arcep les réseaux comme bien commun

« Les technologies du quantique et leur impact sur les réseaux »

11 juin 2026

Réseaux du futur

Sommaire

01

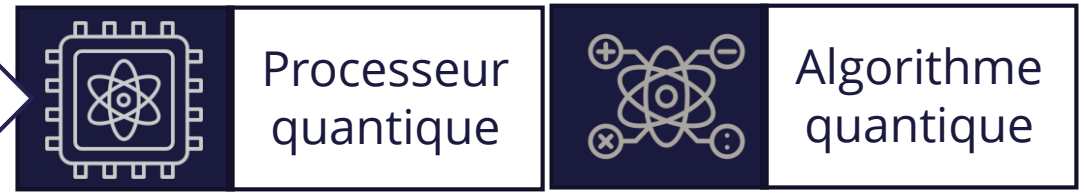
L’ordinateur quantique :
ses principes, ses promesses et les besoins du secteur télécom

Les principes et promesses de l'ordinateur quantique

Les principes de l'ordinateur quantique

Les principes quantiques utilisés :

- Superposition
- Intrication



Les promesses de l'ordinateur quantique…

Dépasser les limites de l'informatique classique

- Augmentation exponentielle de la puissance de calcul

- Capacité à réaliser des calculs en parallèle

L'avantage quantique : la capacité réelle des ordinateurs quantiques à réaliser des calculs utiles

- Actuellement, les ordinateurs quantiques sont imparfaits (bruités et avec un taux d'erreur important) et de taille intermédiaire (en nombre de qubits) (NISQ pour « *Noisy Intermediate-Scale Quantum* »)

- Etape intermédiaire : cadre expérimental permettant d'explorer de nouveaux algorithmes, architectures et techniques de contrôle

…face aux défis pour parvenir à un ordinateur tolérant aux fautes

Les défis techniques à relever :

- La **correction d'erreur** quelle que soit la technologie (instabilité et décohérence des qubits)

- Le **passage à l'échelle** : manipuler et contrôler un grand nombre de systèmes quantiques intriqués avec une précision et une fiabilité suffisantes

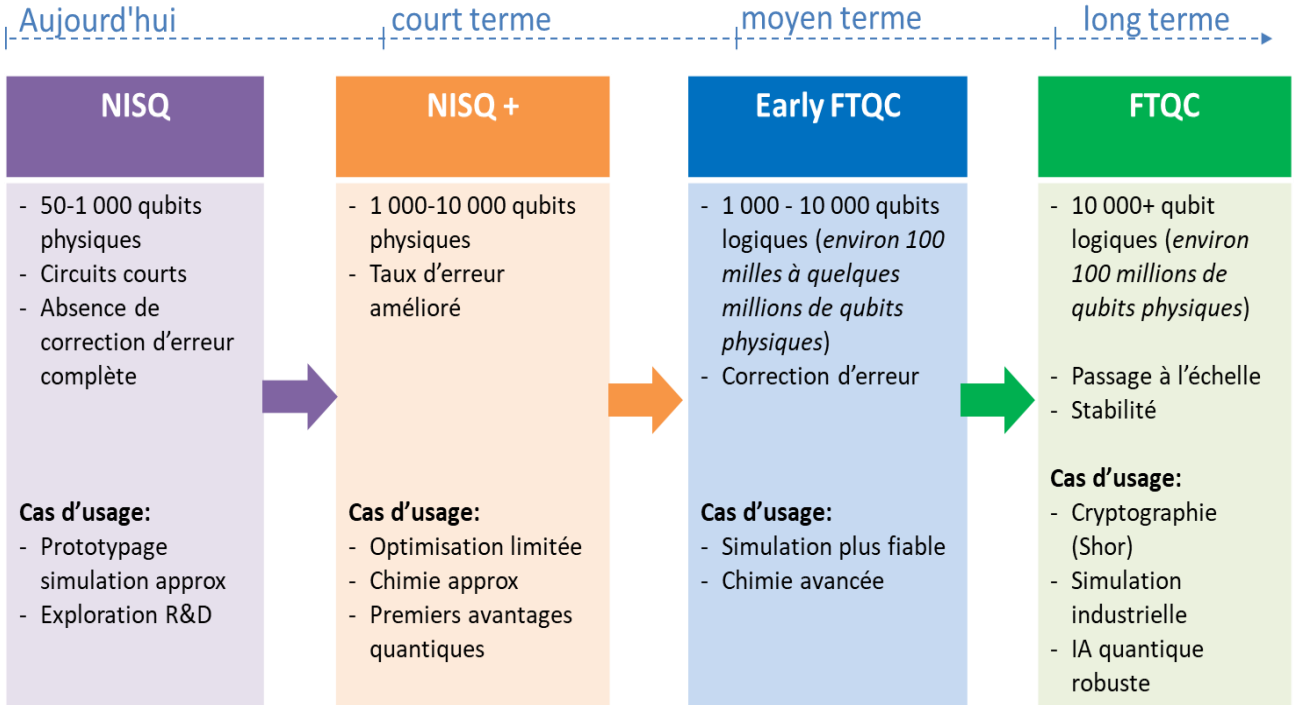
- Les **enjeux économiques** : incertitudes ordinateur FTQC et coûts de développement et de fabrication très élevés

Feuille de route globale

Deux ambitions : augmentation du nombre de qubit et amélioration de la tolérance aux fautes grâce à la correction d'erreurs quantiques

10 000 qubits logiques nécessaires pour que les algorithmes dédiés aux calculateurs FTQC puissent résoudre les problèmes de portée industrielle

Un convergence se dessine pour situer l'émergence du FTQC à l'horizon **2030** et d'un passage à l'échelle vers **2035**



Source : J. Preskill, «Quantum Computing in the NISQ era and beyond,» vol. 2, 2018

L’informatique quantique en nuage et besoins pour les télécoms

Premiers ordinateurs quantiques dans des grands centres de calcul

- Investissements coûteux et risqués

- Besoin de stabilité et d’un haut niveau d’isolation pour être performants

- Connectivité en nuage

- Fourniture de la puissance de traitement quantique pour le développement d’algorithmes, de premières simulations, de calculs et de modélisations complexes par les plateformes de calcul *cloud*

- Premières offres permettant de tester le calcul quantique sur des émulateurs et des ordinateurs NISQ

Ordinateurs et calculs quantiques pour les télécoms

- Optimisation des déploiements et de la gestion des réseaux de plus en plus complexes : routage des flux de données, positionnement des antennes et déploiement du réseau fibre

- L’allocation des ressources radio : optimisation de l’usage du spectre

- Traitement du signal : conception du matériel et des logiciels pour améliorer les performances => optimisation de la couverture et la qualité de service mobile

- Télécoms : Pas une priorité immédiate de la recherche algorithmique de l’informatique quantique => attente des ordinateurs FTQC

02

L’ordinateur quantique et la sécurité des réseaux

L’ordinateur quantique : menace pour la sécurité des communications

L’ordinateur quantique pourrait casser les systèmes de cryptographie classiques tels que RSA, et, par conséquent, la confidentialité des communications et des informations stockées avec l’algorithme de Shor ou de Grover mais l’horizon de la menace est difficile à estimer

Les menaces sur les réseaux télécoms

- Intercepter aujourd’hui pour déchiffrer demain (« *store now, decrypt later* »)
- Fragilisation des mécanismes d’établissement de la confiance
- Menaces hybrides et risque de transition dans des environnements complexes

Solutions face aux menaces quantiques

- Cryptographie post-quantique (PQC) : les algorithmes se basant sur des problèmes mathématiques pour lesquels aucun algorithme quantique efficace n'est connu à ce jour
- Distribution quantique de clés (QKD) : Etablissement d’une clé symétrique entre deux parties en exploitant des propriétés physiques de la mécanique quantique
-Solutions hybrides : combiner plusieurs mécanismes de sécurité reposant sur des mécanismes différents

03

Les défis pour l’internet quantique

Un réseau complémentaire de l'internet classique

Des cas usages très spécifiques: applications de niche à forte valeur ajoutée dans des domaines comme la recherche scientifique, la défense, la cybersécurité ou la finance

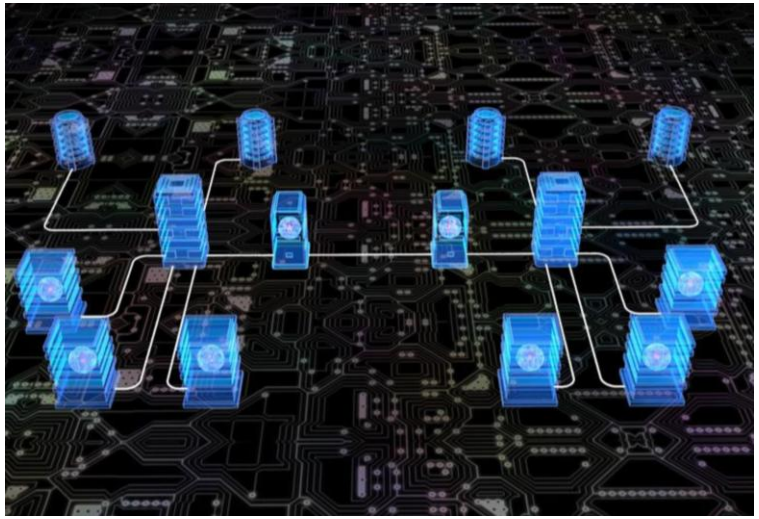
- Renforcement de la sécurité des communications : mise en place les systèmes de cryptographie quantique comme la distribution de clés quantiques (QKD) sur réseaux fibres optiques et satellitaires

- Multiplication de la puissance de calcul : Déploiement de nœuds de calcul quantique interconnectés via un réseau => système de calcul distribué beaucoup plus puissant qu'un seul ordinateur. Partage des états quantiques entre des nœuds distants, essentiel pour coordonner des calculs complexes répartis favorisant l'émergence du calcul quantique distribué.

- Transmission d'informations issues de capteurs quantiques avancés : acheminement sans dégradation de mesures ultra précises générées par les capteurs quantiques

Les défis de l'internet quantique

La construction de réseaux quantiques, encore en stade embryonnaire, s'avère compliquée face à des limitations techniques principalement liés à la difficulté de la mesure quantique ou la fragilité particulière de l'intrication



Source : Quantum Internet Alliance

La transmission à longue distance

- **Propriétés physiques de l'information quantique** extrêmement sensibles aux perturbations et dégradation rapide lors de la propagation notamment dans les fibres optiques

- Perte progressive de cohérence, rendant difficile la **distribution fiable d'états quantiques** sur de grandes distances sans dispositifs spécifiques

-**Solutions potentielles** :

- **répéteurs quantiques** en cours de développement mais besoin d'intégration de mémoires quantiques fiables
- intégration de **communications quantiques s'appuyant sur des satellites**, qui profitent d'atténuations beaucoup plus faibles dans l'espace libre

Autres défis à relever

- **Coût et efficacité des ressources** : développement de composants économiquement viables tout en maintenant des performances élevées
- **Interopérabilité** : assurer la compatibilité entre différentes technologies quantiques et entre les réseaux quantiques et les réseaux classiques
- **Utilisation des réseaux de fibres optiques existants en co-canal pour la QKD** : problématiques liés à la scalabilité

04

Les stratégies quantiques des Etats

Les stratégies quantiques nationales et européennes

55,7 milliards $ les fonds engagés dans la science et la technologie quantiques par les gouvernements du monde entier depuis 2013

Le marché mondial des technologies quantiques devrait atteindre 106 milliards d'ici 2040 selon un rapport de McKinsey de 2023.

Des freins à la coopération et collaboration internationale de plus en plus importants

Tensions géopolitiques actuelles, accent mis sur la sécurité nationale et l'autonomie stratégique notamment vis-à-vis des applications à double usage, restrictions en matière de transfert de technologies

Axes de stratégies nationales différents selon les pays

La Chine semble plus se focaliser sur le domaine des communications quantiques, testant et déployant des réseaux de communication à distribution de clés quantiques (QKD). Les Etats-Unis apparaissent comme l'un des principaux financeurs des travaux dans le domaine de l'informatique quantique (soutien aux grands acteurs comme IBM et aux start-up). L'Europe souhaite être un leader mondial du secteur quantique d'ici à 2030 en se basant sur l'excellence reconnue dans la recherche scientifique et un écosystème dynamique de start-up (ex. projet euroQCI, stratégie « *Quantum Europe* » et le futur Quantum Act).

05

Les enjeux réglementaires et de régulation

Défis majeurs de régulation en termes de souveraineté, sécurité et d'accès

Sécurité

Enjeux sur les standards de cryptographie appelés à être imposés ou recommandés : critères de sélection des solutions, calendrier d'adoption, modalités de leur déploiement, risques de divergence entre les standards. Les plus anciennes générations de technologie mobile pourraient devenir progressivement moins conformes à des exigences de cybersécurité renforcées.

Les enjeux liés à l'informatique quantique en nuage

L'accès à la puissance de calcul quantique via des services d'informatique en nuage pourrait soulever des enjeux réglementaires importants, notamment en matière de souveraineté, de concurrence et de gouvernance des technologies stratégiques. Il existe un risque d'une concentration du marché au profit d'un nombre restreint d'acteurs dominants, susceptible d'engendrer une dépendance stratégique et d'accentuer les inégalités d'accès à ces infrastructures avancées. Nécessité d'adapter le cadre réglementaire aux services quantiques, afin notamment de permettre un accès équitable et une concurrence effective entre services d'informatique quantique ?

Conclusion

Trop **tôt** pour prédire avec certitude l'ampleur exacte des transformations qu'apporteront les technologies quantiques au secteur télécom.

Uniquement renforcer et sécuriser les **infrastructures existantes ou ouverture vers de nouvelles architectures** de communication à mesure que les systèmes et algorithmes se développent ?

La route vers les réseaux quantiques reste **jalonnée d'étapes expérimentales et de défis technologiques** qui définiront le rythme et la nature de cette révolution.

Le développement de **standards et la définition d'une stratégie nationale et européenne** cohérentes joueront un rôle clé pour orienter ces évolutions.

Fin de la présentation

Cette réflexion se veut « vivante ». L'Arcep invite tous ceux qui le souhaitent à s'approprier ces analyses et à lui envoyer des contributions sur :

Reseaux-du-futur@arcep.fr

Retrouvez en ligne toutes les informations sur la démarche « Réseaux du futur » et les notes précédentes sur le site de l'Arcep :

https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/larcep-et-les-reseaux-du-futur.html

Merci de votre attention