Rendu du 08/05/2021 pour le Hackathon à 18h

Elaboration de la stratégie et de la solution

Divers intérêts pour les utilisateurs de la Blockchain quantique et ceux pour tous les niveaux de la structure, que ce soit pour les institutionnels tel que les banques comme pour les plus petits acteurs du marché.

- L'intérêt pour les institutions, peut se traduire par une réduction globale des coûts de gestion notamment au niveau des transactions, de leurs vérifications ainsi que de tout le processus d'assurance et de litige en cas de fraude ou de vol.

- Cette solution engendrerait une suppression d'intermédiaire conséquente, puisque toute l'administration serait réalisée par la blockchain en elle-même, et donc par tous ces utilisateurs.

- Les intérêts pour le consommateur n'en serait que renforcé par la même occasion, car en diminuant les frais de gestion dues aux transactions, pourront être répercutés sur les frais à payer pour les utilisateurs de cette structure, rendant à la fois cette solution plus attrayante pour les utilisateurs car les frais serait réduit comparés à l'utilisation d'une solution existante actuellement.

- Une vitesse de transaction accrue, donc une impossibilité de surcharge du réseau qui pourraient aboutir à des saturations entrainant des frais plus élevés.

- De part cette vitesse de calcul alloué au Hashing de donnée, une sécurité sans faille naîtrait, en rendant la blockchain complètement inviolable, grâce à la puissance de calcul phénoménale qui y serait consacrée, empêchant ainsi tout acteur mal intentionné de recalculer une nouvelle blockchain avant l'émission d'un nouveau bloc de donnée qui serait validé par toute la communauté.

- Notre solution propose aussi un intérêt pour la planète en elle-même, car effectivement les solutions de minage existantes sont très consommatrices en électricité, or les solutions de calcul quantique ne consomment pas d'énergie. Ce qui inciterait d'autant plus les petits acteurs à rejoindre le mouvement et participer au bon calcul de la blockchain.

Technologie quantique utilisée :

- Nous utilisons l'algorithme de Grover afin de miner les blocs, ce qui comparé à une vitesse de calcul standard serait l'équivalent de passer de 2^256 à 2^128 pour résoudre

un calcul de bloc de donnée, on parle ici d'accélération quadratique. (L'exemple de calcul ce base sur le protocole actuel de la blockchain Bitcoin)

- Les clés privées envoyés sur le réseau seront chiffrées via RSA, qui pourrait facilement sauter au vu de la puissance de calcul quantique mise à disposition, soit l'algorithme de Shor. Pour résoudre ce problème, nous avons prévus d'intégrer une sécurité Quantum Proof, ce qui empêcherait les ordinateurs quantiques de venir ' hacker ' ces clés et donc léser un utilisateur. Ce protocole de sécurité serait valable jusqu'au moment où une connexion physique pourra être étendue à tous les ordinateurs quantiques présent dans la structure, et donc une implémentation du QKD (DB84) rendant les transactions sécurisées par la physique quantique elle-même.

Document réalisé le 08/05/2021 par l'équipe du Hackathon CryptoBabies composé de 4 membres :

- Bastien Listemann
- Victor Wauquier
- Adem Rahal
- Nathan Delaroche