RFC 9340 : Architectural Principles for a Quantum Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 avril 2024

Date de publication du RFC : Mars 2023

https://www.bortzmeyer.org/9340.html

Voici un RFC assez futuriste qui explore à quoi pourrait ressembler un futur « Internet » quantique. Je divulgâche tout de suite : ce ne sera pas de si tôt.

Quelques avertissements s'imposent d'abord. Avant tout, rappelez-vous que la quantique produit des résultats qui sont parfaitement cohérents théoriquement et très bien vérifiés expérimentalement mais qui sont hautement non-intuitifs. Avant d'aborder le monde merveilleux de la quantique, n'oubliez pas d'oublier tout ce que vous croyez savoir sur le monde physique. Et ne comptez pas trop sur moi comme guide, on sort nettement ici de mon domaine de compétence. Ensuite, « quantique » est un terme à très forte charge marketing (moins que « IA » mais davantage que « métavers » ou même « blockchain », qui semblent bien passés de mode). Il faut donc être prudent chaque fois qu'un commercial ou un éditorialiste va dire que « c'est quantique » ou que « la quantique va bouleverser tel ou tel domaine ». Enfin, il y a loin de la coupe aux lèvres : de même qu'on n'a pas encore d'ordinateur quantique utile, on n'a pas encore de réseau quantique. Le RFC est à juste titre prudent, pointant les différents obstacles qui restent sur le chemin de l'Internet quantique.

Bon, ces précautions étant posées, qu'est-ce qu'un réseau quantique et pourquoi y consacrer un RFC ? La section 1 du RFC le résume : un réseau quantique est un réseau qui ferait communiquer des dispositifs quantiques pour faire des choses inimaginables avec un réseau classique. Il s'appuierait sur des propriétés spécifiques au monde quantique, notamment l'intrication, propriétés qui n'ont pas d'équivalent dans le monde classique. Attention, et le RFC insiste bien là-dessus, personne n'envisage de remplacer l'Internet classique par un Internet quantique (de la même façon que les futurs ordinateurs quantiques, étant loin d'être généralistes, ne remplaceront pas les ordinateurs classiques). Au contraire, le scénario envisagé est celui d'un réseau hybride, partiellement quantique. (Une lecture recommandée par le RFC est « "*The quantum internet*" <https://www.nature.com/articles/nature07127> ».)

Un exemple typique qui ne serait pas possible avec un réseau classique est celui de la distribution quantique de clés (parfois appelée du terme erroné de « cryptographie quantique »), dont l'utilité pratique est douteuse <https://www.bortzmeyer.org/communication-quantique.html> mais

qui est assez spectaculaire et, contrairement à d'autres applications, est assez avancée techniquement. D'autres applications sont envisageables à plus long terme. C'est le cas par exemple du "*blind quantum computation*", qui n'a pas encore d'article Wikipédia mais est expliqué dans cet article <https://www.nature.com/articles/s41534-017-0025-3>.

En laboratoire, beaucoup de résultats ont été obtenus. Les chercheurs et chercheuses ont déjà mis au point bien des dispositifs physiques étonnants. Mais à l'échelle du réseau, il n'y a pas encore eu beaucoup de travaux. Le RFC compare cette situation à celle d'un réseau classique où on aurait des fibres optiques et des lasers pour les illuminer mais aucun protocole de transport, aucun mécanisme de routage, encore moins de moyens de gérer le réseau. Développer une application pour un réseau quantique revient à toucher directement au matériel, comme, pour un réseau classique, s'il fallait que chaque application parle aux interfaces physiques, sans avoir d'interface de plus haut niveau comme les prises.

La section 2 du RFC est un rappel sur la quantique. Comme dit plus haut, c'est un domaine riche et complexe, où l'intuition ordinaire ne sert pas à grand'chose. Donc, lire ce rappel est une bonne idée mais n'espérez pas tout comprendre si vous n'êtes pas spécialiste de la question. Cette section est conçue pour des gens qui ne connaissent rien à la physique quantique, elle recommande, pour aller plus loin, le livre de Sutor "*Dancing with Qubits*" <https://www.packtpub.com/product/dancing-with-qubits/9781838827366> ou bien celui de Nielsen et Chuang, "*Quantum Computation and Quantum Information*" <http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf>.

Le rappel commence avec la notion d'état quantique. Vous avez sans doute déjà entendu dire qu'un bit classique peut prendre deux valeurs, 0 ou 1, alors que son équivalent quantique, le qubit, a un état qui est une superposition de valeurs possibles, avec des probabilités. Lorsqu'on le mesure, on trouve un 0 ou un 1. (Oui, comme le célèbre chat qui est à la fois vivant et mort.) Attention, ces non-certitudes ne sont pas la conséquence d'un manque d'information mais sont une propriété fondamentale du monde quantique (Alain Aspect a eu un prix Nobel pour avoir prouvé cela). Notez que les versions HTML ou PDF du RFC sont recommandées ici, car il y a quelques équations. Comme un qubit est dans un état qui superpose les deux valeurs possibles, les opérations quantiques agissent sur tout l'état, par exemple l'équivalent quantique d'une porte NOT va inverser les probabilités du 0 et du 1 mais pas transformer un 0 en 1.

Le terme « qubit » (et cette distinction revient souvent dans le RFC) peut désigner aussi bien le concept abstrait que le truc physique qui va le mettre en œuvre (il existe plusieurs techniques pour fabriquer un engin qui gérera des qubits).

On peut ensuite assembler des qubits et, très vite, le nombre de possibilités croît. Mais l'intérêt de mettre des qubits ensemble est qu'on peut les intriquer et ce concept est au cœur de beaucoup de solutions quantiques, notamment du réseau quantique. Une fois intriqués, les deux qubits verront leur sort lié. Une mesure sur l'un affectera l'autre. (Rappel : la quantique n'est pas intuitive et l'intrication n'a pas d'équivalent dans le monde non-quantique, celui sur lequel a été bâtie notre intuition.) La mesure, comme toujours en quantique, est « destructive » au sens où elle ramène à un système classique (le qubit vaut 0 **ou** 1 quand on le mesure, pas un mélange des deux, et le chat est vivant **ou** mort quand on ouvre la boite).

Cette intrication est au cœur des réseaux quantiques (section 3 du RFC). Tous les projets de réseaux quantiques utilisent cette propriété (qui, rappelons-le, n'a pas d'équivalent non-quantique). L'intrication permet de corréler deux nœuds du réseau. Par exemple, pour se mettre d'accord sur une valeur, deux machines n'ont pas besoin de faire tourner des algorithmes de consensus, elles peuvent utiliser deux qubits intriqués, chacune en gardant un. Quand une machine lira la valeur de son qubit, elle sera certaine

de la valeur lue par l'autre. Et l'intrication ne peut pas être partagée : un tiers ne peut pas s'intriquer avec une intrication existante, ce qui peut avoir des applications en sécurité.

Un réseau quantique est donc défini par notre RFC comme un ensemble de nœuds qui peuvent échanger des qubits intriqués.

Bon, tout ça, c'est très joli, mais comment on le réalise, ce réseau quantique ? La section 4 se penche sur les défis :

— Comme toute mesure détruit le caractère quantique du qubit et le transforme en un bit ordinaire, des opérations banales dans le monde classique, comme la copie d'un bit, deviennent non triviales.
— Et copier un qubit sans le mesurer ? On ne peut pas (c'est le théorème d'impossibilité du clonage).
— Tout cela rend très difficile la correction d'erreurs. Un réseau réel, reposant sur des objets physiques, va forcément voir des erreurs (un rayon cosmique passe et paf, un 0 est transformé en 1) et de nombreuses techniques existent pour gérer ce problème dans le monde classique. Mais elles ne peuvent en général pas s'appliquer dans le monde quantique, qui va donc avoir un problème de fidélité : la fidélité est la conformité à ce qu'on souhaitait (elle va de 0 à 1), et les applications doivent en tenir compte.

Distribuer sur le réseau des qubits quelconques n'est pas forcément facile, donc le RFC suggère de plutôt distribuer des paires de Bell. On peut alors plus facilement (tout est relatif) faire de la téléportation, c'est-à-dire « transporter » un qubit d'un point à un autre. Ce n'est pas une violation du théorème d'impossibilité du clonage puisque le qubit n'est pas copié (il disparait de son point de départ). Notez que le terme de « téléportation » est surtout marketing : vous ne pourrez pas déplacer votre chat ou vous-même de cette façon.

Dernier problème, amplifier le signal (sans le copier !) pour tenir compte de sa dégradation avec la distance. Il existe une astuce, l'échange d'intrication, que je ne vais pas essayer d'expliquer, mais qui permet des réseaux quantiques sur des distances importantes.

Revenons à la correction d'erreurs. Les réseaux quantiques ne sont pas complètement démunis, et ont des solutions possibles, comme les codes quantiques.

OK, on a vu que le monde quantique était très spécial. Donc, le réseau quantique va être bizarre aussi, aux yeux de quelqu'un qui a l'habitude des réseaux classiques (section 5 du RFC). Par exemple, il fera face à ces problèmes :

— C'est bien joli, les paires de Bell, mais ce n'est pas l'équivalent d'un paquet portant une charge utile. Il n'y a pas l'équivalent de l'en-tête du paquet, et le réseau quantique va donc devoir utiliser un réseau classique pour l'information de contrôle. On ne fera pas un réseau purement quantique.
— Toute action sur des qubits intriqués doit être coordonnée entre les nœuds puisque l'action sur un qubit va déterminer le résultat d'une action sur les autres (il faut donc que chaque nœud sache contacter les autres).

Répétons-le, chaque nœud du réseau quantique devra également être relié à un réseau classique. Le réseau sera donc complexe et son administration pas évidente.

Une fois qu'on a accepté cela, le réseau classique pourra s'occuper d'opérations comme la construction des tables de routage, pour laquelle les algorithmes et méthodes classiques semblent suffire. On n'aura donc peut-être qu'un seul plan de contrôle (le classique) mais deux plans de données, le classique et le quantique.

Que faut-il construire comme machines pour le plan de données quantique ? D'abord, des répéteurs quantiques qui vont pouvoir créer les intrications, les échanger et contrôler la fidélité. Ensuite :

— Des routeurs quantiques, qui, en plus des fonctions ci-dessus, participeront au routage.

— Les nœuds ordinaires, des répéteurs qui ne participent pas au routage.
— Les nœuds terminaux <https://www.bortzmeyer.org/terminal-host.html>, qui pourront émettre et recevoir des qubits mais pas faire d'échange d'intrication. C'est là que tourneront les applications.

Facile, me direz-vous ? Non, construire ces machines va nécessiter de s'attaquer à quelques problèmes physiques :

— Stocker un qubit est un défi ! Le monde classique n'aime pas les objets quantiques et essaie régulièrement de les rappeler à ses lois. Les bruits divers de l'environnement font rapidement perdre aux qubits leurs propriétés quantiques. (C'est d'ailleurs pour cela que vous ne rencontrez pas de chats de Schr[Caractère Unicode non montré [1]]dinger dans la vraie vie.) Cela se nomme la décohérence et c'est l'un des principaux obstacles sur la route des réseaux quantiques (ou des calculateurs quantiques). Les durées de vie qu'on atteint étaient, lors de la rédaction du RFC, de l'ordre de la seconde (ou de la minute si on n'est pas connecté au réseau, source de perturbations).
— La capacité <https://www.bortzmeyer.org/capacite.html> des liens quantiques est un autre problème. Générer des qubits intriqués prend du temps. Quand on en fabrique dix par seconde, on est contents. Bien sûr, la technique progresse sans cesse (pas mal des références du RFC sont un peu datées, car il a mis du temps à sortir) mais pas assez.
— On l'a dit, on peut réaliser des qubits intriqués par différentes méthodes physiques, avec des performances différentes selon la métrique utilisée. Mais ces méthodes ne communiquent pas entre elles, ce qui veut dire que tous les nœuds du réseau doivent utiliser la même.

Si vous n'êtes pas découragé·e (mais il ne faut pas l'être : même si les difficultés sont colossales, le chemin est rigolo), il faut maintenant, en supposant qu'on aura les composants de base d'un réseau, les assembler. (À moins que le choix décrit dans le RFC des paires de Bell et de l'échange d'intrication ne soit remis en cause par les futurs progrès…) La section 6 se penche sur la question. Elle démarre par un bel excès d'optimisme, en expliquant que, contrairement à ce qui s'est passé avec l'Internet classique, on a de l'expérience sur la construction de réseau, et qu'on pourra donc ne pas faire d'erreur comme la taille trop réduite des adresses IPv4.

Des services essentiels pour un réseau réel seront difficiles à assurer sur un réseau quantique. Par exemple, l'impossibilité du clonage interdira d'utiliser un logiciel équivalent à tcpdump (remarquez, pour la sécurité, c'est un plus). Le RFC liste les principes de base d'un réseau quantique :

— Le service de base sera l'intrication.
— La fidélité est aussi un service (contrairement au réseau classique où on peut espérer une fidélité parfaite).
— Le temps va être un facteur crucial, compte tenu de la décohérence. Pas question de faire patienter des qubits trop longtemps dans une file d'attente, par exemple.
— Il faudra être flexible, notamment parce que le matériel va continuer à évoluer.

Et le RFC se termine par une exploration d'une architecture de réseau quantique possible, inspirée de MPLS. Dans ce réseau (pour l'instant) imaginaire, tout fonctionne en mode connecté (comme MPLS) : on doit d'abord créer un circuit virtuel (car créer les paires de Bell et les utiliser va nécessiter de la coordination, donc il vaut mieux établir d'abord une connexion). Ce QVC ("*Quantum Virtual Circuit*") a des caractéristiques comme une qualité de service choisie, qui se décline en, par exemple, une capacité <https://www.bortzmeyer.org/capacite.html> mesurée en nombre de paires de Bell par seconde et bien sûr une fidélité (toutes les applications des réseaux quantiques n'ont pas les mêmes exigences en terme de fidélité). La signalisation peut être décentralisée (comme avec RSVP) ou centralisée (comme avec OpenFlow). Comme vous le verrez en lisant cette conclusion du RFC, les détails sont encore approximatifs.

Ce RFC a mis longtemps à être écrit, vous pouvez trouver une description ancienne du projet sur le blog de l'IETF <https://www.ietf.org/blog/quantum-internet/>. Notez que l'écriture de ce RFC a été en partie financée par la Quantum Internet Alliance <https://quantuminternetalliance.org/> européenne.

N'hésitez pas à vous plonger dans la bibliographie très détaillée de ce RFC, vous y trouverez beaucoup de lectures passionnantes. Il y a même déjà des livres entiers sur les réseaux quantiques comme celui de Van Meter <https://onlinelibrary.wiley.com/doi/book/10.1002/9781118648919>.

1. Car trop difficile à faire afficher par LaTeX