pour la modélisation moléculaire, la conception de médicaments, ou l'optimisation de catalyseurs.
2. **Finance :** pour l'optimisation de portefeuille, la détection de corrélations complexes, et la simulation de scénarios de risque.
3. **Énergie :** dans la gestion intelligente des réseaux, l'optimisation du stockage ou la modélisation des matériaux pour les batteries.
4. **Logistique et transport :** pour la résolution de problèmes d'optimisation combinatoire, comme les itinéraires ou la gestion de flotte.
5. **Industrie manufacturière :** dans la simulation de matériaux, l'automatisation de procédés et la maintenance prédictive.
6. **Climat et environnement :** pour modéliser des systèmes complexes et prévoir des évolutions climatiques.

1998 — Première démonstration expérimentale réalisée avec 2 qubits

2001 — IBM et l'université de Stanford factorisent le nombre 15 avec 7qubits.

2007 à 2011 — D-Wave propose le premier ordinateur quantique commercial.

2008 — Le processeur 54 qubits de Google résout en 3 minutes un problème qui aurait pris 3000 ans à un supercalculateur.

2025 — Les ordinateurs quantiques dits NISQ sont opérationnels, mais encore instables.

La métrologie quantique

La métrologie quantique permet de dépasser les limites imposées par la physique classique, notamment dans la détection de champs magnétiques, de forces, de temps ou de gravité. En augmentant la résolution des instruments de mesure, la métrologie quantique ouvre la voie à de nombreux usages civils, industriels et militaires. Il existe aujourd'hui plusieurs technologies de métrologie quantique, certaines sont déjà utilisées dans des applications industrielles de pointe. L'un des exemples les plus emblématiques est celui des horloges atomiques de nouvelle génération qui permettent de définir le temps avec une précision sans précédent, utile notamment pour la synchronisation des systèmes de navigation par satellite. Comme l'ensemble des technologies quantiques, la métrologie implique plusieurs défis techniques majeurs, dont la maîtrise de la décohérence quantique.

Métrologie classique versus métrologie quantique

Métrologie classique	Métrologie quantique
■ Utilise des capteurs fondés sur les lois de la physique classique (électromagnétisme, mécanique, thermodynamique). ■ La précision est limitée par le bruit thermique, les fluctuations classiques et les contraintes instrumentales. ■ Capacité limitée à sonder les phénomènes à l'échelle atomique ou subatomique.	■ Utilise des capteurs exploitant les propriétés de la mécanique quantique (superposition, intrication, effet tunnel). ■ Permet d'atteindre des niveaux de précision au-delà des limites classiques grâce à des effets quantiques comme le bruit réduit (états comprimés). ■ Capacité à sonder avec une extrême sensibilité des phénomènes à l'échelle atomique, moléculaire ou quantique.

Les principaux cas d'application de la métrologie quantique

1. **Santé & imagerie médicale :** pour améliorer la résolution des IRM, développer de nouvelles techniques de tomographie ou détecter précocement certaines pathologies grâce à une sensibilité accrue des capteurs.
2. **Navigation & spatial :** remplacer ou compléter les systèmes GPS dans des environnements inaccessibles (sous-sols, espaces confinés, sous-marins) via des gyroscopes et accéléromètres quantiques à haute précision.
3. **Défense & sécurité :** détection d'anomalies gravitationnelles ou magnétiques pour repérer des objets dissimulés ou des activités souterraines ; applications dans les systèmes de surveillance avancée.
4. **Environnement & géophysique :** mesure fine des variations du champ gravitationnel terrestre, surveillance des nappes phréatiques, analyse des sols, ou suivi des mouvements tectoniques.

INTERVIEW

Frédéric Barbaresco
KTD PCC Quantum
Algorithms & Computing Segment Leader
THALES

> **Le quantique entre dans une phase industrielle. Il est urgent de s'y préparer.**

Où en est la maturité des technologies quantiques ?

Nous assistons à une montée en puissance des technologies quantiques. Dans le domaine du calcul quantique, certains supercalculateurs offrent déjà des **gains significatifs**, pour résoudre des problèmes dans l'ingénierie ou les opérations par exemple, où les ordinateurs classiques atteignent leurs limites. Nous restons dans une logique de machines NISQ ou analogiques, donc limitées en taille et en précision, mais le potentiel est déjà perceptible.

Dans ce contexte, le **projet BACQ (Benchmark Applicatif des Calculateurs Quantiques)** du programme MetriQs du LNE, que pilote Thales avec le CEA, Eviden, le CNRS et TERATEC, vise à offrir une vision pragmatique des performances des calculateurs quantiques. Nous cherchons à évaluer quel supercalculateur est le plus efficace sur un cas d'usage industriel précis. C'est une approche orientée « utilisateur final », qui rencontre un fort intérêt, avec des réflexions en cours pour la valoriser au niveau européen. Elle pourrait devenir un standard utile pour accompagner les choix technologiques des entreprises.

Pourquoi les entreprises doivent-elles s'emparer dès maintenant du sujet quantique ?

Il est stratégique que les entreprises s'approprient ces sujets dès aujourd'hui. Plusieurs grands groupes en France l'ont compris : en plus de Thales, on peut citer EDF, La Poste, le Crédit Agricole. Il s'agit d'organisations disposant de fortes capacités en algorithmique et confrontées à certaines limites computationnelles concrètes des approches classiques.

Mais les freins sont réels. La diversité des technologies, des environnements logiciels de programmation et l'absence de standards peuvent déstabiliser les décideurs. Sans parler des enjeux de souveraineté, dans un contexte où l'accès aux calculateurs sera restreint par des contraintes d'exportations. Face à cela, quelques bonnes pratiques émergent. D'abord, **partir d'un cas d'usage bien identifié** où le quantique peut faire la différence. Ensuite, **bâtir une équipe transverse** mêlant métiers et experts algorithmes pour structurer ce besoin. Enfin, **planifier la transition** vers le quantique. In fine, **ces technologies vont être matures à court et moyen termes. Il est préférable de se préparer dès à présent**.

Une compétition internationale inédite

Face aux enjeux de souveraineté et d'avantages stratégiques, la course aux technologies quantiques s'intensifie entre les grandes puissances. Chaque nation ambitionne d'être leader dans cette révolution technologique qui redessine les rapports de force économiques et militaires.

Un marché porté par une constellation d'acteurs

Les technologies quantiques sont aujourd'hui développées par une **constellation d'acteurs industriels et académiques répartis entre l'Amérique du Nord, l'Europe et l'Asie**. Aux États-Unis, des entreprises comme IBM, Google, Microsoft, Rigetti Computing, Amazon, Honeywell et IonQ figurent parmi les pionniers, chacune développant des architectures de qubits distinctes (supraconducteurs, ions piégés, topologiques). La Chine dispose également de ses propres champions. Alibaba, Baidu ou l'Université des sciences et technologies de Chine (USTC) reçoivent des investissements massifs de l'État pour accélérer le développement technologique de la nation chinoise. En Europe, des startups innovantes comme Pasqal, Quandela, Alice & Bob en France, River Lane en Angleterre, PlanQC en Allemagne ou IQM en Finlande portent haut les couleurs du quantique sur le devant de la scène internationale.

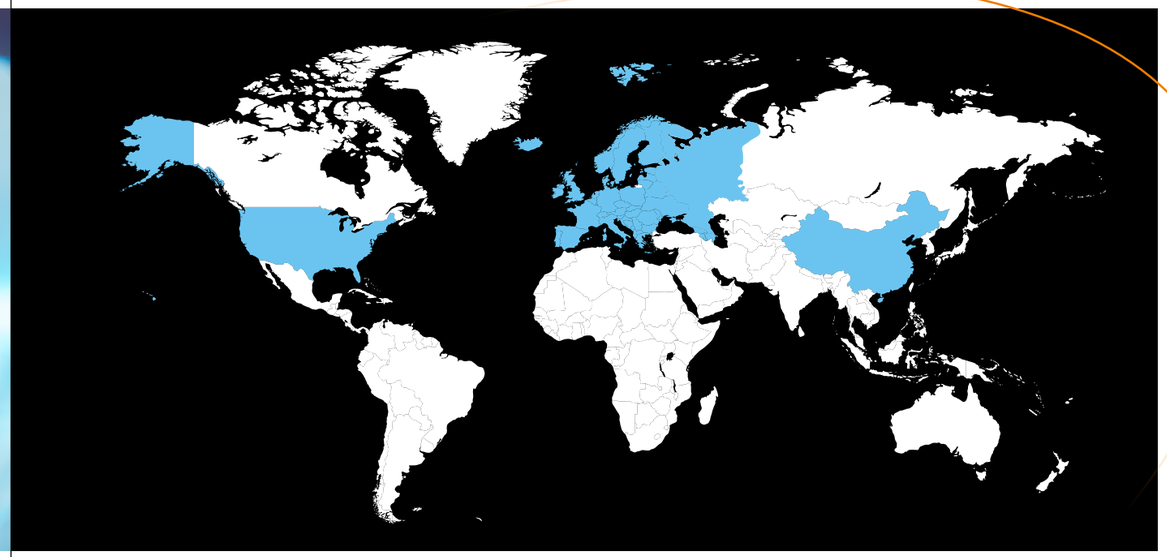
Des disparités étatiques fortes

La compétition étatique autour des technologies quantiques s'apparente aujourd'hui à **une véritable course géopolitique, comparable à celle du développement de l'internet et du cloud**. Trois puissances dominent actuellement cette dynamique : les États-Unis, la Chine et l'Union européenne.

Les États-Unis adoptent une approche fondée sur l'innovation par le secteur privé, soutenu par des programmes publics ciblés comme le National Quantum Initiative Act. Le pays capitalise sur une dynamique business extrêmement forte qui **associe la recherche universitaire** (MIT, Caltech, etc.), les **aides d'État** (DARPA, NIST) et la domination technologique de **géants de la tech** (IBM, Microsoft, Google).

La Chine, de son côté, suit une trajectoire ancrée dans une **planification à long terme** de son développement technologique. Une dynamique doublée d'une **capacité d'investissement forte**. La Chine aurait ainsi investi plus de 15 milliards USD dans la R&D quantique. Les priorités de la Chine sont notamment liées au développement de satellites de communication quantique et d'applications militaires. Le pays est le **premier en volume de publications** scientifiques dans le secteur du quantique.

L'Union européenne est engagée dans une **dynamique de coordination** des différents programmes de ses États membres. Les programmes de coopération **Quantum Flagship** et **QuantERA** réunissent un budget de plus d'un milliard d'euros pour les dix prochaines années. L'Europe dispose également de **centres universitaires de pointe** (CNRS, Max Planck, CEA) et d'un **écosystème foisonnant de startups** réparties sur l'ensemble de son territoire. L'investissement public des nations européennes avoisine les **13 milliards d'euros**.



Géopolitique
des investissements mondiaux

Avec plus de 40 milliards de dollars investis, les stratégies nationales se distinguent : la Chine privilégie l'investissement public massif, les États-Unis s'appuient sur leur secteur privé, tandis que l'Europe tente de structurer un écosystème fédéré autour de projets transnationaux.

Focus sur les financements privés : les États-Unis, la Chine et l'Union européenne

Les investissements privés mondiaux jouent un **rôle déterminant dans la compétition** pour le développement de technologies quantiques. La répartition géographique des capitaux met en lumière une concentration significative dans les pays anglo-saxons.

Les États-Unis captent à eux seuls près de **44 %** des investissements privés globaux dans le quantique, portés par un **écosystème mature** combinant capital-risque, soutien public indirect et leadership industriel (IBM, Google, Microsoft).

La Chine, bien que **dominante dans les investissements publics**, mobilise également 17 % du capital privé, en grande partie via des acteurs étatiques ou semi-publics.

L'Union européenne, malgré une excellence scientifique reconnue, peine à attirer les financements privés, avec une part inférieure à 13 %, illustrant un **déséquilibre structurel entre recherche académique et valorisation industrielle**.

Tableau récapitulatif des financements cumulés des grands acteurs mondiaux issus du marché quantique (en millions de $)

SandboxAQ	US	$ 950.0
XtalPi Technology	China	$ 862.9
IONQ	US	$ 825.9
D-Wave	Canada	$ 750.0
Quantinuum	US	$ 625.0
Rigetti Computing	US	$ 571.5
China Telecom Quantum Group	China	$ 424.2
QuantumCTek	China	$ 352.9
Xanadu	Canada	$ 282.4

L'Europe face au défi de la coordination entre l'Union et ses industries

Structurer un écosystème d'investissement attractif, capable de rivaliser avec les hubs nord-américains ou asiatiques, est une condition sine qua non pour faire du quantique un levier économique et stratégique à l'échelle du continent. L'Union européenne a engagé **plusieurs initiatives pour renforcer la coordination** entre ses champions industriels et scientifiques.

- **Le programme Quantum Flagship,** lancé en 2018 avec un budget de 1 milliard d'euros sur dix ans. Cette initiative soutient des projets collaboratifs intégrant laboratoires publics, startups et grands groupes industriels. Elle structure son action autour de quatre piliers : le calcul quantique, la communication quantique, la détection quantique et la simulation.
- **Le réseau QuantERA** joue un rôle clé dans la coordination des financements nationaux à l'échelle européenne. Ce programme transnational permet à des agences de recherche de mutualiser leurs ressources pour financer des projets de R&D appliquée en consortium.
- **Le programme EIC Accelerator** soutient les startups deeptech. Assuré par le Conseil européen de l'innovation (EIC), il combine subventions et financement en equity pour accompagner des entreprises stratégiques dans leur passage à l'échelle.

La France, en bonne place dans la compétition quantique internationale

La France a su se donner une position stratégique dans la compétition internationale liée aux technologies quantiques. **La France maîtrise quatre des six technologies quantiques les plus prometteuses** (atomes neutres, photons intriqués, supraconducteurs, systèmes spin/silicium). La nation a dégagé un budget de 1,8 milliard d'euros pour le développement des technologies quantiques sur le territoire. Cependant, la France reste peu présente sur les segments logiciels et intergiciels, dominés par des acteurs nord-américains et israéliens.

Déclaration de M. Emmanuel Macron, Président de la République, sur la stratégie nationale concernant les technologies quantiques, à Saclay le 21 janvier 2021.

« ... La stratégie quantique a une importance capitale. En effet, 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 clefs du futur que la France doit absolument avoir en main.
... Cette stratégie repose sur deux piliers principaux. Le premier, c'est 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. »

INTERVIEW

Neil Abroug
Head of Quantum
INRIA

« Compétition quantique : une position stratégique à consolider pour la France »

Avant de rejoindre l'INRIA, M. Abroug a notamment occupé la fonction de Directeur de la Stratégie Quantique Nationale Française.

Quelle est la position de la France dans la compétition quantique internationale ?

Avec près d'un milliard d'euros d'investissements publics consacrés au quantique (auxquels s'ajoutent 800 millions issus du privé), **la France figure dans le peloton de tête mondial. Rapporté au PIB, elle se positionne même au premier rang des pays investisseurs**. Cette dynamique a été initiée très tôt : dès 2018, une mission parlementaire a jeté les bases de la stratégie nationale, officialisée par le président en 2021.

La France fait partie des rares nations disposant de tous les éléments technologiques nécessaires à la construction d'un ordinateur quantique – cryogénie, photonique, microélectronique, industrie nucléaire. Aujourd'hui, elle est, avec les États-Unis, le seul pays à maîtriser l'ensemble des verticales technologiques de calcul quantique.

Sur le plan européen, elle se classe première en matière de levées de fonds privées, avec plus de 500 millions d'euros, juste derrière les États-Unis au niveau mondial. Les premiers résultats sont là. Toutefois, il ne faut pas relâcher l'effort. Les applications les plus avancées ne verront le jour qu'à l'horizon 2030. **Le risque principal est celui du relâchement stratégique** en cours de route, dans un moment où la science progresse mais où les promesses industrielles peinent encore à se matérialiser.

Pourquoi les entreprises doivent-elles s'emparer dès maintenant du sujet quantique ?

Aujourd'hui, un consensus émerge chez les industriels : **la vitesse des progrès technologiques est plus rapide que prévu**. Les roadmaps s'accélèrent, et il est dès lors essentiel d'intégrer le quantique dans les réflexions stratégiques. Mais les freins sont réels : le manque de lisibilité sur les cas d'usage, l'incertitude du retour sur investissement et le coût encore élevé de l'expérimentation. Cependant le calcul quantique permet de rendre calculable ce qui était jusque-là incalculable. Les secteurs disposant d'une culture forte de la simulation numérique – comme **l'énergie, la défense ou les matériaux** – sont les plus à même d'amorcer cette transition. C'est ce que font déjà des acteurs comme EDF, Thales ou Total.

À moyen terme, toutes les entreprises devront évaluer les opportunités offertes par ces nouvelles capacités de calcul. Il s'agit d'un enjeu de souveraineté autant que de compétitivité. L'État peut jouer un rôle déterminant, notamment en développant des politiques de co-investissement dans les technologies quantiques. **Il est essentiel de maintenir le cap que la France a engagé**. Toutes les initiatives pour consolider l'intégration des technologies quantiques au sein des industries seront déterminantes.

INTERVIEW

Jean-Michel Torres
Quantum Ambassador
IBM FRANCE

« Il faut anticiper l'intégration du quantique car se préparer prend du temps »

Où en est la maturité des technologies quantiques ?

Nous commençons à entrevoir l'horizon du calcul quantique. Pour prendre une métaphore, nous pourrions dire que nous approchons d'une île qui maintenant se profile à l'horizon. Ses contours deviennent plus précis et révèlent d'autres questions pour l'approche et l'accostage. La recherche avance rapidement. **Les éléments technologiques essentiels, qualité des qubits, correction d'erreurs, capacités de calcul progressent de manière spectaculaire**. Chez IBM, nous avançons selon une feuille de route que nous suivons avec succès. Il y a environ six ans, notre premier QPU permettait de prendre en charge 20 qubits.

Actuellement, nous mettons en œuvre des processeurs que nous appelons Héron autour de 150 qubits et travaillons à en connecter plusieurs dans une machine, pour cela nous mettons en œuvre les technologies permettant de les relier. Ceci nous permet de construire des système à plusieurs milliers de qubits. Ces évolutions technologiques sont vertigineuses. Pour les exploiter, **il faut des compétences rares** : comprendre les principes de mécanique quantique sous-jacents, et une théorie de l'information quantique totalement différente menant à de nouveaux types d'algorithmes, et maîtriser l'environnement de développement correspondant. Pour cela il faut structurer des équipes autour de projets de développement pour les cas d'usages de l'entreprise.

Pourquoi les entreprises doivent-elles s'emparer dès maintenant du sujet quantique ?

Parce que s'y préparer prend du temps. **Il faut former, expérimenter, construire une manière de penser le calcul tout à fait différente**. Pour faciliter cette transition, IBM a lancé de nombreux programmes d'accompagnement avec la mise à disposition de ressources de formation, du temps machine, des ingénieurs pour aider les membres du réseaux de partenaires d'IBM à structurer leurs cas d'usage. **Les premières applications concrètes apparaissent** : la simulation moléculaire pour la chimie, la résolution d'équations différentielles pour l'aéronautique ou l'énergie, ou encore l'optimisation logistique. Ces catégories de problème deviennent très vite trop complexes pour les ordinateurs classiques – placement d'antennes, affectation de portes d'embarquement à l'aéroport – le calcul quantique présente des solutions.

Les entreprises doivent se préparer. Il est essentiel de construire les compétences, pour explorer avec des partenaires et identifier et valider les cas où le saut quantique sera pertinent. **Que ce soit en 2025 ou en 2029, ceux qui auront pris de l'avance seront seuls sur le pont**.

L'intégration des technologies quantiques : défis et perspectives

Les technologies quantiques sont aux portes des entreprises. Les premiers déploiements expérimentaux se multiplient avec succès en France et à l'international depuis plusieurs années. Si des freins technologiques demeurent, les promesses liées au développement du quantique sont cependant considérables.

Technologies quantiques : du laboratoire au terrain

Alors que les nations sont engagées dans une compétition pour le développement des futures technologies quantiques, les entreprises sont, elles, en deuxième ligne. **Les industries les plus avancées opèrent déjà sous la forme de proofs of concept l'intégration des premières briques** quantiques dédiées à leur activité métier. Une dynamique du laboratoire au terrain qui implique un rapprochement avec les acteurs du quantique : startups, industriels de la tech, programmes de recherche.

Déploiement du quantique : des défis de taille

L'intégration du quantique est cependant freinée par une série de défis technologiques.
À l'échelle matérielle, la **stabilité précaire des qubits** et la complexité des environnements cryogéniques limitent la fiabilité des processeurs actuels. Sur le plan logiciel, la **faible maturité des algorithmes** contraint les usages à des approches hybrides mêlant quantique et calcul classique. L'enjeu est également lié aux **environnements IT actuels des entreprises**. Ces architectures intègrent difficilement les outils quantiques.

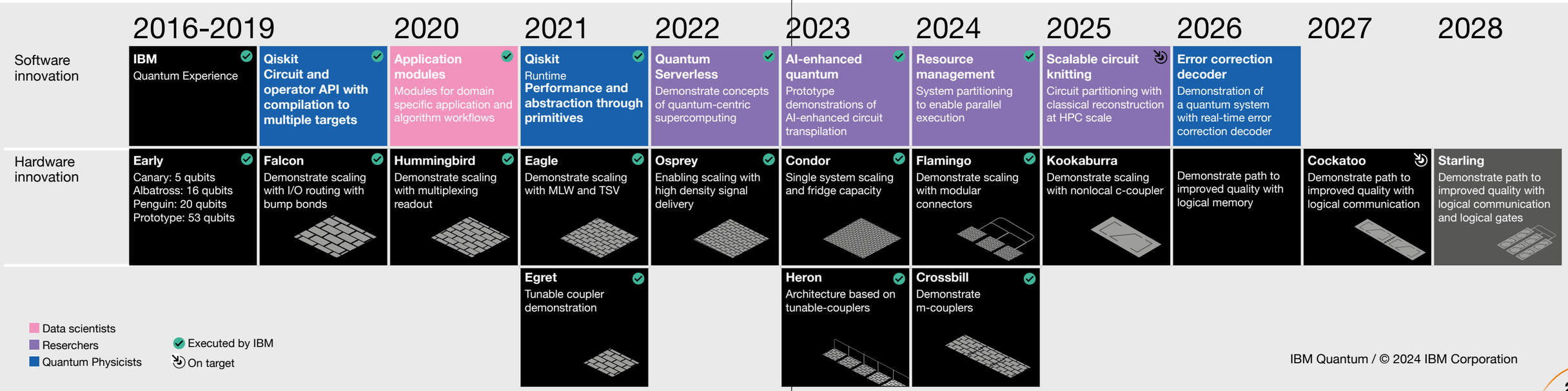
Maturité des technologies quantiques : des disparités sectorielles

L'accélération de la mise en œuvre de projets quantiques est réelle depuis les 5 dernières années. Finance, pharmaceutique, chimie, cybersécurité, logistique ... les applications sectorielles de ces technologies présentent cependant des niveaux de maturité différents.

Agenda R&D et time to market des applicatifs

À l'horizon des 5 prochaines années, les technologies quantiques vont progressivement dépasser le stade expérimental. **La pré industrialisation est en marche** dans plusieurs secteurs clés. L'horizon **2030** s'annonce comme une période charnière pour le passage du quantique exploratoire au quantique appliqué.

Secteur	Application quantique
Finance & Banque	Optimisation de portefeuille, génération de nombres aléatoires
Pharma & Chimie	Simulation moléculaire, modélisation de réactions chimiques
Energie & Materiaux	Découverte de matériaux (batteries, catalyseurs, alliages)
Cybersécurité	Cryptographie post-quantique (QKD), génération de clés quantiques Cryptographie post-quantique (QKD), génération
Télécommunications	Sécurisation de réseaux optiques via QKD
Logistique & Supply Chain	Optimisation des routes, simulation de chaînes de valeur
Défense & Sécurité	Communication sécurisée, traitement de signal quantique
Cloud & Services IT	Accès distant à des processeurs quantiques (Quantum-as-a-Service)



IBM Quantum / © 2024 IBM Corporation

INTERVIEW

Cécile Perrault

Head of Innovation & Partnerships
ALICE & BOB
Vice Presidente
EUROPEAN QUANTUM INDUSTRY CONSORTIUM (QUIC)

> **Nous devons bâtir une souveraineté numérique et industrielle autour du quantique et cela commence maintenant.**

Où en est la maturité des technologies quantiques ?

2030 va marquer un point de bascule majeur avec l'émergence des premiers ordinateurs quantiques capables d'exécuter des algorithmes complets. Toutefois, leurs impacts resteront limités à des usages scientifiques. Les premières retombées commerciales ne sont attendues qu'en 2040 avec des architectures pleinement tolérantes aux fautes. **2030 peut sembler lointain, mais dans une temporalité industrielle, cinq ans, c'est très court**. Chez Alice & Bob, notre feuille de route suit précisément cet horizon. Nous avançons étape par étape sur les verrous techniques. Ce que je souhaite souligner, c'est que les entreprises peuvent dès maintenant s'impliquer dans le quantique pour poser les briques fondamentales à l'utilisation du calcul quantique dans leurs équipes. **Attendre que les technologies soient 100% efficientes, c'est prendre le risque d'être marginalisé ou de travailler dans l'urgence comme beaucoup aujourd'hui avec l'IA**.

Quels sont les atouts de la France et de l'Europe dans cette compétition internationale ?

L'Europe a une carte unique à jouer dans la compétition internationale. **Nous avons, sur notre territoire, tous les composants nécessaires à la construction d'une infrastructure quantique complète** : du hardware très compétitif en **France** et **Finlande** aux briques logicielles en **Allemagne**, aux **Pays Bas**, en **Suède** et au **Danemark**. C'est une configuration rare dans le monde, et historiquement exceptionnelle pour notre continent. Encore faut-il la structurer. C'est là tout l'enjeu pour l'Europe : **dépasser les initiatives nationales**, miser sur des coopérations structurées et **faire émerger une chaîne de valeur intégrée**. Des instruments comme le Quantum Act vont dans ce sens, mais il faut accélérer. La France, pour sa part, est en très bonne position sur le plan scientifique et technologique. Grâce à son expertise en supraconducteurs, photons ou spin-silicium, elle peut être un leader du hardware quantique. Les entreprises doivent désormais s'approprier les usages et envisager une intégration opérationnelle. La construction de la souveraineté numérique et industrielle autour du quantique commence maintenant.

Les prochaines étapes du déploiement quantique d'ici à 2030

Finance & banque	Montée en puissance des modèles hybrides combinant calcul classique et quantique pour l'optimisation de portefeuilles, la simulation de scénarios économiques ou le pricing d'actifs complexes. Les majors du cloud offre des services de calcul quantique on demand conçus pour les applications financières.
Pharmacie & chimie	Le quantique va jouer un rôle catalyseur dans la recherche moléculaire. Les simulations de liaisons et de réactions chimiques complexes sont plus précises, notamment pour des petites et moyennes molécules d'intérêt thérapeutique.
Énergie & matériaux	Des avancées majeures en modélisation moléculaire et en simulation de matériaux à propriétés complexes sont réalisées. Les énergéticiens explorent l'optimisation des réactions catalytiques et le design de nouveaux électrolytes pour batteries. Côté matériaux, les simulations quantiques favorisent la mise au point de composites à haute performance.
Cybersécurité	La distribution quantique de clés (QKD) sort des laboratoires pour équiper des infrastructures critiques dans les secteurs bancaires et institutionnels. Les algorithmes post-quantiques (PQC) sont standardisés et intégrés dans les protocoles de communication (VPN, TLS, 5G).
Télécommunications	Les technologies quantiques ouvrent la voie à des réseaux ultra-sécurisés. La distribution quantique de clés (QKD) est intégrée aux infrastructures optiques, notamment dans les backbones critiques. Les opérateurs explorent des interconnexions entre nœuds quantiques via satellite.
Logistique & supply chain	Les algorithmes quantiques d'optimisation (ordonnancement, planification, allocation de ressources) atteignent un niveau de maturité suffisant et sont intégrés à des chaînes logicielles industrielles. Des modules d'optimisation quantique, compatibles avec les ERP sont proposés via le cloud.
Défense & sécurité	Les communications ultra-sécurisées via QKD sont industrialisées pour des usages stratégiques. Des capteurs quantiques de nouvelle génération, capables de détecter des variations gravimétriques, des anomalies magnétiques ou des mouvements sous-marins, sont intégrés à des plateformes de renseignement.
Services cloud & IT	Le quantique accessible à la demande (Quantum-as-a-Service) se structure autour de plateformes unifiées. Des applications sectorielles verticales, telles que la cryptographie post-quantique, la simulation ou l'optimisation, sont progressivement proposées en standard.

Quantique : la nécessité de franchir le pas

La transition vers le quantique est une démarche qui s'initie dans le temps et qui demande une préparation ad hoc de la part des entreprises. Il est essentiel de définir plusieurs points clés : quels sont les **objectifs métier**, quelles **technologies** quantiques privilégier, quels sont les **enjeux budgétaires**, avec quelles **équipes** et pour quel **agenda** ces projets doivent-ils être mis en place.
Des questions qui doivent être abordées via un accompagnement conseil robuste.

Quatre cas concrets de déploiement de technologies quantiques

Retour sur des applications concrètes déployées sur le terrain par des industries ainsi que des acteurs des technologies quantiques. Ces business cases ont pour objectif de démontrer de quelle manière le quantique se déploie auprès des entreprises.

Cryptographie post-quantique

SK telecom THALES

L'objectif du projet quantique

L'opérateur Coréen SK Telecom sélectionne Thales pour l'accompagner dans un projet visant à **intégrer des mécanismes de cryptographie post-quantique (PQC) dans les réseaux 5G** afin de renforcer la sécurité des communications. Cette initiative répond à la menace potentielle que représentent les ordinateurs quantiques pour les algorithmes cryptographiques actuels, en particulier face aux attaques de type «record now, decrypt later».

Le projet

Thales et SK Telecom déploient des cartes SIM 5G compatibles avec la cryptographie post-quantique, développées par Thales, au sein du réseau autonome 5G de SK Telecom. **Ces cartes SIM utilisent l'algorithme Crystals-Kyber, sélectionné par le National Institute of Standards and Technology (NIST)** pour sa résistance aux attaques quantiques. L'innovation réside dans la capacité à chiffrer et déchiffrer l'identité des abonnés **directement sur le réseau commercial 5G**, assurant ainsi une protection efficace contre les menaces futures. Cette approche permet de sécuriser l'identité numérique des utilisateurs dès le niveau de la carte SIM. **Les tests réalisés ont démontré l'efficacité de cette solution dans un environnement réel**, marquant une avancée significative dans la mise en œuvre de la PQC dans les réseaux mobiles commerciaux.

Les bénéfices du projet

La réussite de ce projet permet à SK Telecom de se positionnant parmi les premiers opérateurs à intégrer ces technologies dans un réseau 5G commercial, l'entreprise renforce ainsi sa proposition de valeur auprès de ses abonnés mais également de ses clients B2B et institutionnels, sensibles aux enjeux de sécurité. Ce choix stratégique favorise également l'accès à de nouveaux segments de marché, en particulier dans les secteurs régulés.

SK Telecom

SK Telecom est le premier opérateur de télécommunications en Corée du Sud. Fortement engagé dans les technologies avancées telles que l'intelligence artificielle et l'Internet des Objets, SK Telecom investit en R&D pour anticiper les défis futurs du numérique. L'entreprise, proactive dans la sécurité des données et la cybersécurité, contribue au développement de nouvelles technologies et à la définition des normes internationales.

Thales

Acteur clé dans les domaines de la défense, de l'aéronautique, de l'espace et de la sécurité numérique, Thales dispose d'un département de recherche et développement dédié aux technologies quantiques. Thales a développé des cartes SIM 5G intégrant des algorithmes de cryptographie post-quantique, tels que le Crystals-Kyber, sélectionné par le National Institute of Standards and Technology (NIST) pour sa résistance aux attaques quantiques. Cette innovation permet de sécuriser l'identité des abonnés directement au niveau de la carte SIM, renforçant ainsi la protection des données personnelles sur les réseaux 5G.

Calcul quantique

CA PASQAL

L'objectif du projet quantique

Le Crédit Agricole CIB souhaite évaluer la capacité de l'informatique quantique à résoudre des problèmes financiers concrets. Pour cela, la banque engage **dès 2021** une collaboration avec la startup française Pasqal. Deux cas d'usage sont rapidement identifiés : l'évaluation des produits dérivés et la prévision des dégradations de notation de crédit. Le projet visait à **comparer les performances des algorithmes quantiques et classiques**, à mesurer les gains en termes de temps de calcul et de mémoire, et à **déterminer la scalabilité** des solutions quantiques en fonction du nombre de qubits utilisés.

Le projet

Le projet se déroule sur une période de 18 mois. Le premier cas d'usage porte sur **l'évaluation de produits dérivés complexes**. Les modèles classiques, bien que robustes, montrent des limites lorsqu'ils doivent traiter de grandes volumétries de données avec précision. L'utilisation d'algorithmes inspirés du quantique a permis d'optimiser les temps d'entraînement des modèles tout en réduisant la consommation de mémoire.
Le second cas d'usage visait à prédire les **dégradations de notation de crédit**. CA-CIB a appliqué un algorithme hybride classique/quantique sur un véritable portefeuille de contreparties. Les résultats, obtenus avec des processeurs quantiques limités à 50 qubits, ont montré une précision comparable à celle des systèmes actuels de production, démontrant ainsi le potentiel des architectures quantiques pour des analyses de risques futures.

Les bénéfices du projet

Les expérimentations ont démontré le potentiel réel de l'informatique quantique pour la finance, malgré le fait que ces technologies en soient encore à leurs débuts. **CA-CIB a profité de cette initiative pour commencer à développer les compétences internes** afin de se préparer à une avancée technologique qui, si elle se produit, aura un impact direct et décisif sur la compétitivité dans le secteur. **Les résultats obtenus indiquent que le point de basculement n'est pas si éloigné, probablement moins de deux ans**, et qu'il est donc urgent pour les utilisateurs d'adopter rapidement ces nouvelles méthodes, comme l'a fait CA-CIB.

Le Crédit Agricole CIB

Crédit Agricole Corporate and Investment Bank (CA-CIB) est la branche de banque d'investissement du groupe Crédit Agricole. Avec plus de 8 900 employés, CA-CIB couvre les marchés de capitaux, la banque d'investissement, le financement structuré, la banque commerciale et le commerce international. Face à des besoins computationnels exigeants, CA-CIB explore des technologies avancées telles que l'informatique quantique pour améliorer son efficacité opérationnelle et maintenir son avantage concurrentiel.

Pasqal

Startup française spécialisée dans le développement d'ordinateurs quantiques basés sur des atomes neutres. Fondée en 2019, Pasqal finalise une levée de fonds de 100M€ en 2023.
Pasqal développe une technologie d'ordinateur quantique basée sur les atomes neutres piégés, refroidis à des températures proches du zéro absolu. Ces atomes sont manipulés par des lasers dans des réseaux optiques pour former des qubits.

Communication quantique

JPMorgan Chase & Co. TOSHIBA

L'objectif du projet quantique

JPMorgan Chase entend tester l'efficacité de la cryptographie post-quantique pour **protéger les données échangées sur des réseaux de communication critiques**. L'entreprise sélectionne Toshiba Europe et Ciena pour l'accompagner dans ce projet. En intégrant la QKD à des VPN haut débit, la banque entend évaluer comment une architecture quantique pourrait être efficace face aux menaces liées aux capacités futures des ordinateurs quantiques.

Les bénéfices du projet

JPMorgan Chase renforce la sécurité de ses communications critiques, tout en **se préparant à un avenir où la cryptographie actuelle pourrait devenir obsolète**. L'intégration de la QKD permet une protection théoriquement inviolable, fondée sur les lois de la physique quantique. En anticipant les normes post-quantiques et en testant l'interopérabilité avec ses systèmes existants, la banque se dote d'un avantage stratégique en matière de cybersécurité, de conformité réglementaire et de continuité d'activité.

Le projet

En 2022, la banque et ses partenaires technologiques établissent **un réseau métropolitain sécurisé** par QKD, **reliant deux centres de données** de JPMorgan Chase à New York. Le système, déployé sur des fibres optiques classiques, a utilisé les dispositifs QKD de Toshiba pour distribuer des clés symétriques à usage unique, inviolables par nature, même face à un attaquant disposant d'un ordinateur quantique. Ces clés ont servi à chiffrer des flux de données transitant via des VPN opérés sur la plateforme Waveserver 5 de Ciena, assurant un débit de 100 Gbps sur une seule fibre. **Les tests ont été réalisés dans un environnement de production simulée, avec des applications bancaires réelles, dont le réseau blockchain Liink développé par JPMorgan**. L'ensemble de l'infrastructure était capable de détecter toute tentative d'interception des photons, invalidant immédiatement la clé en cas d'attaque. **En 2024, une extension du projet a permis d'établir un réseau crypto-agile, combinant QKD et techniques de gestion évolutives de la cryptographie**, renforçant la capacité de la banque à faire évoluer ses algorithmes en fonction des avancées technologiques.

JPMorgan Chase

Acteur mondial de la finance, JPMorgan Chase s'appuie sur des infrastructures technologiques de pointe pour sécuriser ses activités critiques. En expérimentant des solutions de cryptographie post-quantique, JPMorgan anticipe une nouvelle génération de cyberattaques dans un contexte où la menace posée par l'émergence de l'informatique quantique remet en question la robustesse des systèmes cryptographiques traditionnels.

Toshiba et Ciena

Le projet s'est appuyé sur l'expertise combinée de Toshiba Europe pour les technologies de distribution quantique de clés (QKD), et de Ciena, fournisseur de solutions de réseau optique. Toshiba a apporté son système QKD basé sur la manipulation de photons uniques pour la transmission sécurisée de clés cryptographiques. Ciena a intégré cette technologie à sa plateforme optique Waveserver 5 permettant le chiffrement de données à très haut débit sur une fibre unique.

Métrologie quantique

NEWTON-g exail TECHNOLOGIES

L'objectif du projet quantique

Financé par la commission européenne, le projet NEWTON-G vise à démontrer l'efficacité des gravimètres quantiques pour la surveillance volcanologique. En installant un réseau de capteurs sur le mont Etna, Exail entend détecter les variations de masse souterraines liées aux mouvements magmatiques. Cette approche permettrait d'améliorer la compréhension des processus éruptifs et de renforcer les capacités de prévision des éruptions, en offrant une résolution spatio-temporelle sans précédent.

Les bénéfices du projet

L'intégration du gravimètre quantique absolu d'Exail permet à la Commission européenne de bénéficier de mesures gravimétriques précises, stables et continues, essentielles pour la détection précoce des mouvements magmatiques. La robustesse de l'instrument face aux conditions extrêmes du mont Etna renforce la fiabilité des données. Ce dispositif ouvre la voie à une modélisation plus fine des risques volcaniques et à une surveillance renforcée à l'échelle européenne.

Le projet

En août 2020, Exail installe son gravimètre quantique absolu (AQG) sur le mont Etna, à environ 2,5 km des cratères actifs. L'AQG utilise une technologie d'interférométrie atomique avec des atomes de rubidium refroidis par laser pour **mesurer les variations du champ gravitationnel**. Cette méthode permet des mesures absolues et continues de la gravité, avec une sensibilité de l'ordre de 10^{-9} G. Les données collectées ont permis de détecter des changements subtils dans la masse souterraine, associés aux mouvements du magma, offrant ainsi des informations précieuses pour la modélisation des processus volcaniques.
Parallèlement, le projet prévoit l'intégration de capteurs MEMS relatifs, plus compacts et moins coûteux, pour compléter le réseau de surveillance. Ces capteurs, bien que moins précis que l'AQG, permettent une couverture spatiale étendue, chaque capteur agissant comme un «pixel» dans l'imagerie gravitationnelle du volcan. L'ensemble du réseau vise à fournir une cartographie dynamique et en temps réel des variations de densité sous la surface du volcan.

Le projet NEWTON-G

Le projet NEWTON-g (New Tools for Terrain Gravimetry) est une initiative financée par le programme Horizon 2020 de la Commission européenne. Coordonné par l'Istituto Nazionale di Geofisica e Vulcanologia (INGV) en Italie, ce projet vise à développer une nouvelle génération d'instruments de gravimétrie pour la surveillance géophysique. L'objectif principal est de créer un «imager gravitationnel» combinant des gravimètres quantiques absolus et des capteurs MEMS relatifs, permettant une cartographie en temps réel des variations de densité souterraines, notamment sur des volcans actifs comme l'Etna.

Exail

Exail est une entreprise française spécialisée dans les technologies de navigation, de photonique et de capteurs quantiques. Exail développe des instruments de mesure de haute précision, notamment des gravimètres quantiques basés sur l'interférométrie atomique. Ces dispositifs utilisent des atomes de rubidium refroidis par laser pour mesurer les variations du champ gravitationnel avec une sensibilité exceptionnelle.

Agir en faveur de l'innovation quantique

Face à l'essor des technologies quantiques, Orange entend jouer un rôle structurant dans la réponse industrielle française et européenne. Le groupe investit dans la recherche appliquée, la normalisation et le développement de cas d'usage concrets, notamment en cybersécurité et en connectivité.

Une stratégie technologique alignée sur des enjeux de souveraineté

L'approche d'Orange en matière de technologies quantiques est étroitement liée aux enjeux de souveraineté numérique et de résilience des infrastructures critiques. Les travaux de nos équipes R&D s'articulent autour de trois axes structurants :

Les communications quantiques, notamment la distribution de clés quantiques (QKD), destinées à **renforcer la confidentialité des échanges de données** sur les réseaux. Orange est co-pilote du projet ParisRegionQCI, qui vise à déployer une infrastructure de communication quantique régionale, s'appuyant sur un réseau fibré sécurisé.

La cryptographie post-quantique, anticipant l'obsolescence des systèmes de chiffrement asymétrique actuels face aux futurs ordinateurs quantiques. Les équipes d'Orange Cyberdéfense et d'Orange Innovation sont engagées dans la construction de **mécanismes de chiffrement résistants au « quantum breaking »**.

Le calcul quantique et les cas d'usage sectoriels, qui font l'objet d'explorations conjointes avec des partenaires industriels (finance, défense, énergie, santé) via Orange Consulting. L'objectif est d'identifier les problématiques métiers susceptibles de bénéficier à moyen terme d'un avantage quantique (optimisation, simulation moléculaire, classification complexe) et de **construire des feuilles de route** d'adoption réalistes.

Orange contribue aux projets majeurs

Nos équipes de chercheurs ont participé à plusieurs projets collaboratifs au niveau France (Agence Nationale de la Recherche, ANR) ou Union européenne et notamment au projet PROMETHEUS sur la cryptographie post-quantique qui a été récompensé du prix spécial du jury du trophée des étoiles de l'Europe. Par leur expertise scientifique, leurs publications et leurs actions au sein du Groupe Orange, les membres de l'équipe sont concrètement et directement impliqués dans le sujet de la menace quantique et des solutions de remédiation.

Retrouvez les publications scientifiques d'Orange sur : https://crypto.orange-labs.fr/

Une mobilisation transverse du groupe Orange

La spécificité de la démarche d'Orange réside dans sa capacité à **fédérer les expertises de ses entités internes — recherche, cybersécurité, conseil, systèmes d'information — dans une logique de projet transversal structuré**. Des travaux coordonnés sont menés entre **Orange Innovation** (Châtillon, Lannion), **Orange Business**, **Orange Cyberdéfense** et **Orange Consulting**, sous le pilotage de directions techniques et stratégiques dédiées aux sujets quantiques.
Orange met en œuvre une stratégie partenariale ouverte, qui associe acteurs **industriels** (Thales, Nokia), **startups** (Pasqal, Alice & Bob, Quandela), **laboratoires publics** (CNRS, INRIA, CEA) et **institutions européennes** (DG CONNECT, ETSI). Cette logique de co-développement vise à inscrire l'Europe dans la chaîne de valeur mondiale du quantique.

Une vision de long terme, ancrée dans les politiques publiques

Orange contribue activement aux réflexions stratégiques menées dans le cadre du Plan Quantique national français et des initiatives du European Quantum Flagship. Orange défend **une approche industrielle du quantique** : il s'agit de faire émerger des briques technologiques matures, exploitables par les opérateurs d'infrastructures et les grands utilisateurs de services numériques. Ce positionnement est consolidé par des **contributions aux travaux de normalisation** (ETSI, ITU-T) et une stratégie de **dépôt de brevets** orientée sur la cryptographie et les protocoles de communication sécurisés.

ParisRegionQCI : un projet quantique coordonné par Orange

ParisRegionQCI est une infrastructure pilote de communication quantique en Île-de-France, déployée sous la coordination d'Orange. Ce projet fédère industriels, laboratoires et administrations pour tester la distribution quantique de clés dans un réseau fibré sécurisé.

Orange au cœur de la stratégie française pour l'EuroQCI

Le projet Quantum Communication Infrastructure (QCI), également connu sous le nom d'**EuroQCI**, est dévoilé par l'Union européenne en **2019**. Ce projet a pour but de **déployer un réseau de communication quantique sécurisé réunissant les 27 États membres**. Reposant sur des technologies de distribution de clés quantiques (QKD) dans les infrastructures de communication existantes, ce réseau permettra de protéger les données sensibles et les infrastructures critiques des différents pays : institutions gouvernementales, hôpitaux, data centers et les réseaux énergétiques. En France, Orange joue un rôle central en tant que coordinateur dans cette initiative à travers son implication dans le projet FranceQCI. Le projet vise à établir un réseau de communication quantique sécurisé en France, en s'appuyant sur les infrastructures existantes.

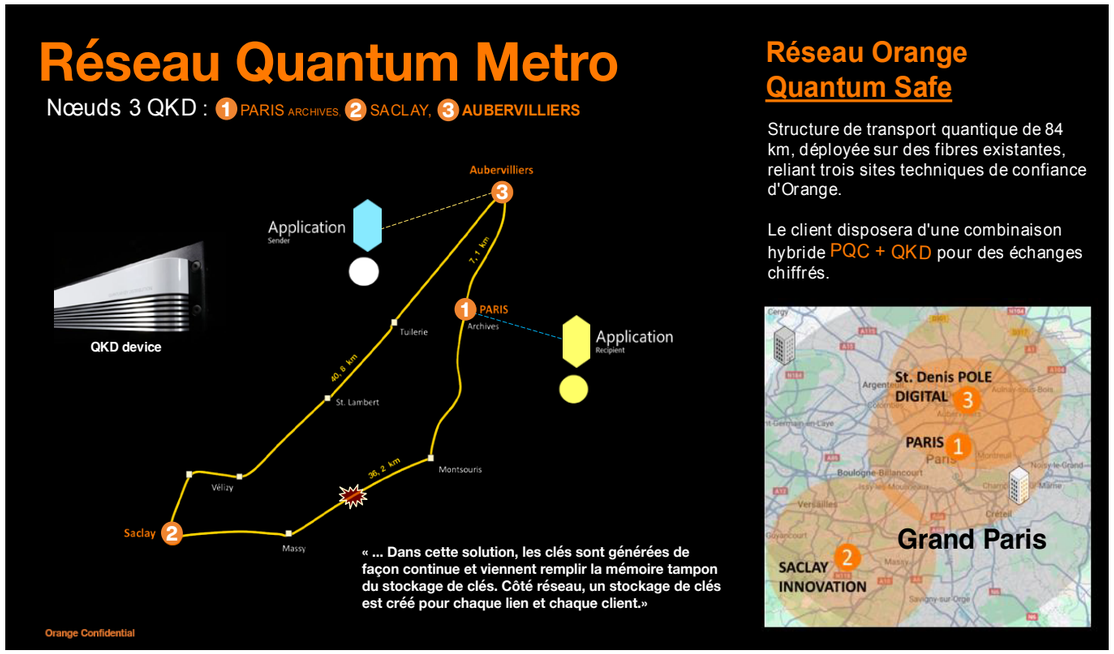
ParisRegionQCI : déployer des clés quantiques sur réseau optique existant

Le projet ParisRegionQCI, inscrit dans FranceQCI, a permis de démontrer la faisabilité de la distribution de clés quantiques (QKD) sur des fibres optiques déjà existantes en Île-de-France. **Déployé entre janvier 2021 et décembre 2023, le projet s'appuie sur un consortium réunissant des industriels (Orange, Thales, Nokia Bell Labs), des start-ups (Quandela, CryptoNext, VeriQloud, Kets Quantum) et des laboratoires académiques (LIP6, Télécom Paris, IOGS)**. Le réseau quantique s'étend sur environ 80 km, reliant neuf nœuds dont les sites de Sorbonne Université (LIP6), Orange Gardens à Châtillon, Thales à Palaiseau et le plateau de Saclay. Il repose sur un backbone optique utilisant des fibres existantes et adaptées aux exigences de la communication quantique. Les tests réalisés ont validé l'efficacité des systèmes DV-QKD et CV-QKD, notamment pour le chiffrement d'un flux vidéo 4K via des chiffreurs Mistral de Thales, **une première en France sur réseau optique commercial**. Ce système a permis d'établir un lien sécurisé avec une atténuation maîtrisée sur 43 km entre Télécom Paris et Orange Gardens, et sur 14 km entre Orange et Jussieu.

Vers des applications industrielles critiques et sécurisées

Le projet ParisRegionQCI ouvre la voie à des usages industriels variés, en particulier dans des secteurs où la confidentialité et la robustesse des communications sont critiques. Plusieurs cas d'usage ont été explorés, notamment dans le cadre des démonstrations réalisées : transmission de flux vidéo sécurisé, intégration dans les processus de chiffrement de données sensibles et mise en œuvre d'algorithmes post-quantiques (PQC).

À terme, les technologies testées dans ParisRegionQCI pourraient être utilisées pour sécuriser les communications des hôpitaux, des centres de données critiques, ou encore des infrastructures énergétiques. Le projet représente aussi **une brique technologique stratégique** pour le développement d'offres de cybersécurité avancées dans les services publics et les industries sensibles (défense, finance, télécommunications).
Cette perspective industrielle s'inscrit également dans un **contexte plus large de souveraineté numérique**, avec une volonté forte d'ancrer ces infrastructures sur des technologies européennes et de renforcer la résilience des réseaux face à la menace post-quantique.



Réseau Quantum Safe Orange

Structure de transport quantique de 84 km, déployée sur des fibres existantes, reliant trois sites techniques Orange de confiance. Le client disposera d'une combinaison hybride de PQC + QKD pour des échanges cryptés.

INTERVIEW

Emmanuel Cartron
Head of Anticipation & Transformation Practice
ORANGE BUSINESS

L'offre Quantum Safe Infrastructure d'Orange ouvre la voie à une cybersécurité inviolable

Face à l'émergence de la menace post-quantique, Orange Business lance **Quantum Secure Network, une offre de cybersécurité fondée sur les principes inviolables de la physique quantique**. Emmanuel Cartron, Responsable Anticipation & Transformation, détaille les enjeux, les cas d'usage et la feuille de route de cette innovation stratégique.

Pouvez-vous nous présenter l'offre Quantum Safe Infrastructure ?

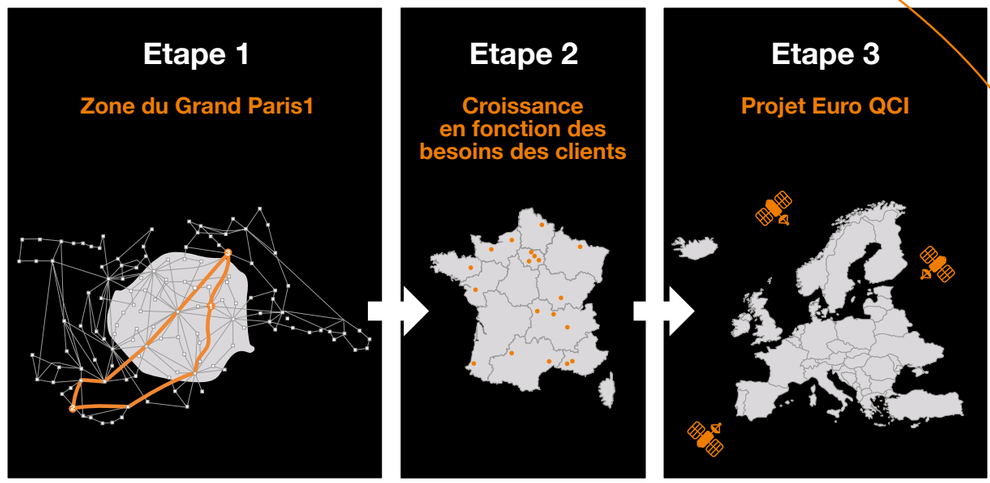
Notre ambition avec Quantum Safe Infrastructure est de repenser en profondeur la notion de sécurité numérique. Elle s'appuie sur trois piliers : **1) un usage hybride de solutions quantiques (QKD + PQC) pour générer des clés de chiffrement, 2) une infrastructure totalement sécurisée à l'état de l'art pour garantir le bon fonctionnement et l'intégration avec l'IT des clients, l'évolutivité et la pérennité, et enfin 3) des équipements quantiques reposant sur l'expertise et l'expérience de notre partenaire stratégique Toshiba.** Cette triple couche rend notre chiffrement inviolable à ce jour (tant que les fondements quantiques démontrés et prouvés ne sont pas invalidés).

Quels types de données sont concernées ?

Nous ciblons toutes les **données dites longue durée**, c'est-à-dire sensibles pour une période de 5 à 10 ans, voire au-delà. A titre d'exemple, cela inclut des informations stratégiques industrielles, des données de défense, des plans d'infrastructure critiques ou des échanges bancaires majeurs. L'objectif est d'assurer que ces informations, même interceptées aujourd'hui, restent indéchiffrables demain, lorsque les ordinateurs quantiques atteindront une puissance suffisante.

Quels sont les secteurs les plus concernés ?

Les banques sont historiquement les premières concernées, mais notre solution s'adresse également à l'industrie, la chimie, la défense, le retail stratégique et même les télécoms eux-mêmes. **Toutes les structures manipulant des données à haute valeur et à long terme sont exposées à la menace post-quantique** et donc concernées par notre solution.



Quelles étapes une entreprise doit-elle suivre pour migrer vers cette solution ?

La première phase consiste à **évaluer son exposition** à la menace quantique. Orange Cyberdéfense propose des audits de cartographie des algorithmes cryptographiques utilisés et de leur vulnérabilité. Ensuite, nous accompagnons nos clients dans la **définition d'un plan de mitigation**, puis dans la **mise en place progressive de l'infrastructure** quantique. Il est essentiel d'identifier les données sensibles, de prioriser les flux à sécuriser, et d'installer les équipements nécessaires, notamment les modules Toshiba dans les datacenters.

Quel est le calendrier type pour une telle migration ?

Il faut compter entre 12 et 24 mois pour une transition complète, incluant l'audit, la montée en compétence des équipes, et le déploiement technique. Les premiers tests peuvent être réalisés dès les premiers mois, sur un périmètre restreint.

Quelle est l'ambition à long terme pour Quantum Secure Network ?

Nous réfléchissons déjà à l'extension géographique de la couverture au-delà de la région parisienne. Aujourd'hui notre offre couvre une zone de 80km depuis Paris. **D'ici 6 mois, nous devrions couvrir plus de 300km et couvrir l'ensemble du territoire en 2026**.

Un mot sur les équipes qui rendent cela possible ?

Ce projet est le fruit du travail conjoint de nos équipes **Orange Innovation, Orange Cyberdéfense et Orange Business**. Nous disposons d'une division R&D dédiée, composée d'ingénieurs en cryptographie, d'architectes réseau et de spécialistes de la physique quantique. C'est cette combinaison d'expertises et la culture de l'anticipation qui nous permettent d'être à l'avant-garde de la cybersécurité quantique.

Orange Consulting :
des experts pour vous accompagner dans votre transition quantique

Orange Consulting se positionne comme un partenaire pour accompagner les entreprises dans leur transformation. Nos équipes proposent une approche structurée et pragmatique pour aider les entreprises à anticiper et à intégrer les innovations quantiques.

Une approche sur mesure pour chaque secteur

Orange Consulting collabore étroitement avec les entreprises pour identifier les cas d'usage pertinents des technologies quantiques dans leur domaine d'activité. Que ce soit dans la finance, la santé, l'énergie ou la défense, les consultants d'Orange analysent les besoins spécifiques de chaque secteur pour proposer des solutions adaptées ou accompagner de premières expérimentations. Cette démarche permet de **construire des feuilles de route technologiques réalistes, alignées sur les objectifs stratégiques** de ses clients.

Des compétences pluridisciplinaires au service de l'innovation

Les équipes d'Orange Consulting s'appuient sur une synergie entre experts en cybersécurité, chercheurs en R&D et spécialistes des systèmes d'information pour offrir une vision globale des enjeux liés aux technologies quantiques. Cette collaboration permet de **couvrir l'ensemble des aspects techniques, organisationnels et réglementaires**, garantissant ainsi une intégration harmonieuse des solutions quantiques au sein des infrastructures existantes.

INTERVIEW

Guillaume Grard
Directeur Général
ORANGE CONSULTING

> **Les entreprises françaises doivent être quantum ready.**

Les technologies quantiques doivent être priorisées par les entreprises françaises. L'investissement massif des principaux acteurs internationaux de l'univers des technologies donne le ton. D'ici à 5 ans, le quantique jouera une place déterminante dans les programmes d'innovation des principales entreprises mondiales. D'ici à 10 ans, ces technologies joueront un rôle clé. Les industries qui n'auront pas su engager ce tournant risquent d'être moins compétitives que leurs concurrents. La cybersécurité est également au cœur de ces enjeux. Il est primordial que les industries actent que les nouvelles générations de menaces informatiques seront portées par des technologies quantiques. Dans ce contexte, **alors que les secteurs industriels les plus matures ont déjà engagé leur conversion vers le quantique, il revient désormais à l'ensemble des entreprises françaises de franchir ce cap décisif**.

Sous l'impulsion de différents programmes européens, et suivant une politique nationale offensive, **la France se situe dans une position favorable** pour engager cette bataille technologique. Nos startups innovent, elles développent sur le terrain des premiers projets pour des entreprises. L'État réagit et engage des investissements conséquents et fédère les acteurs de la filière quantique dans des programmes structurants.

Orange est au cœur de ces enjeux. Notre groupe figure en très bonne place dans le développement et l'intégration de technologies quantiques au niveau mondial. Nos chercheurs et nos experts accompagnent déjà des entreprises et construisent avec ces dernières les cadres de leur transformation quantique. Orange Consulting fut il y a quelques années cloud ready et sut accompagner les entreprises dans cette révolution technologique. Nous sommes aujourd'hui **quantum ready** et offrons à nos clients les conditions pour leur permettre de faire de ces technologies un levier de croissance et de compétitivité.

Crédits

Nous tenons à remercier tous les contributeurs de ce livre blanc.

Remerciements particuliers à :
Neil Abroug (INRIA) **Frédéric Barbaresco** (Thalès), **Cécile Perrault** (Alice et Bob), **Jean-Michel Torrès** (IBM), **Emmanuel Cartron** (Orange Business), **Guillaume Grard** (Orange Consulting).

Réalisation : **Robin Ferriere**, Orange Consulting. Avec les contributions d'**Axel Miomandre**, **Yolande Garcia** et **Camila Benedetti**

Rédaction : **Paul Gillet**, Leibniz Agency
Conception graphique : **Anne Morineau**

Pour aller plus loin...

Être accompagné dans l'élaboration de votre approche par Orange Consulting ?

En savoir plus sur les offres d'Orange Cyberdéfense (PQC, QKD) ?

Accéder aux publications s la Recherche d'Orange en r Cryptographie ?