Annexe 5 – Les différences fondamentales entre les réseaux classiques et quantiques

La polarisation et la superposition : La différence évidente entre les bits et les qubits est que, à cause de leurs natures, ils ne peuvent pas encoder le même nombre d'informations. En effet, les bits, qui sont simplement formés par la présence ou l'absence d'un courant électrique, vont pouvoir encoder deux valeurs, à savoir 0 ou 1. Un bit aura donc une valeur possible. Dans le monde quantique, un qubit est formé grâce à une particule. Celle-ci a des propriétés quantiques très utiles comme la polarisation et la superposition. La polarisation, qui donne un « pôle » à une particule, permet d'ajouter un discriminant aux qubits, sans avoir à créer de protocoles complexes, et ainsi former des trames plus rapidement. En effet, il sera possible de coder des fonctions qui permettent de choisir tel ou tel qubit en fonction de sa polarisation, et ainsi faire du tri dans des paquets de qubits pour former une trame spécifique. Enfin, la superposition permet à un qubit d'encoder à lui tout seul deux valeurs possibles. Ce constat n'est pas très pertinent en présence d'un seul qubit seulement, mais à partir de deux qubits, nous pouvons percevoir qu'il est possible de transporter plus d'informations dans un réseau quantique que dans un classique. En prenant l'exemple de 2 bits/qubits donnés :

Pour les réseaux classiques : bit(0) et bit(1). Ces derniers peuvent encoder deux messages différents : 01 ou 10. Soit, n bits encodent n informations.

Pour les réseaux quantiques : qubit(0-1) et qubit(0-1) étant en état de superposition, ils peuvent encoder quatre messages différents : 00, 01, 10, 11. Soit, n qubits encodent 2^n informations.

L'intrication et la téléportation : Très simplement, un qubit est une particule. Une particule peut être liée à une autre particule. Si une de ces particules se fixe sur une valeur en bit, elle fixera automatiquement la valeur de l'autre particule, pour être son égale ou son contraire, en fonction de ce que l'expérimentateur décide. Après avoir lié, donc intriqué, ces particules entre elle, il est possible d'en envoyer une sur un ordinateur, et l'autre sur un autre ordinateur. Malgré cette distance qui les sépare, fixer la valeur d'une des deux particules fixera également la valeur de l'autre particule. C'est ce qu'on appelle la téléportation quantique. Ainsi, nous pouvons imaginer construire des trames entières de qubits intriqués, à envoyer à deux hôtes différents, dont nous fixerons les valeurs pour former des trames clientes et serveurs, en fonction du destinataire sur lequel cette trame arrive. La création d'une trame A sur un hôte donné, créera instantanément, peu importe la distance, une trame B sur un second hôte. Des trames IP entières pourraient donc être « téléportées ».

Le principe de non-clonage : Dans les réseaux quantiques, les qubits étant des particules, la moindre interaction avec ces derniers vont les faire se « fixer », à la fois dans leur état et dans leur position, puis s'effondrer. Cela signifie qu'à la première mesure d'un qubit, celui-ci est détruit. L'observateur obtiendra une valeur ou plusieurs valeurs sous forme de bit, mais n'aura pas l'occasion de pouvoir manipuler plus longtemps le qubit. Cette particularité permet aux qubits d'être impossible à dupliquer, ou cloner, tant leur existence est éphémère. C'est d'ailleurs cette propriété qui permet de rendre l'attaque Man in the Middle obsolète dans de tels réseaux. Sur un réseau classique, le moindre bit peut être intercepté, dupliqué, et renvoyé

sur le canal par un tier malveillant. Ainsi, des trames IP entières peuvent être reforgées, ce qui n'est pas le cas dans les canaux quantiques.

Au niveau de la stabilité du réseau : La fragilité des qubits apporte ses avantages en termes de sécurité, mais surtout ses inconvénients pour la stabilité du réseau. En effet, à cause du phénomène de décohérence, les qubits vont se désagréger très rapidement au fur et à mesure de leur voyage dans le canal quantique. Ainsi, une quantité importante de qubits va être perdue proportionnellement à la longueur du réseau. Dans les réseaux classiques, les perturbations sont de plus en plus rares, surtout sur de courtes distances, et les communications sont très stables. Pour un canal quantique, on parle d'une distance maximale de survie de qubit à environ 10 kilomètres. Cette situation apporte la nécessité de mettre en place un matériel très particulier, non utilisé dans les réseaux classiques, à savoir les répéteurs quantiques. Ces derniers, grâce à leur capacité de calcul exceptionnelle, vont être capable de mettre en mémoire les états des particules qu'ils reçoivent, et de les regénérer entièrement. Il ne s'agit pas d'un simple clonage, qui n'est pas possible pour un qubit, mais plutôt une analyse très poussée afin de recréer de zéro un qubit similaire. Ainsi, il est nécessaire, à intervalle régulière, de capter tout le trafic quantique, le mesurer et le recréer entièrement, en faisant de la correction d'erreur au passage, pour l'aider à poursuivre son voyage. C'est pourquoi la mise en place de réseaux quantiques est actuellement très laborieuse et surtout coûteuse.

Conclusion : D'après toutes nos recherches, nous avons pu construire le tableau suivant en début de projet :

Eléments de comparaison	Réseaux classiques	Réseaux quantiques
Puissance de calcul	*n bits peuvent encoder n informations* *Exemple pour 2 bits : 0 et 1. Résultats possibles : 01 ou 10.* *Potentiel de calcul linéaire.*	*n qubits peuvent encoder 2^n informations* *Exemple pour 2 bits : (0 ou 1) et (0 ou 1), car superposition. Résultats possible : 00, 01, 10, 11.* *Potentiel de calcul exponentiel.*
Sensibilité aux perturbations	*Si ce n'est des coupures d'électricité ou des interférences électromagnétiques, il y a peu de perturbations possibles. Les bits sont stables.*	*Les qubits sont des particules qui voient leur état modifié au contact des autres particules. Ils sont donc très instables.*
Distance supportée	*Plusieurs centaines de kilomètres.*	*Quelques dizaines de mètres.*
Application actuelle	*Transmettre de l'information en masse, à de nombreux hôtes, sur de longues distances.*	*Générer des clés cryptographiques complexes entre deux machines très proches.*