Un balado de KPMG sur la cybersécurité

Série 2

Épisode 1 : Informatique quantique

Alexander Rau (KPMG)

Ce n'est pas uniquement une question de rapidité. Il s'agit aussi de la capacité des ordinateurs quantiques à résoudre des problèmes que nous ne pouvons pas résoudre, que nous ne pouvons même pas demander aux ordinateurs traditionnels de résoudre.

Pavan Chander (KPMG)

Quand devriez-vous commencer à vous préparer à l'informatique quantique? Je pense que c'est maintenant : nous en sommes au point où les experts de l'industrie reconnaissent que les avantages et les risques de cette technologie sont réels et presque à nos portes. Il est donc nécessaire de comprendre comment et où l'informatique quantique affectera nos entreprises.

Sean Wagner (IBM)

Je crois que les craintes de nombreux consommateurs porteront sur la capacité d'un futur ordinateur quantique à potentiellement percer le chiffrement des données. Tout le monde a ses renseignements personnels stockés sur son téléphone, sur son ordinateur portatif ou dans le nuage. Les consommateurs voudront savoir si ces renseignements demeureront protégés ou non.

Narratrice

Nous traçons le parcours de l'humanité à travers le progrès comme un chemin linéaire. Davantage de résultats avec moins d'intrants, des découvertes qui en engendrent d'autres, et une exploration scientifique [de l'univers] qui nous a mené des idées de Galilée à la percée des secrets de galaxies lointaines. Et depuis le siècle dernier, les ordinateurs ont été nos fidèles compagnons dans cette quête constante de connaissance – évoluant, traitant des données et performant à un rythme aussi impressionnant que mesurable.

Mais aujourd'hui, nous sommes au bord d'un changement de paradigme, un moment de l'histoire où le tissu même du progrès computationnel est en train d'être réinventé, créant une nouvelle réalité et de nouvelles possibilités qui ont le pouvoir de changer, voire de perturber, l'expérience humaine. La question est de savoir si nous y sommes prêts.

Introduction

Narratrice

Bienvenue dans cet épisode du balado « Pour l'avenir » de KPMG qui explore l'incidence de l'informatique quantique, une technologie révolutionnaire qui pourrait reconfigurer notre façon de vivre, de travailler et de découvrir. Je suis Tamara Stanners. Plongez avec moi dans un monde de possibilités presque illimitées – et de risques multiples. Nous verrons comment les entreprises peuvent mieux se préparer aux promesses de l'informatique quantique, pour aujourd'hui, pour demain et pour l'avenir.

Pavan Chander (KPMG)

Pensons à la façon dont nos ordinateurs ont évolué au cours des deux dernières décennies : chaque année, ils deviennent plus rapides, plus puissants. De plus, il y a toujours un nouveau produit ou une nouvelle technologie qui fait son entrée sur le marché, ou un fournisseur qui annonce un progrès technologique incroyable.

Narratrice

Selon Pavan Chander, directeur principal au sein de l'équipe de cyberdéfense de KPMG au Canada, l'informatique quantique brisera plusieurs des règles que nous associons aux processeurs et aux appareils utilisés aujourd'hui, y compris une loi importante.

Pavan Chander (KPMG)

La loi de Moore est un concept introduit par [l'ingénieur] Gordon Moore, qui a cofondé Intel dans les années 1960. Selon cette loi, le nombre de transistors pouvant tenir sur une puce informatique double tous les deux ans environ. En termes simples, la puissance et la performance de nos ordinateurs augmentent considérablement au fil du temps parce que nous installons de plus en plus de ces composants minuscules sur une même puce. Ainsi, nous améliorons continuellement la technologie qui rend nos appareils plus rapides, plus petits, plus efficaces. C'est comme avoir une boîte à outils améliorée de plus en plus grande pour résoudre des problèmes plus complexes d'année en année.

Cela dit, maintenant, nous n'arrivons pas à faire [des composants] beaucoup plus petits que ceux que nous faisons

déjà : nous avons atteint un plateau en termes de progrès technologiques, ainsi que de capacité et de puissance informatique. Par conséquent, nous nous attendons à ce que la loi de Moore – et les concepts qui en découlent – sombre dans l'obsolescence au cours des deux ou trois prochaines années.

Narratrice

Ce tournant n'annonce pourtant pas la fin, mais une renaissance du traitement de l'information.

L'informatique quantique, dans toute sa splendeur, promet de démêler en quelques secondes les complexités qui, autrement, occuperaient les ordinateurs traditionnels pendant des mois, voire des années. Avec sa vitesse stupéfiante, elle a le potentiel de relever les défis les plus pressants de l'humanité – en générant des percées médicales, des solutions climatiques, des moyens de renforcer la cybersécurité – et d'ouvrir ainsi une nouvelle ère de découvertes et d'innovations sans précédent.

Mais comme le dit l'adage : « Un grand pouvoir implique de grandes responsabilités. »

Quiconque exploite la puissance de la mécanique quantique vous dira qu'il y a peu de secteurs, voire aucun, qui ne seront pas touchés par ce progrès spectaculaire de la puissance et de la capacité informatique. Soulignons que, si des acteurs malveillants sont en mesure d'accéder à de futurs ordinateurs quantiques beaucoup plus performants, de nouveaux dangers menaceront certainement tous les secteurs.

Sean Wagner (IBM)

Je crois que les craintes de nombreux consommateurs porteront sur la capacité d'un futur ordinateur quantique à potentiellement percer le chiffrement des données, ce qui les affecterait directement.

Narratrice

Selon Sean Wagner, chercheur et défenseur de la technologie chez IBM Canada, pour se préparer aux énormes avantages d'un monde quantique, il faut aussi comprendre certains des risques importants qu'il présente.

Sean Wagner (IBM)

Tout le monde a ses renseignements personnels stockés sur son téléphone, sur son ordinateur portatif ou dans le nuage, qu'il s'agisse de photographies ou d'autres types de données, comme des données financières concernant des comptes bancaires et des renseignements gouvernementaux. Les consommateurs voudront donc savoir si ces renseignements demeureront protégés ou non. Il est certain que l'annonce d'un système qui pourrait perturber tout cela sera une source de préoccupation pour le consommateur moyen. Cependant, je peux vous dire que des solutions sont à notre portée.

Narratrice

Les avantages – et les risques – que posent de ce nouveau type d'informatique sont déterminants pour notre futur proche et pour l'avenir, une situation représentant rien de moins qu'une réinitialisation de notre façon d'envisager le rôle de la technologie dans nos vies. Dans cet épisode, nous explorerons cette transformation à venir et découvrirons pourquoi l'informatique quantique n'est pas qu'une théorie, mais une évolution inéluctable.

Préparer le terrain

Narratrice

Il n'y a probablement pas de meilleure illustration de la façon dont la puissance et le potentiel de l'informatique quantique sont perçus aujourd'hui que la suivante : nous employons l'adjectif « classique » pour décrire la technologie qui alimente nos ordinateurs portatifs et de bureau actuels. Ce mot renvoie à quelque chose de style traditionnel qui se conforme à des méthodes établies depuis longtemps. En fait, « informatique classique » est maintenant le terme utilisé pour désigner même le plus rapide de nos superordinateurs actuels, à puce et à disque dur. Un autre indice du changement radical qui s'opère est l'utilisation du mot « quantique » lui-même, comme l'explique Sean Wagner.

Sean Wagner (IBM)

L'adjective « quantique » dans « informatique quantique » fait vraiment référence à l'application de principes de la mécanique quantique – une branche de la physique – pour faire des calculs. La mécanique quantique est l'étude du comportement des particules microscopiques et de leur interaction entre elles. Ces particules, comme des atomes, des molécules et des électrons, se comportent de manière très différente de ce à quoi nous sommes habitués dans le monde macroscopique. Donc, ce que nous faisons en ce moment dans un ordinateur quantique, c'est d'exploiter ces comportements observés en mécanique quantique et de les appliquer en calculs de sorte à –nous l'espérons bientôt – dépasser les capacités des ordinateurs traditionnels, que nous qualifions maintenant de « classiques ».

Narratrice

Les ordinateurs quantiques fonctionnent selon un principe tout à fait différent de l'informatique classique, une approche complètement nouvelle qui exploite les forces qui ont créé l'univers. Leurs propriétés uniques permettent un traitement incroyablement rapide des données, ainsi que la capacité d'effectuer les calculs les plus complexes. Précisons que ce principe est compris depuis un certain temps, et que les spéculations sur ce qui pourrait se produire lorsque les composants électroniques atteindraient des échelles microscopiques remontent à la fin des années 1950. Bien que d'énormes progrès aient été réalisés dans le domaine de l'informatique quantique, comme le développement de prototypes élémentaires, il faudra encore quelques années avant de faire une utilisation fiable et pratique de cette technologie. Alors, pourquoi l'informatique quantique suscite-t-elle autant d'intérêt ces derniers temps, et en quoi est-elle si prometteuse? Qu'est-ce qui a changé, et pourquoi les dirigeants d'entreprise et d'autres organisations devraient-ils s'y intéresser?

Voici Pavan Chander.

Pavan Chander (KPMG)

L'informatique quantique nous permet de faire un bond exponentiel, ce qui change un peu la donne. Ainsi, je pense que certains des éléments clés auxquels il faut vraiment réfléchir portent sur les risques qu'elle représente.

Pensons au chiffrement des données, qui est un fondement de la sécurité de l'information. Les moyens utilisés pour assurer la confidentialité des données que nous considérons comme sûrs aujourd'hui pourraient ne pas l'être demain. En fait, il existe toute une gamme d'algorithmes de chiffrement qui sont considérés comme vulnérables aux risques associés à l'avancement quantique.

Narratrice

En plus des préoccupations liées à la cybersécurité, l'attention accrue portée à l'informatique quantique au cours des dernières années pourrait s'expliquer par le sentiment d'urgence de mieux se préparer à la prochaine pandémie. En effet, nous nous attendons à ce que les ordinateurs quantiques puissent non seulement aider à mettre au point des vaccins plus rapidement, mais aussi à gérer d'autres problèmes, comme les perturbations dans les chaînes d'approvisionnement qui étaient si fréquentes au début de la pandémie de COVID-19. Pour certains, comme Alexander Rau, collègue de Pavan Chander et responsable des Services-conseils en gestion des risques quantiques chez KPMG au Canada, il est peut-être temps que les gens se préparent à se doter des capacités informatiques nécessaires pour faire le grand sauf évolutif.

Alexander Rau (KPMG)

Les ordinateurs binaires, comme nous le savons, ont été développés pendant la Seconde Guerre mondiale, puis ont évolué jusqu'à aujourd'hui. Pendant la pandémie, nous avons assisté à l'essor du télétravail, des télécommunications et d'autres secteurs connexes, qui a été possible grâce à l'environnement informatique à notre disposition. La prochaine étape de cette évolution sera l'informatique quantique, qui s'associera à l'humanité par l'intermédiaire des technologies de l'information, passant du binaire au monde quantique, pour résoudre des problèmes que nous aimerions résoudre aujourd'hui et qui prendraient trop de temps, voire une éternité, mais que nous voulons résoudre beaucoup plus rapidement.

L'avancée des technologies de l'information ne sera pas seulement une croissance exponentielle à deux dimensions. Je pense qu'elle sera presque tridimensionnelle. Cette évolution ouvrira également de nouveaux domaines en informatique – ou même en recherche et en science – auxquels nous ne pensons même pas aujourd'hui. Il y a donc beaucoup de possibilités de « prochaines étapes » qui ressortent de ces changements.

Narratrice

Pour Alexander Rau, une allusion historique peut renforcer la nécessité pour les entreprises, les gouvernements et les consommateurs de porter attention à la puissance et à la portée de la technologie quantique.

Alexander Rau (KPMG)

Devrions-nous déjà nous soucier de l'informatique quantique? La réponse est oui. C'est presque comme – si certains d'entre nous s'en souviennent – le problème du bogue de l'an 2000 : au début des années 1990 ou peut-être à la fin des années 1980, nous avons pris conscience qu'il y avait un problème avec nos ordinateurs binaires. Nous avons donc travaillé à une solution quelques années avant l'événement. Alors pourquoi devons-nous faire la même chose avec le virage quantique? Parce que l'un des problèmes de ce changement est le risque quantique, c'est-à-dire que les ordinateurs quantiques seront en mesure de percer les algorithmes cryptographiques traditionnels beaucoup plus rapidement. Par exemple, si vous avez des données qui datent de 20 ans et que quelqu'un les déchiffrait en 20 ans, est-ce que ces données lui seraient vraiment utiles? Toutefois, si l'informatique quantique se mettait de la partie au cours des 5 à 10 prochaines années et accélérait le déchiffrement, ces mêmes données confidentielles pourraient toujours être pertinentes. Comme les ordinateurs quantiques pourraient accéder à des données utiles, nous devons nous pencher sur le risque quantique. Les propriétaires d'entreprise devez vraiment réfléchir aux données et aux renseignements qu'ils stockent aujourd'hui et qui pourraient être vulnérables aux ordinateurs quantiques de demain.

Narratrice

La cybersécurité et le chiffrement des données sont des sujets chauds de l'informatique quantique, et nous les examinerons plus loin dans cet épisode. Mais tout d'abord, à quoi ressemble un ordinateur quantique, et que se passe-t-il à l'intérieur de ces dispositifs bizarres tout droit sortis de vieux films de science-fiction? Pour le savoir, nous devons visiter l'un des endroits les plus froids de l'univers.

Sean Wagner (IBM)

Une chose que je voudrais souligner à propos des ordinateurs quantiques, c'est que nous devons en refroidir le processeur à une température très basse. Il s'avère que cette température est en fait très proche de la température la plus basse que nous pouvons atteindre, appelée le zéro absolu. C'est à peu près moins 273 degrés Celsius. Nous faisons fonctionner nos processeurs quantiques à 0,015 degré au-dessus du zéro absolu. C'est même plus froid que l'espace. Vous pensiez que l'espace était l'endroit le plus froid de l'univers? Non, c'est en fait à l'intérieur d'un ordinateur quantique en ce moment.

Narratrice

Comme l'explique Sean Wagner d'IBM, l'ennemi numéro un des ordinateurs quantiques est la chaleur.

Sean Wagner (IBM)

Nous devons garder la température du processeur quantique aussi basse que possible parce que c'est à cette température que nous observons des propriétés supraconductrices des matériaux qui le composent, en particulier l'aluminium qui est utilisé dans les circuits du processeur. Donc, nous avons besoin de cette température pour obtenir ces propriétés et, ainsi, un certain comportement de la mécanique quantique.

L'autre raison pour laquelle nous devons refroidir le processeur à une très basse température est d'éliminer les sources d'interférence. En effet, l'information contenue dans les bits quantiques est assez sensible. Elle peut être perturbée par une infime quantité d'énergie, comme l'énergie perdue qui provient de n'importe où et qui nuit au fonctionnement de tout le système. Ainsi, en refroidissant le processeur à une très basse température, nous éliminons l'énergie thermique qui pourrait causer cette interférence.

En résumé, nous avons besoin de cette basse température pour que le processeur quantique fonctionne au mieux de ses capacités.

Narratrice

Lorsqu'on demande à Sean Wagner de parler de l'apparence des ordinateurs quantiques d'IBM, sa description est pour ainsi dire éclairante.

Sean Wagner (IBM)

Souvent, les gens regardent [un ordinateur quantique] et trouvent que ça ressemble à un lustre sophistiqué, un luminaire luxueux qu'on pourrait voir, par exemple, dans un bel hôtel ou dans la maison de quelqu'un. Nous l'appelons donc le lustre.

Il existe de nombreuses formes différentes d'ordinateurs quantiques, et cela dépend vraiment du type de technologie qui est employée dans ces systèmes. Chez IBM, nous utilisons un type particulier de technologie basée sur des dispositifs supraconducteurs. Et donc, au cœur de notre système se trouve une puce de traitement quantique. C'est une micropuce, au même titre que les micropuces numériques, sauf qu'elle se compose d'un ensemble de dispositifs que nous appelons des bits quantiques ou qubits. Cette puce est à l'intérieur d'un grand cylindre que nous appelons un cryostat, qui sert à refroidir ce processeur à une température très basse – dont nous avons besoin pour obtenir les effets supraconducteurs de la puce. À l'intérieur de ce système cylindrique très complexe, qui sert de refroidisseur, il y a aussi un ensemble de plaques métalliques à plusieurs niveaux reliées avec des fils.

Cette configuration sert à refroidir le processeur quantique et à envoyer des signaux vers le bas, qui viennent de la partie supérieure du système et voyagent à travers des fils. Ces derniers transmettent ensuite les signaux aux composants électroniques de commande. Enfin, ce sont ces composants qui commandent les dispositifs quantiques sur cette puce.

Narratrice

Au cas où vous vous demandez si votre service informatique aura besoin de construire une « salle de stockage » quantique géante comme celle de l'ordinateur HAL, dans le film *2001: l'odyssée de l'espace* de Stanley Kubrick, ne vous inquiétez pas. Selon Pavan Chander, l'informatique quantique est et sera disponible sur le nuage dans un avenir pas très lointain.

Pavan Chander (KPMG)

L'informatique quantique n'est pas une puce ou une sorte d'accessoire USB qu'on pourrait ajouter à un ordinateur. Bien qu'on parle dernièrement beaucoup de l'apprentissage machine intégré des téléphones intelligents et d'autres appareils, l'informatique quantique ne sera pas accessible comme cela. Je pense que, pour donner accès à cette technologie et à la puissance qu'elle promet, nous allons nous retrouver avec un modèle d'« ordinateur central » de la vieille école, qui agira comme un superordinateur dans un emplacement centralisé auquel plusieurs personnes accèdent par bloc de temps. Par exemple, certaines grandes organisations pourraient décider de fournir un ordinateur quantique sur leur lieu de travail, comme pour les efforts de leur service de recherche et développement, et en louer l'accès à de plus petites organisations.

Un autre exemple serait quelque chose comme Google Cloud, qui est un fournisseur centralisé permettant aux organisations d'accéder à ses capacités informatiques. Ainsi, un ordinateur quantique pourrait être mis à votre disposition dans un format similaire à celui que nous utilisons pour accéder à nos ressources infonuagiques actuelles.

Narratrice

Pour que la transformation quantique se concrétise pleinement, les leaders des affaires, des gouvernements et de l'éducation devront collaborer pour sortir la technologie des laboratoires d'expérimentation et pour l'intégrer au reste du monde, ce qui représente une tâche colossale : convaincre à la fois leurs équipes et leur conseil d'administration qu'il y a des problèmes que les ordinateurs classiques ne seront tout simplement jamais en mesure de résoudre, et qu'il est impératif, dans cette optique, d'adopter l'informatique quantique non seulement pour prospérer, mais aussi pour survivre. Notons aussi que, comme toujours, ceux qui mènent de front la transformation seront probablement les premiers à en retirer les fruits.

La quantique, pertinente pour tous les secteurs

Narratrice

Imaginez que vous êtes responsable de l'exploitation ou des systèmes d'information d'une grande entreprise et que vous devez présenter à la direction une nouvelle technologie formidable et révolutionnaire qui en est encore à la phase de développement – et qui ne sera pleinement applicable à votre entreprise que dans plusieurs années. De plus, vous devez convaincre les décideurs que c'est **maintenant** le moment de se préparer à ce changement majeur.

Un bon point de départ serait peut-être le plus simple : les entreprises prêtes à tirer parti de l'énorme capacité de l'informatique quantique bénéficieront d'un avantage concurrentiel inestimable. Qu'il s'agisse d'exploiter un réseau de distribution plus efficace ou d'effectuer des recherches scientifiques plus poussées, les résultats atteindront des proportions inimaginables. Toutefois, la transition opérationnelle n'a pas besoin d'être compliquée. Selon Alexander Rau, l'adaptation à la quantique devrait s'apparenter à une évolution plutôt qu'à une révolution.

Alexander Rau (KPMG)

Il ne s'agit pas de réinitialiser le système. Je pense que ce sera une continuation. Comparons [cette transition] à des changements associés à l'évolution de la science, comme le travail manuel des années 1600 qui a été transformé par l'arrivée des moteurs à vapeur. Nous n'avons pas appuyé sur le bouton Réinitialiser; nous avons tout simplement intégré ou mis en œuvre les nouvelles technologies dans les processus déjà en place pour les simplifier afin de les rendre plus efficients, plus efficaces et plus productifs. Et je pense que ce sera la même chose pour l'informatique quantique : nous l'intégrerons à l'évolution des technologies de l'information et, ainsi, deviendrons plus efficaces et plus efficients, et pourrons nous attaquer à des problèmes différents ou émergents que nous n'aurions pas été en mesure de régler auparavant.

Narratrice

Alexander Rau nous donne également un exemple remarquable d'un secteur qui aurait intérêt à profiter de l'avantage quantique et nous parle de la façon dont KPMG au Canada pourrait contribuer à faciliter la transition technologique [dans ce secteur].

Alexander Rau (KPMG)

Dans l'industrie médicale, par exemple, nous pourrions utiliser les ordinateurs quantiques pour simuler ou mettre au point de nouveaux médicaments ou traitements qui peuvent aider l'humanité à être en meilleure santé, à vivre plus longtemps et, au bout du compte, à avoir une meilleure qualité de vie. Supposons que vous êtes propriétaire d'une entreprise dans le secteur médical, comme un organisme de recherche médicale ou quelque chose du genre. Comment pourriez-vous vous préparer à l'arrivée de l'informatique quantique, qui vous permettra d'accélérer considérablement le développement de médicaments? La raison pour laquelle vous devriez réfléchir à cette question aujourd'hui est que si vous ne le faites pas, la concurrence le fera. La première personne à utiliser la technologie pour accéder plus rapidement au marché aura l'avantage concurrentiel et attirera évidemment plus de clients.

C'est comme tout ce qui se rapporte à l'innovation. Si vous créez quelque chose de génial et que vous le mettez rapidement en marché, vous pouvez tirer parti du fait d'en avoir l'exclusivité. Je crois que ce sera aussi très pertinent et très important avec l'informatique quantique. Alors pourquoi devriez-vous penser à cette technologie aujourd'hui? Nous voulons nous assurer que vous êtes au courant des possibilités qui s'offrent à votre entreprise – des secteurs d'activité où l'informatique quantique pourrait vous aider à en améliorer l'efficacité et l'efficience – et qu'elle est prête à la transition en discutant avec les experts.

Narratrice

Ce n'est pas seulement dans les laboratoires de recherche que l'informatique quantique peut produire des résultats qui changeront la donne. Pour Sean Wagner d'IBM peu d'aspects de la vie **ne** seront **pas** touchés par l'énorme puissance du calcul quantique de la technologie.

Sean Wagner (IBM)

Certes, il y a de gros problèmes auxquels nous pourrons nous attaquer à l'aide d'un ordinateur quantique, comme la découverte de nouveaux médicaments, le développement de nouveaux matériaux, la lutte contre des enjeux importants – les changements climatiques, le développement durable, etc. Oui, l'informatique quantique jouera un rôle à cet égard. Cependant, il y a des problèmes de tous les jours dans le monde des affaires que nous pourrons aussi résoudre à l'aide de ceux-ci, et j'en ai plusieurs exemples.

D'abord, beaucoup d'entreprises ont une chaîne d'approvisionnement à optimiser. Ainsi, il est possible qu'elles puissent utiliser un ordinateur quantique pour trouver de meilleures solutions globales à des problèmes d'optimisation de la livraison de leurs biens ou de la réception des intrants pour les produits qu'ils fabriquent.

Ensuite, bon nombre d'organisations rencontrent des difficultés dans l'optimisation de leur planification, n'est-ce pas? Pensez aux compagnies aériennes qui doivent gérer leurs équipages, leurs équipements, leurs pilotes et tous les autres services opérationnels de leur flotte. Il s'agit là de choses qui pourront être optimisées à l'aide d'un ordinateur quantique, qui pourra exécuter ce genre de processus de façon continue au fil des changements et de l'évolution des activités de la compagnie aérienne, et ce, dans le but de corriger, disons, les perturbations qui peuvent survenir quotidiennement. Ainsi, la compagnie pourra continuellement atteindre son meilleur point d'exploitation chaque jour.

Par ailleurs, dans le cas de nombreuses entreprises, il est nécessaire d'analyser les tendances dans les données qui pourraient révéler des choses, comme de la fraude ou d'autres utilisations abusives de leurs services. Les ordinateurs quantiques peuvent potentiellement aider à effectuer ce travail au fur et à mesure que les données entrent.

Enfin, sur le plan économique, il y aura peut-être des façons d'utiliser les ordinateurs quantiques pour modéliser continuellement la façon dont l'économie se porte – voire la façon dont [des fonds] comme votre portefeuille de placements se porte sur le marché, pour trouver les meilleures stratégies qui vous permettront d'améliorer son rendement.

Il y a donc de nombreuses applications commerciales quotidiennes pour les ordinateurs quantiques – outre les problèmes d'envergure sur lesquels nous croyons que la technologie aura une grande incidence.

Narratrice

Au carrefour des défis technologiques à grande échelle et de l'usage quotidien se trouve la quête constante d'améliorer les batteries qui alimentent les véhicules électriques. Selon Pavan Chander, le potentiel de l'informatique quantique en matière d'innovation et de résolution de problèmes y sera évident.

Pavan Chander (KPMG)

Un autre exemple où l'informatique quantique sera bénéfique est la conception de batteries pour véhicules électriques. Nous utilisons actuellement des batteries aux ions de lithium. Nous les utilisons depuis de nombreuses années, et elles fonctionnent bien. Malgré cela, il y a évidemment des limites à ce qu'elles peuvent faire. Alors que la technologie des batteries progresse lentement depuis un certain temps, nous espérons qu'un ordinateur quantique pourra nous aider à modéliser l'interaction complexe entre les éléments chimiques pour nous permettre de concevoir un tout nouveau type de batterie qui utilise des éléments complètement différents au lieu des ions de lithium.

Contrairement à un ordinateur classique, qui peut prendre cinq mois à concevoir un modèle et des années à en faire l'essai, nous pourrions réduire cela à quelques jours ou à quelques semaines avec un ordinateur quantique.

Narratrice

Les avantages de l'informatique quantique pour la société seront incommensurables. De découvertes médicales et d'avancées technologiques qui changent la vie des gens à la prestation de services locaux courants ou de livraison, l'incidence de cette technologie se fera sentir à tous les niveaux.

Cependant, en tant que technologie transformatrice,

l'informatique quantique peut aussi potentiellement causer beaucoup de tort. On craint que la puissance du calcul quantique ne soit exploitée à des fins d'espionnage criminel ou industriel, et qu'un « retard quantique » ne laisse les pays sous-développés encore plus à la traîne. Et pourtant, la puissance quantique pourrait offrir une solution aux problèmes mêmes qu'elle pourrait créer…

Faire le saut quantique

Narratrice

Pour quiconque connaît le potentiel de la technologie quantique, comme Pavan Chander, les risques devraient être traités aussi sérieusement que les avantages que promettent les ordinateurs quantiques. Un exemple que le directeur utilise pour renforcer ce point est à la portée de la plupart des gens.

Pavan Chander (KPMG)

Nous avons enseigné aux gens que lorsqu'ils utilisent un réseau wifi public, saisissent leurs données de connexion ou effectuent des opérations bancaires ou des achats en ligne, ils doivent toujours chercher l'icône de cadenas, [qui apparaît quand l'URL contient] le « HTTPS ». Cette icône indique qu'il y a un canal sécurisé entre eux, sur leur appareil, et où ils essaient de se connecter. Ainsi, lorsque vous tapez votre mot de passe pour accéder à vos services bancaires en ligne ou pour [passer une commande sur le site d']un détaillant, ou lorsque vous faites toute autre chose que ce soit en ligne, grâce à un protocole TLS, vos données sont sécurisées pendant le transfert. Et avec la technologie actuelle, nous considérons qu'il s'agit d'un moyen de communication sûr.

Maintenant, le risque que pose l'informatique quantique est que si quelqu'un était en mesure d'intercepter ce transfert de données et d'avoir accès à un ordinateur quantique suffisamment puissant, il serait en mesure de déchiffrer ou de surveiller l'information en texte brut. Ainsi, tout ce que nous avons appris au public à propos de l'importance de cette icône de cadenas, ce « HTTPS », n'aura en quelque sorte plus de valeur dès qu'un ordinateur quantique se mettra de la partie. Notre technologie actuelle ne peut pas vraiment assurer la sécurité quantique, et donc la connexion sécurisée d'aujourd'hui ne sera pas sûre pour toujours dans un avenir quantique.

Narratrice

Pour Alexander Rau, de KPMG au Canada, et bien d'autres, l'une des plus grandes menaces économiques et politiques du risque quantique de notre époque est : le vol de renseignements.

Alexander Rau (KPMG)

Mon inquiétude au sujet de l'informatique quantique, c'est l'idée que chaque technologie peut être transformée en arme et utilisée par des acteurs malveillants, par exemple, pour voler de l'argent, ou pour accéder à des données [confidentielles] ou pour attaquer des organisations. Je sais que chaque bonne technologie entre de mauvaises mains peut être dangereuse, et c'est ce qui m'empêche de dormir sur mes deux oreilles.

Si les chercheurs d'un centre de recherche universitaire en médecine utilisent l'informatique quantique pour développer le prochain médicament ou traitement contre le cancer, c'est génial. C'est vraiment à cela que nous, l'humanité, espérons que cette technologie serve. Cependant, de la même façon, cette puissance de calcul [au service de la science] que permet l'informatique quantique peut aussi être utilisée par les « méchants » pour créer de nouvelles techniques, de nouveaux outils d'attaque et de nouvelles façons d'utiliser les rançongiciels – par exemple, de trouver les failles du jour zéro, comme des vulnérabilités dans les défenses organisationnelles pour avoir accès à leurs réseaux et y déployer des rançongiciels. Donc, ce qui me cause de l'insomnie la nuit, c'est comment les « méchants » utiliseront cette bonne technologie pour extorquer de l'argent ou autres choses.

Narratrice

Selon toute probabilité, les méthodes de chiffrement actuelles ne seront tout simplement pas à la hauteur de la tâche pour nous défendre contre de futures attaques quantiques. Et si l'on croit qu'il s'agit d'un enjeu à aborder plus tard, Pavan Chander suggère de changer son fusil d'épaule.

Pavan Chander (KPMG)

Au cours des deux dernières années, le gouvernement américain a vraiment fait pression pour élaborer de nouveaux types d'algorithmes de chiffrement qui seront sûrs, même sur le plan quantique. Et très bientôt, on peut s'attendre à ce que les fournisseurs de logiciels commencent à implémenter ces nouveaux algorithmes dits « résistants » ou « sûrs » dans leurs produits. À ce moment-là, les organisations devront commencer à suivre et à bien comprendre ce qui est mis sur le marché, à comprendre quelles sont les capacités offertes, et à effectuer un examen interne pour voir où elles peuvent être plus fortes. Ainsi, quels de vos produits technologiques devriez-vous remplacer? Il se peut que vous restiez avec le même fournisseur et qu'il lance simplement une nouvelle version de son produit. Ou peut-être que certains fournisseurs n'avancent pas assez vite et que de nouvelles entreprises en démarrage offrent [des produits ou des services] plus rapidement qu'eux sur le marché. Il se peut que vous ayez à comparer des fournisseurs ou à évaluer le paysage du secteur pour connaître ce qui existe.

Narratrice

Avec les États-nations priorisant leurs efforts en matière d'informatique quantique et d'intelligence artificielle, il ne semble pas y avoir de temps à perdre non seulement pour se préparer aux avantages de l'informatique quantique, mais aussi pour éviter tout excès de confiance à l'égard de vos mesures actuelles de chiffrement des données, peu importe leur efficacité apparente. Voici à nouveau Pavan Chander.

Pavan Chander (KPMG)

Par conséquent, en ce qui concerne le risque que posent les ordinateurs quantiques pour les organisations, l'un des plus grands champs d'intérêt qui me viennent à l'esprit est la protection des données. Aujourd'hui, nous utilisons le chiffrement pour protéger nos données. Il existe une grande variété d'algorithmes et de façons différentes et sophistiquées de protéger les données qui sont robustes, selon les normes actuelles. Comme nous savons que les ordinateurs sont de plus en plus puissants, nous concevons ces mécanismes de

protection en nous demandant pendant combien de temps nous voulons que les données soient en sécurité. Une organisation, par exemple, cherche probablement à assurer la sécurité de ses données pour les prochaines décennies. Et c'est probablement dans les limites de sa tolérance au risque. Nous n'avons pas nécessairement besoin de concevoir des algorithmes qui seront résistants pendant 50 ans, voire 100 ans.

Cela dit, en ce qui concerne l'informatique quantique, le taux de progression est beaucoup plus élevé que l'informatique classique – je dirais même exponentiellement plus élevé. Donc, ce que nous pensions être sûr aujourd'hui pour des décennies ne le sera plus. Nous nous attendons à ce qu'un ordinateur quantique soit capable de prendre des données chiffrées – considérées comme protégées aujourd'hui – et de percer ce chiffrement en très peu de temps.

Narratrice

À mesure que l'informatique quantique deviendra plus accessible, elle ne sera pas nécessairement exploitée par des génies criminels. Pour Alexander Rau, le danger que posent les pirates informatiques amateurs ne sera pas moins dommageable pour les organisations qui ne sont pas préparées [au monde quantique].

Alexander Rau (KPMG)

Lorsque l'informatique quantique commencera à alimenter l'infrastructure sous-jacente, ces éléments technologiques pourront être utilisés par des personnes sans connaissance technique pour concevoir des outils ou des stratégies d'attaque contre les organisations. Ainsi, quelqu'un qui n'a aucune compréhension technologique peut simplement taper [son intention] et, avec l'aide de l'informatique quantique et, par-dessus le marché, celle de l'intelligence artificielle, créer une arme pouvant servir à attaquer des organisations à travers le monde.

Je ne sais pas si vous avez déjà entendu le terme « pirates néophytes », ou « *script kiddies* » en anglais. Il s'agit de jeunes ou de novices – installés dans un sous-sol, je suppose – qui copient des codes d'attaques [disponibles sur le Web] et qui déchaînent ces programmes nuisibles sur les organisations du monde entier. Avec des progrès technologiques, comme l'informatique quantique et l'intelligence artificielle, n'importe qui pourrait faire partie de la prochaine génération de pirates amateurs et [même] créer du code pour nuire ou attaquer les organisations.

Narratrice

Toutefois, compte tenu du potentiel d'atteintes à la sécurité de plus en plus graves et dommageables, de nouvelles normes de chiffrement seront nécessaires pour contrer l'extraordinaire puissance de déchiffrage du calcul quantique. Selon Sean Wagner, des efforts sont déjà en cours.

Sean Wagner (IBM)

Heureusement, de nouvelles normes cryptographiques sont en cours d'élaboration. Aux États-Unis, le National Institute of Standards and Technology, aussi connu sous le nom de NIST, est en train de procéder à une normalisation. Trois des quatre normes qui seront mises de l'avant ont en fait été corédigées par IBM. Nous avons donc investi considérablement dans la recherche de nouveaux protocoles cryptographiques à l'épreuve du calcul quantique. Il existe des outils que les entreprises peuvent utiliser pour entamer un processus d'analyse qui déterminera où la cryptographie est utilisée au sein de leur organisation, puis pour commencer à élaborer un plan d'action avant même que les normes ne soient entièrement établies – ce qui devrait être le cas plus tard cette année. Et il y a beaucoup d'organisations qui ont commencé ce travail.

Narratrice

Afin de souligner à quel point ces menaces à la cybersécurité pourraient nous toucher directement, Sean Wagner parle d'une cible commerciale potentielle avec laquelle la plupart d'entre nous sommes quotidiennement en contact.

Sean Wagner (IBM)

Par exemple, le secteur des télécommunications est très préoccupé par la possibilité que des acteurs malveillants utilisent un ordinateur quantique à l'avenir pour percer le chiffrement de leurs données. Ainsi, IBM, en collaboration avec Vodafone, a formé un groupe de travail sous l'égide de la Global Telecommunications Industry Association, ou GSMA, pour créer un parcours ou un ensemble de méthodes et de conseils pour accompagner ce secteur dans la transition vers la sécurité quantique et, ultimement, pour rendre tous nos systèmes de communication résistants aux futurs ordinateurs quantiques.

Narratrice

Avec les menaces à la sécurité qu'alimente l'ouverture quantique d'un monde anarchique d'espionnage et de cybercriminalité, d'autres gouvernements suivront-ils l'exemple des États-Unis dans la création d'un nouveau cadre de réglementation et [dans la mise en place] de mesures de sécurité [renforcées]. Alexander Rau en est persuadé parce que ne pas le faire pourrait mener au pire scénario envisageable.

Alexander Rau (KPMG)

Quel genre de règlements verrons-nous à l'avenir? Je pense que l'avenir, c'est maintenant. Nous voyons déjà des gouvernements qui considèrent [le calcul quantique] comme un risque. En particulier, le gouvernement des États-Unis est très proactif lorsqu'il s'agit de mettre en place des lois ou des cadres réglementaires en matière de risque quantique. En fait, il a déjà établi des échéanciers en ce qui concerne le moment où ses organismes devraient avoir au moins un plan de préparation ou de mise en œuvre quantique qui répond à ce risque. Et à mesure que la course à l'informatique quantique s'intensifiera et que nous nous rapprocherons [de la ligne d'arrivée], de plus en plus de pays et de gouvernements emboîteront le pas pour assurer la sécurité non seulement de leurs entreprises et organisations, mais aussi de leurs citoyens.

Notons que la technologie pourrait être utilisée pour faire la guerre : de la même manière que les ordinateurs traditionnels sont déjà utilisés en temps de guerre, les ordinateurs quantiques le seront tout autant. Ainsi, nous devons nous assurer d'être prêts. Je pense donc qu'aux États-Unis et dans l'Union européenne, nous commençons à voir certaines de ces mises en œuvre initiales ou l'apparition des premières formes

de loi ou de règlement. Les États-Unis sont vraiment une force motrice dans le domaine. Au Canada, rien n'a été annoncé, mais nous suivons de très près – ou encourageons les organisations à suivre – le modèle américain parce que nous avons l'impression qu'il sensibilise au moins les gens et les entreprises à la nécessité d'agir.

Narratrice

Certaines sociétés en sont déjà aux premières étapes de l'adoption de l'informatique quantique dans leurs stratégies d'affaires. Selon Pavan Chander, de KPMG au Canada, une partie de la transition consistera à intégrer les capacités de la technologie quantique à l'infrastructure informatique actuelle.

Pavan Chander (KPMG)

Il y a beaucoup de travail en cours actuellement pour déterminer à quoi ressemblera l'intégration. En effet, des efforts considérables sont déployés pour développer ce que nous appelons un intergiciel visant à implémenter la quantique. Il s'agit d'un moyen de connecter les infrastructures informatiques traditionnelles, y compris les ordinateurs classiques qui y sont associés, et l'infrastructure quantique. Une fois que vous avez cette solution, vous devez déterminer où installer cet intergiciel. Comment communique-t-il avec le système quantique dorsal? Comment accède-t-il aux données et aux autres ressources dans l'infrastructure informatique classique de votre organisation?

La tâche s'annonce difficile. Il faudra beaucoup de temps pour trouver la solution optimale pour un secteur d'activité donné ou même pour une organisation en particulier. Mais pour l'instant, je dirais que l'objectif est que les entreprises commencent à réfléchir à leurs cas d'utilisation et à ce qu'elles voudraient mettre en œuvre comme démonstration de faisabilité. La clé, c'est vraiment de commencer maintenant.

Narratrice

Compte tenu du potentiel extraordinaire qui s'offre aux entreprises, un personnel formé sera un élément essentiel pour se préparer à entrer dans un monde quantique auquel elles ne sont peut-être pas tout à fait prêtes. Voici Alexander Rau.

Alexander Rau (KPMG)

La réticence des organisations à ne pas aller de l'avant pour répondre à leurs besoins opérationnels n'est pas tant causée par la peur que par un manque d'éducation du grand public à l'égard de l'informatique quantique. En effet, s'il y a un nouveau progrès technologique qui s'en vient et que nous n'y connaissons rien, notre première réaction – qui est une réaction tout à fait humaine à mon avis – est la méfiance, n'est-ce pas? Plutôt que d'être optimiste et de voir les avantages – et les inconvénients – évidents de ces types de technologie. Je pense donc que l'éducation visant à aider les organisations à comprendre les avantages potentiels de l'informatique quantique –non seulement pour elles-mêmes, mais aussi pour les humains et l'humanité dans son ensemble – aidera vraiment à éviter ou à ne pas alimenter une peur.

Se préparer aujourd'hui à un avenir quantique

Narratrice

Tout au long de cet épisode, vous avez entendu nos invités parler de l'importance – ou de l'urgence, selon certains – de préparer votre entreprise ou votre organisation au jour où l'accès à l'informatique quantique et à ses énormes capacités ne sera plus qu'à un clic. Peu d'entreprises disposeront probablement du soutien interne nécessaire pour rendre leurs mesures de chiffrement résistantes à des cyberattaques quantiques, ou simplement pour se préparer au fardeau opérationnel de l'implémentation de l'informatique quantique qui pèsera sur le flux de travail et la productivité. C'est là que, pour Pavan Chander, des cabinets comme KPMG au Canada peuvent contribuer à mettre de l'ordre dans ce qui peut sembler une situation incroyablement chaotique. Selon lui, la technologie offre une occasion en or d'augmenter l'efficacité opérationnelle.

Pavan Chander (KPMG)

Je pense que les organisations devraient commencer à se demander si elles ont la capacité interne de déterminer lesquelles de leurs composantes technologiques pourraient être considérées comme faibles sur le plan quantique. Si ce n'est pas le cas, envisagez de faire appel à un tiers qui pourrait vous fournir ce genre d'expertise cryptographique : pour repérer les algorithmes utilisés, dans quels produits et dans quels secteurs de votre entreprise, pour examiner les processus opérationnels et voir quels cas d'utilisation du chiffrement pourraient être vulnérables à l'informatique quantique, et pour aider l'organisation à dresser un inventaire de ses diverses composantes qui sont considérées comme non sécuritaires sur le plan quantique.

D'après nos observations, nous constatons souvent que la majorité des entreprises n'ont pas nécessairement une équipe chevronnée de cryptographie à l'interne. Nous avons pu collaborer avec ces organisations pour les aider à déterminer où la cryptographie est utilisée, dans quel processus opérationnel, et à savoir si elle est considérée comme sûre sur le plan quantique.

Narratrice

Comme Pavan Chander, Alexander Rau croit qu'en faisant appel à une expertise externe, les entreprises pourront évaluer leur exposition au risque et accéder à des moyens de surveiller leurs arrières, ainsi que prendre les devants et pouvoir saisir les nouvelles occasions.

Alexander Rau (KPMG)

Comment KPMG peut-il vous aider? Nous pouvons aider votre organisation à effectuer une évaluation du risque quantique, par exemple, pour examiner [la vulnérabilité de] vos données. Il s'agit là du premier volet. L'autre volet porte sur la compréhension de ce que l'informatique quantique apportera en termes de possibilités. Nous voulons nous assurer que vous êtes au courant des possibilités qui s'offrent à votre entreprise – des secteurs d'activité où l'informatique quantique pourrait vous aider à en améliorer l'efficacité et l'efficience – et qu'elle est prête à la transition en discutant avec les experts.

Narratrice

Les détails sont importants aux yeux des sociétés et des organisations qui se penchent sur les avantages et les risques pratiques associés à l'informatique quantique. Et pourtant,

Alexander Rau conseille aux leaders du monde des affaires – aux leaders en tout genre, en fait – de ne pas oublier que cette technologie extraordinaire pourrait ouvrir notre monde à des avancées incroyables dans l'exploration spatiale, à de nouvelles mesures de protection de l'environnement, à de grandes percées médicales… et à d'autres progrès pour l'avenir.

Alexander Rau (KPMG)

Ce qui m'emballe avec l'informatique quantique, c'est qu'elle pourra aider l'humanité à résoudre des problèmes que les ordinateurs traditionnels ne sont pas en mesure de résoudre ou prennent très longtemps à faire. Mais plus encore, les problèmes que nous ne connaissons même pas encore et que des ordinateurs quantiques pourront résoudre. En effet, l'avantage technologique, c'est aussi de voir une technologie [sous tous ses angles] et de faire quelque chose à laquelle personne n'a vraiment pensé. Par exemple, est-ce qu'elle pourrait nous transporter plus vite sur Mars? Pourrait-elle créer une énergie de fusion propre? C'est ce qui m'enthousiasme, car je crois que l'informatique quantique est une bonne technologie. Elle aidera l'humanité à progresser plus rapidement dans des domaines, au-delà même de notre imagination.

Grâce à cette technologie, j'ai l'espoir d'un monde meilleur en matière de santé, d'environnement… L'informatique quantique sera-t-elle en mesure de créer des batteries électriques qui nécessitent moins de ressources, y compris moins d'extraction à la source? J'espère ardemment qu'elle règlera certains des problèmes auxquels l'humanité est confrontée de nos jours – en matière d'environnement, de soins de santé et, peut-être de façon un peu trop optimiste, de guerre. C'est peut-être un peu trop ambitieux de penser que [cette technologie] résoudra tous les problèmes du monde, mais j'ai vraiment espoir qu'elle en résoudra beaucoup.

Narratrice

Dans le prochain épisode de *Pour l'avenir* : l'intelligence artificielle est sur le point de s'attaquer aux problèmes commerciaux et scientifiques les plus complexes. L'IA promet de nouvelles perspectives, de nouveaux outils, un traitement rapide des mégadonnées, sans compter une capacité [incroyable] d'imiter le comportement humain. Tout cela s'en vient, et bientôt. En fait, le développement de l'IA est plus rapide que prévu. Toutefois, cette technologie qui offre des avantages économiques présente aussi de réels dangers.

Votre entreprise est-elle prête pour cette transformation?

L'IA et vous, la prochaine fois à *Pour l'avenir*.

Merci de votre écoute.