

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.

C

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



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>

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.



envoyer des fichiers un peu partout», remarque la physicienne.

Stephanie Wehner s'est connectée pour la première fois en ligne en 1992, quelques années avant que cela ne devienne largement accessible. À l'époque adolescente en Allemagne, elle s'y connaissait déjà en programmation et est vite devenue une pirate informatique sur l'internet naissant. À 20 ans, elle a obtenu un poste de «corsaire», c'est-à-dire de pirate pour le bien: sa tâche consistait à détecter les vulnérabilités du réseau pour un fournisseur d'accès à internet. Puis elle s'est lassée et a cherché à comprendre plus en profondeur les réseaux et les systèmes de transmission d'information.

Aujourd'hui, Stephanie Wehner fait partie des meneurs du mouvement visant à créer une toute nouvelle forme d'internet. Elle travaille à la conception d'un «internet quantique», un réseau qui transmettrait – au lieu des bits classiques ayant soit une valeur de 0, soit de 1 – des bits quantiques dans lesquels les deux

possibilités, 0 et 1, coexistent. Ces «qubits» pourraient être faits de photons qui sont une combinaison de deux différentes polarisations. La capacité d'envoyer des qubits d'un endroit à un autre *via* des câbles de fibres optiques ne bouleversera peut-être pas la société aussi profondément que ne l'a fait l'internet classique, mais elle pourrait révolutionner de nombreux aspects de la science et de la culture, de la sécurité à l'informatique, en passant par l'astronomie.

UN ARPANET QUANTIQUE

Stephanie Wehner coordonne la *Quantum Internet Alliance*, une initiative de l'Union européenne pour élaborer un réseau de transmission d'information quantique à travers le continent. Dans un article paru dans la revue *Science* en octobre 2018, elle et deux collègues ont dévoilé leur plan pour la création d'un internet quantique en six étapes, chacune d'elle devant se traduire par de nouveaux algorithmes et applications.

Stephanie Wehner, à l'université de technologie de Delft, aux Pays-Bas, où elle pose les premières pierres d'un futur internet quantique.

> La première étape est en cours, elle consiste en la construction d'un réseau quantique de démonstration qui connectera quatre villes aux Pays-Bas, une sorte d'analogie quantique de l'Arpanet. Tracy Northup, de l'université d'Innsbruck et membre de la *Quantum Internet Alliance* loue «l'ampleur de la vision de Stephanie et son engagement pour construire le genre de structure nécessaire à la réalisation d'un tel projet.»

Après le piratage, Stephanie Wehner est allée à l'université pour étudier l'informatique et la physique. À Leyde, elle a entendu le théoricien de l'information quantique John Preskill donner une conférence, durant laquelle il décrivait les avantages des bits quantiques pour communiquer. Quelques années plus tard, après avoir son doctorat, elle a

abandonné les bits classiques et rejoint le groupe de John Preskill à l'institut de technologie de Californie (Caltech), aux États-Unis, pour un postdoctorat.

Là, en plus d'avoir démontré plusieurs théorèmes notables sur l'information quantique, la cryptographie quantique et la nature de la mécanique quantique elle-même, Stephanie Wehner s'est naturellement imposée comme une «meneuse naturelle», raconte John Preskill; elle «était souvent le lien qui unissait les gens». En 2014, après avoir occupé un poste de professeure à Singapour, elle a déménagé à Delft, où elle a commencé à collaborer avec des expérimentateurs pour poser les fondations de l'internet quantique.

Afin d'en savoir plus, nous avons rencontré Stephanie Wehner en août 2019.

« Nous travaillons à un réseau quantique à travers toute l'Europe »

L'internet quantique est un réseau de transmission de qubits entre deux lieux distants. Pourquoi en a-t-on besoin ?

Stephanie Wehner : L'idée n'est pas de remplacer l'internet que nous utilisons tous aujourd'hui, mais plutôt d'y ajouter des fonctionnalités nouvelles et spéciales. Les réseaux quantiques ont toutes sortes d'applications encore à imaginer, mais nous en connaissons déjà un certain nombre. Bien sûr, la plus célèbre est la communication sécurisée: le fait que l'on puisse utiliser la communication quantique pour distribuer des clés quantiques de cryptographie, garantissant la sécurité, même si l'attaquant est équipé d'un ordinateur quantique. Or une telle machine pourrait vaincre de nombreux protocoles de sécurité existant aujourd'hui.

Qu'est-ce qui rend ces clés quantiques si sûres ?

Stephanie Wehner : Une bonne manière de comprendre ce que l'internet quantique peut faire est de penser à «l'intrication quantique»

(voir *Pas d'échappatoire pour l'intrication*, par R. Hanson, page 26), une propriété qui unit deux bits quantiques. La première propriété de l'intrication est sa «coordination maximale»: si j'avais un bit quantique ici, à Delft, et un autre à New York, j'utiliserais l'internet quantique pour les intriquer. Dès lors, une mesure de mon qubit ici et celle du qubit de New York donneraient toujours le même résultat, alors même qu'il n'était pas prédéterminé. Donc, intuitivement, grâce à cette première propriété de l'intrication quantique, l'internet quantique serait très utile pour des tâches nécessitant une coordination à distance.

On peut alors se demander: «Ne serait-ce pas génial de partager cette intrication avec des centaines de personnes?» Peut-être, mais c'est impossible, car la seconde propriété de l'intrication est son caractère intrinsèquement privé. Si mon qubit d'ici est intriqué avec le vôtre à New York, alors nous savons que rien d'autre ne peut partager cette intrication. C'est pour cela que la communication quantique est si pratique pour les problèmes requérant un certain niveau de sécurité.