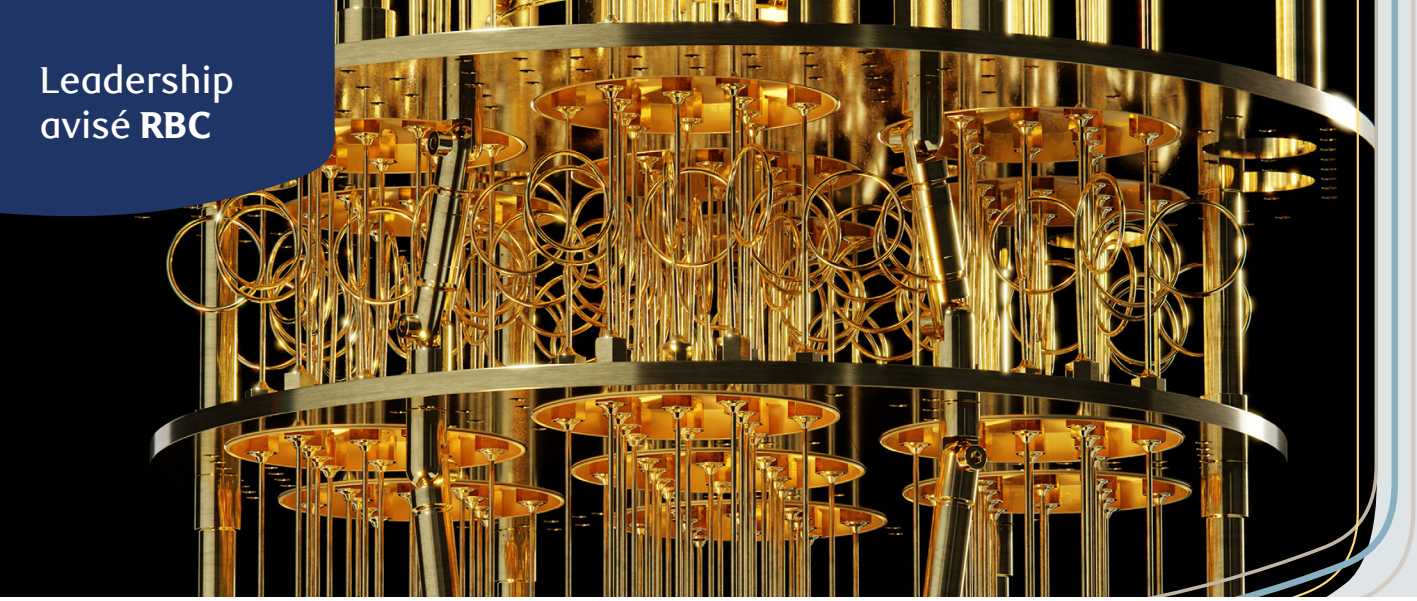

Expliqué

Démystification de l'informatique quantique

Ce qu'il faut savoir sur ce domaine en pleine expansion, capable de résoudre les problèmes plus rapidement qu'un super-ordinateur

L'informatique quantique est en train de passer d'un défi de physique intéressant à une solution stratégique potentielle pour les entreprises du monde entier. Le marché mondial de la technologie quantique devrait atteindre 97 milliards de dollars américains d'ici 2035. Le Canada, qui dispose d'une importante base de recherche et d'un petit nombre d'entreprises qui cherchent à transformer cet avantage scientifique en capacité industrielle, est bien placé pour tirer parti de cette évolution.

Qu'est-ce que l'informatique quantique ?

Les ordinateurs quantiques ne remplacent pas les machines classiques. Ce sont des outils spécialisés pour résoudre des problèmes que même les meilleurs super-ordinateurs actuels ne sont pas en mesure de traiter. En 2024, la puce Willow de Google a effectué en moins de cinq minutes un calcul de référence qui prendrait environ 10 septillions d'années à un super-ordinateur de pointe – bien au-delà de l'âge de l'univers.

Un ordinateur classique teste les possibilités une par une, au moyen de bits binaires (0 ou 1). Un ordinateur quantique, lui, utilise des qubits (ou bits quantiques), qui maintiennent simultanément de nombreuses possibilités **(superposition)**. Il relie les différentes parties du problème afin qu'elles évoluent ensemble **(intrication ou enchevêtrement)** et exploite des phénomènes d'annulation et de renforcement pour faire disparaître les mauvaises réponses et faire ressortir les bonnes **(interférence)**.

Pourquoi faut-il dès à présent s'intéresser à l'informatique quantique ?

Elle peut résoudre des problèmes qu'aucun ordinateur classique ne peut traiter. Selon Bain & Company, l'informatique quantique pourrait générer jusqu'à 250 milliards de dollars de valeur dans les secteurs de la pharmaceutique, de la finance, de la logistique et de la science des matériaux. Prenons l'exemple de la découverte de médicaments : la mise en marché d'un médicament peut coûter jusqu'à 4 milliards de dollars et prendre plus d'une décennie, sans compter qu'environ 90 % des essais de médicaments échouent. Les ordinateurs quantiques peuvent simuler les interactions moléculaires au niveau atomique – ce que les machines classiques ne peuvent qu'approximer – réduisant fortement les délais.

Le compte à rebours en matière de sécurité a déjà commencé. Le risque le plus immédiat pour les entreprises est celui d'obtenir l'information chiffrée nécessaire et de la déchiffrer plus tard : les concurrents recueillent des données chiffrées aujourd'hui, mais attendent de disposer des capacités quantiques pour les déchiffrer rétroactivement. Pour le National Institute of Standards and Technology (NIST), la National Security Agency (NSA) et le Centre canadien pour la cybersécurité, il s'agit-là d'une menace réelle qui nécessite des mesures. Si votre entreprise détient des données à longue durée de vie (dossiers médicaux, recherche exclusive, propriété intellectuelle industrielle), la fenêtre de vulnérabilité est déjà ouverte.

Où se situe le Canada ?

La puissance quantique canadienne se construit depuis des décennies. En 25 ans, la « Vallée quantique » de Waterloo, vaste écosystème composé notamment de l'Institut Périmètre et de l'Institut d'informatique quantique, a attiré plus de 1,5 milliard de dollars d'investissements et a formé plus de 3 500 spécialistes en physique quantique.

Le défi est de conserver cet avantage au pays. En décembre 2025, Ottawa a lancé le **Programme des champions quantiques canadiens**, qui investit 92 millions de dollars dans quatre sociétés : **Xanadu** (Toronto), **Nord Quantique** (Sherbrooke), **Photonic** (Vancouver) et **Anyon Systèmes** (Montréal). Ce programme s'inscrit dans le cadre de l'engagement de 334,3 millions de dollars sur cinq ans du gouvernement en faveur du secteur quantique.

Les résultats prévus : selon une estimation, le secteur pourrait contribuer de plus de 3 % au PIB du Canada d'ici 2045, rivalisant avec l'aérospatiale, et soutenir plus de 200 000 emplois.

Le principal obstacle : la fragilité des qubits

Un qubit conserve son état quantique durant une période infime, généralement environ 100 microsecondes pour le matériel de pointe actuel, ce qui suffit pour effectuer une centaine d'opérations avant que l'information ne disparaisse. C'est comme résoudre une équation complexe sur un tableau blanc qui s'efface chaque fraction de seconde.

Pour compenser, les ingénieurs utilisent la **correction d'erreur** : des qubits redondants qui vérifient et protègent le calcul. Mais la création d'un seul « qubit logique » stable peut nécessiter des milliers de qubits physiques, bien plus que ce que n'offrent les machines actuelles. C'est là que tout se joue : Google, Microsoft et Xanadu, au Canada, rivalisent pour résoudre le défi de la correction d'erreur à grande échelle et faire des percées dans la simulation moléculaire, la cryptographie et l'optimisation que les ordinateurs classiques ne peuvent pas atteindre.

Points à surveiller :

- **Échéances de la cryptographie post-quantique :** la feuille de route du Canada pour les services publics requiert des plans de migration d'ici avril 2026, des systèmes hautement prioritaires à résistance quantique d'ici 2031 et une migration complète d'ici 2035. Ces dates auront des répercussions sur les contrats avec les fournisseurs et les chaînes logistiques.
- **Attrait commercial prometteur :** les projets pilotes voient le jour dans les domaines de la découverte de médicaments, de la science des matériaux et de l'optimisation financière. Si cette technologie s'avère systématiquement plus avantageuse que les méthodes traditionnelles, elle aura franchi un cap décisif.

Rédigé par Sabreena Shukul, adjointe à la recherche, Leadership avisé RBC