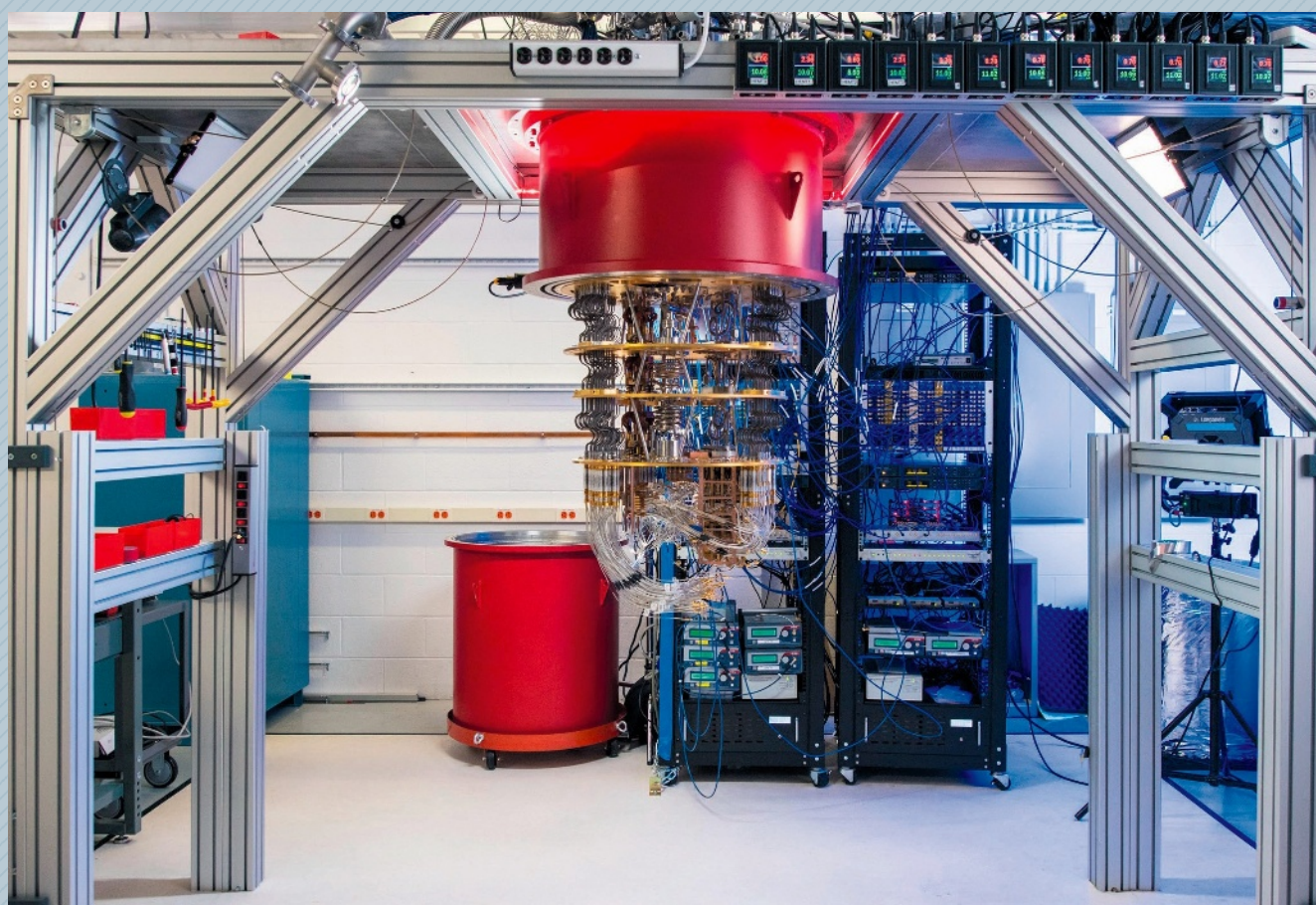




idée plus précise en tête lorsqu'ils parlent de suprématie quantique. Ils font la distinction entre les programmes exécutés en un temps polynomial «rapide» et en un temps exponentiel «lent». Les programmes rapides le restent, même lorsqu'on leur soumet un très grand nombre. Les programmes lents ralentissent exponentiellement à mesure que la taille des problèmes posés augmente.

Dans son étude, Google démontre que son ordinateur quantique de 53 qubits effectue un calcul spécialisé (appelé «échantillonnage de circuit aléatoire») en temps polynomial rapide. Or, pour l'heure, un ordinateur classique ne peut effectuer pareille tâche qu'en un temps exponentiel lent. Pour William Fefferman, de l'université de Chicago, ce constat est bien plus important que n'importe quel délai impliqué, qu'il s'agisse de deux jours et demi ou de 10 000 ans. «L'estimation du temps n'est pas très importante, précise-t-il. Je pense qu'IBM ne devrait pas invalider les déclarations principales de Google, en dehors de l'estimation de 10 000 ans.»

Ce qui compte, c'est que la machine de Google résout un problème de calcul d'une façon fondamentalement différente de celle dont un

ordinateur classique est capable. Cette différence signifie que, à chaque fois que son ordinateur quantique croît d'un simple qubit, un ordinateur classique aura besoin de voir sa taille doubler pour suivre le rythme. Lorsqu'un ordinateur quantique aura atteint les 70 qubits – probablement d'ici aux deux prochaines années – un supercalculateur classique aura besoin d'un espace équivalent à celui d'une ville pour l'égaliser.

ÉCHEC ET MAT

Scott Aaronson – empruntant l'analogie d'un ami – explique que la relation entre les ordinateurs quantiques et classiques, à la suite de l'annonce de Google, ressemble beaucoup à celle, dans les années 1990, entre le champion d'échecs Garry Kasparov et le supercalculateur Deep Blue... d'IBM. Le champion arrivait à suivre les premières versions qui allaient s'améliorant, mais il apparaissait clairement qu'il allait être inéluctablement dépassé par son adversaire algorithmique. IBM, désormais à la place de Garry Kasparov, «peut faire son baroud d'honneur durant l'ère de transition qui durera peut-être un an ou deux, explique Scott Aaronson. Mais, fondamentalement, il est mat.» ■

BIBLIOGRAPHIE

F. ARUTE ET AL., Quantum supremacy using a programmable superconducting processor, *Nature*, vol. 574, pp. 505-510, 2019.

E. PEDNAULT ET AL., Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits, 2019. <https://arxiv.org/abs/1910.09534>

L'ESSENTIEL

● Les ordinateurs quantiques communiqueront *via* un internet tout aussi quantique qui reste à inventer.

● Les premières pierres sont d'ores et déjà posées et l'on imagine de nombreuses applications que l'internet classique n'autorise pas.

● Ces réseaux quantiques reposeront également la question de la sécurité des transmissions.

● Garantir la confidentialité des communications quantiques impose de réfléchir à de nouveaux protocoles et à de nouvelles hypothèses sur lesquelles les fonder.

L'AUTRICE



NATALIE WOLCHOVER
est journaliste
à *Quanta Magazine*.

Inventer l'internet du futur

L'internet que nous connaissons depuis quarante ans est fondé sur des machines « classiques ». À quoi ressemblera celui qui reliera les ordinateurs quantiques ? Stephanie Wehner apporte quelques éléments de réponse.



Quanta
magazine

Cet article a d'abord été publié en anglais par *Quanta Magazine*, une publication en ligne indépendante soutenue par la Simons Foundation afin de favoriser la diffusion des sciences : <http://bit.ly/QM-Wehner>

C

e soir-là, des informaticiens de l'université de Californie, à Los Angeles, étaient au téléphone avec leurs homologues de l'Institut de recherche Stanford à Menlo Park, situé à quelque 560 kilomètres de là. La conversation était surréaliste se rappelle Leonard Kleinrock, chercheur en informatique à l'université de Californie. «Avez-vous bien reçu le L?» «Oui», a répondu l'autre équipe. «Vous avez reçu le O?» «Oui.» De même pour le G... et puis c'est le crash! Le serveur de l'Institut avait planté.

C'était le 29 octobre 1969. Les trois premières lettres du mot «LOGIN», tel a été le premier message transmis par l'Arpanet, le précurseur d'une révolution, ce que nous appelons aujourd'hui internet.

TROP DE CRÉATIVITÉ NUIT

La capacité des réseaux à transmettre des données, ainsi que leur tendance à planter, sinon à se comporter de façon imprévue, a toujours fasciné Stephanie Wehner. «Dans un ordinateur, tout se passe bien et reste ordonné», explique cette physicienne et informaticienne à l'université de technologie de Delft, aux Pays-Bas. «Dans un réseau, en revanche, de nombreux imprévus surviennent parfois.» Et c'est vrai pour deux raisons. D'abord, quand les programmes sur les ordinateurs connectés interfèrent, ce qui engendre des effets surprenants. Et ensuite, lorsque la créativité des utilisateurs de réseaux déborde. Au départ, «les gens pensaient que nous utiliserions internet pour