RAIFFEISEN

Raiffeisen Suisse
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Le point de vue du chef économiste de Raiffeisen

Une once de réconfort

«Quantum of Solace» («une once de réconfort») est le titre du film de James-Bond réalisé par Marc Forster, qui est sorti fin 2008 dans les salles de cinéma. C'est aussi le deuxième film de la série dans lequel Daniel Craig incarne le personnage principal. Initialement, le film devait s'intituler «un minimum de réconfort», mais le titre fut modifié par la suite afin de souligner le lien avec l'organisation secrète que combat James Bond dans le film. Il nous reste aussi un peu de réconfort quand nous nous intéressons à l'informatique quantique. Alors que l'intelligence artificielle est sur toutes les lèvres, l'informatique quantique devrait bientôt être «the next big thing». Une technologie prometteuse qui se développe à une vitesse fulgurante, mais qui crée aussi déjà une zone d'ombre sur l'ici et maintenant.

Comment les ordinateurs quantiques fonctionnent-ils?

Les ordinateurs quantiques travaillent avec des bits quantiques, également qualifiés de qubits. Non seulement, ceux-ci peuvent peut représenter simultanément les états 0 et 1, mais aussi n'importe quel état intermédiaire. Cette capacité qualifiée de «superposition» permet à l'ordinateur quantique d'effectuer simultanément un grand nombre de calculs. En raison du principe de l'«enchevêtrement», les qubits peuvent par ailleurs restés liés même sur de longues distances. Ces deux propriétés confèrent à l'ordinateur quantique le potentiel de résoudre des problèmes qui seraient insolubles pour des ordinateurs classiques ou qui nécessiteraient des moyens gigantesques.

Obsolescence des procédés de cryptage courants

Cette évolution débouche sur un problème majeur: la sécurité des données. En raison de la puissance bien supérieure des ordinateurs quantiques par rapport aux super-ordinateurs traditionnels, tous les procédés de cryptage des données actuels ne suffiront plus. L'algorithme pour percer les méthodes de cryptage actuelles existe déjà. Il manque juste l'ordinateur suffisamment puissant pour l'exécuter. Le «Q-Day», à savoir le jour où un ordinateur quantique atteindra ce palier, n'est cependant pas prévu avant plusieurs années. Il n'empêche que des mesures significatives sont requises dès à présent.

Une action requise de toute urgence

La sécurité des données est l'un des principaux piliers de notre monde et le cryptage est omniprésent. La consultation d'un site Internet sécurisé ou le virement d'une somme d'argent sont cryptés. En l'absence de protection des données sensibles, la confiance dans le système financier mondial s'effondrerait. Ou des forces obscures pourraient accéder à la gestion des infrastructures nationales critiques sans la protection offerte par le cryptage. Un cauchemar. Il en va de même de la propriété intellectuelle et des secrets de nombreuses entreprises. Dès à présent, des criminels et des États voyous volent et enregistrent des données cryptées pour les décrypter avec un ordinateur quantique dans quelques années. On qualifie aussi cette stratégie de «harvest now, decrypt later». Il est donc grand temps de passer à un meilleur procédé de cryptage. Des chercheurs du monde entier travaillent déjà sur un «post-quantum» ou des méthodes de cryptage «à résistance quantique» qui résistent à la puissance de calcul des ordinateurs quantiques.

Un maigre réconfort

Selon les experts, il faudra encore une dizaine d'années avant la révolution quantique et nous avons donc encore un peu de temps, ce qui constitue une maigre consolation. Les calculs utiles réalisés par les ordinateurs quantiques requièrent une quantité gigantesque de qubits. Le plus grand ordinateur quantique actuel d'Atom Computing en compte déjà 1180. Selon Craig Gidney, scientifique chez Google, le décodage d'un cryptage actuel nécessiterait 20 millions de qubits. A cela s'ajoute le fait que les bits quantiques sont sujets aux erreurs. Les

Raiffeisen Suisse
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Le point de vue du chef économiste de Raiffeisen

Une once de réconfort

vibrations thermiques, les rayons cosmiques, les interférences électromagnétiques ou toute autre perturbation peuvent engendrer une erreur par centaine voire dizaine de milliers d'opérations. Un tel taux d'erreur ne permet pas de résoudre des tâches complexes qui nécessitent des millions d'étapes de calcul. Mais dans ce domaine aussi, l'évolution est très rapide. Des chercheurs de Google ont dernièrement réussi à abaisser fortement le taux d'erreur en regroupant en damier plusieurs bits quantiques en un bit quantique logique, ce qui permet d'identifier et de corriger les erreurs.

L'évolution de la technologique des ordinateurs quantiques est passionnante à suivre. Elle recèle un potentiel économique considérable. Des applications sont par exemple envisageables dans le domaine de la gestion des risques, de l'optimisation des processus logistiques, de la découverte de nouveaux matériaux et de processus chimiques qui permettent d'espérer de nouveaux médicaments révolutionnaires et donc l'éradication de certaines maladies. Mais les ordinateurs quantiques nous rappellent aussi combien notre monde est devenu fragile. En juillet, nous avons par exemple connu la plus grosse défaillance informatique de tous les temps, imputable à la société Crowdstrike qui développe des logiciels de sécurité. Une mise à jour erronée a paralysé des aéroports, des hôpitaux et des entreprises de médias dans le monde entier. Dans le monde réel, des serrures mécaniques protègent les biens précieux. Une serrure peut être forcée pour peu qu'on déploie les efforts nécessaires, mais pas toutes les serrures en même temps. Mais l'arrivée des ordinateurs quantiques pourrait forcer d'un coup les serrures numériques utilisées depuis des décennies, si nous ne les remplaçons pas au plus vite. Peut-être est-ce aussi l'une des raisons pour lesquelles le prix de l'or ne cesse de voler de record en record.

Fredy Hasenmaile,
chef économiste de Raiffeisen

RAIFFEISEN

Raiffeisen Suisse
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Le point de vue du chef économiste de Raiffeisen

Une once de réconfort