Les experts s'inquiètent d'une future «apocalypse quantique»

Oubliez la sécurité telle que vous la connaissez.

Repéré par Thomas Burgel sur BBC

28/01/2022 à 6h54

L'informatique quantique, nouveau nerf de la guerre? Chaque jour, à la faveur des sommes colossales engagées par les firmes privées comme Google et IBM ou des gouvernements désireux de prendre l'ascendant dans le domaine, les machines quantiques progressent.

En théorie, ces machines d'un nouveau type devraient, à terme, offrir à celles et ceux qui les maîtrisent une formidable puissance de calcul, une capacité inédite à résoudre des problèmes trop complexes pour l'informatique actuelle.

Bien que ces annonces puissent être sujettes à caution, la technologie avance à grands pas; Google et IBM ont déjà affirmé avoir atteint cette *«suprématie quantique»* signalant le basculement dans une nouvelle ère.

Et si la science peut se réjouir de pouvoir, bientôt, accéder à cette puissance de calcul phénoménale pour s'ouvrir de nouveaux horizons, certains experts s'inquiètent de ce qu'ils appellent *«l'apocalypse quantique»*.

À lire aussi

Depuis la Voie lactée, un mystérieux objet envoie un signal à la Terre toutes les 18,18 minutes

Car si la puissance quantique peut permettre à la médecine ou à la physique –pour ne prendre que ces deux exemples de grands bonds en avant–, elle pourrait également servir à de bien plus noirs desseins. Parmi ceux-ci, rendre la cybersécurité sous sa forme actuelle, et tous vos mots de passe a priori incassables, complètement caducs.

«Les ordinateurs quantiques vont rendre inutiles la plupart des méthodes existantes de chiffrement. Ils sont une menace pour notre mode de vie», avance Ilyas Khan de Quantinuum à la BBC. Son confrère Harri Owen, de PostQuantum, ne dit pas autre chose.

«Ce que nous faisons aujourd'hui sur internet, des achats en ligne aux transactions bancaires, est chiffré, explique-t-il. *Mais une fois qu'un ordinateur quantique fonctionnel sera capable de casser ces clés… cela peut créer la possibilité pour quiconque l'ayant développé de vider des comptes en banque, de faire complètement s'effondrer des systèmes de défense nationale –des portefeuilles en bitcoins seront vidés.»*

Demain, c'est déjà aujourd'hui

Or, comme l'écrivait il y a peu la MIT Technology Review, il est fort possible sinon probable que des hackers soient aujourd'hui en train de récolter, partout où ils le peuvent, des montagnes de données chiffrées.

Celles-ci leurs sont encore inaccessibles, mais il accumulent ces trésors qui ne demandent qu'à être ouverts en attendant de pouvoir en briser les codes quand le quantique le leur permettra, peut-être plus tôt qu'on ne le pense, et d'en tirer les éventuels fruits, au risque de faire s'effondrer l'ensemble de l'édifice.

Et si une récente étude centrée sur le bitcoin affirme que la prétendue incassable cryptomonnaie ne pourrait être cassée que par des ordinateurs quantiques dix millions de fois plus puissants que ceux qui existent aujourd'hui, l'inquiétude est réelle, notamment au niveau des gouvernements.

À lire aussi

Plus fort que les pénuries, il fabrique ses propres processeurs dans son sous-sol

Comme l'explique la BBC, Quantinuum comme PostQuantum, dont des cadres alarmistes ont été cités plus haut, sont deux des firmes travaillant activement sur *«l'ère post-quantique»* et la nouvelle sécurisation qu'elle requiert –bien qu'elle soit incontestable, il est à noter qu'agiter la menace fait partie de leur business plan.

Les géants de la tech ne sont pas en reste, et les gouvernements prennent déjà des mesures pour protéger leurs secrets. Selon le site britannique, les documents classifiés par le gouvernement de Sa Majesté sont déjà adaptés à la nouvelle menace. Tout ceci coûtera sans doute des fortunes, mais ne rien faire en fera perdre des plus grandes encore.

La kotiidienne

Une sélection personnalisée des articles de korii. Tous les matins dans votre boîte mail.

Votre e-mail

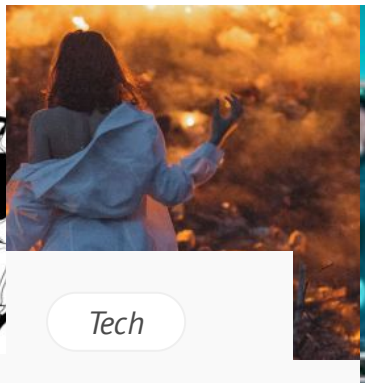
S'abonner

Et Cætera

Les licornes auraient existé à l'époque des premiers humains

Et c'est la science qui l'affirme.

Thomas Messias -
28 janvier 2022

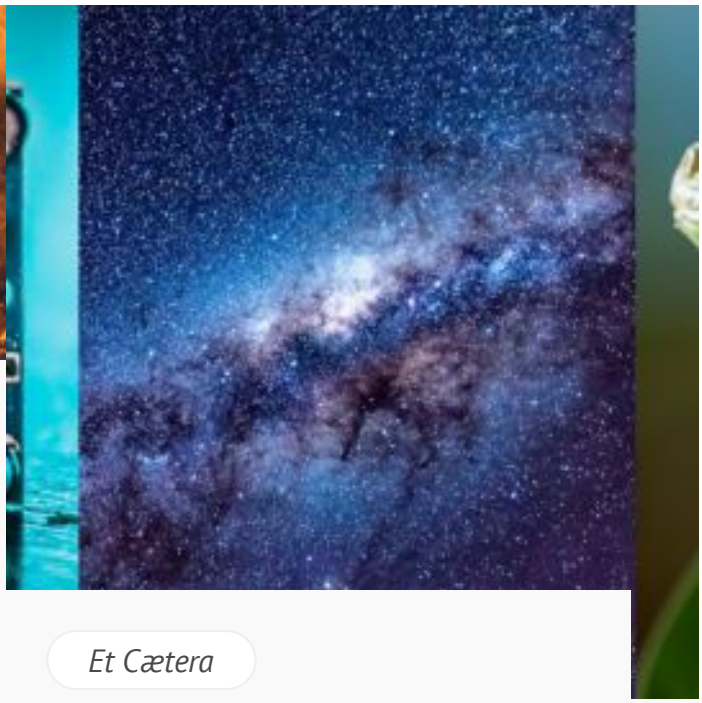


Tech

Les experts s'inquiètent d'une future «apocalypse quantique»

Oubliez la sécurité telle que vous la connaissez.

Thomas Burgel -
28 janvier 2022



Et Cætera

🌌 Un mystérieux signal toutes les 18 minutes 🦎 Une alerte à la pluie d'iguanes 💻 Des microprocesseurs DIY, hier sur korii.

Quatre articles pour comprendre le monde

Quatre articles pour comprendre le monde autrement.

korii.fr - *28 janvier 2022*

korii.

Slate

CONTACTS

QUI SOMMES-NOUS

MENTIONS LÉGALES

GESTION DES DONNÉES PERSONNELLES

La kotiidienne →