Rendu du 09/05/2021 pour le Hackathon à 10h

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, ces derniers 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 puisque les frais seraient réduits comparé 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 de transactions plus élevés (Comme il a été constater sur la blockchain ETH lors du pic de revente des Tokens représentant les intérêts du Yielding sur une plateforme utilisant cette blockchain).
  De plus comme les transactions se ferait plus rapidement, il serait possible de baisser le prix de la transaction, afin de rendre la blockchain encore plus attrayante au grand public, tout en dégageant des bénéfices conséquents au vu du nombre de participants dans la structure.

- 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.

- Il est évidant qu'une blockchain totalement gouvernée et sécurisée par des ordinateurs quantiques, serait d'une sureté sans faille pour les capitaux des clients d'un établissement bancaire par exemple. Si l'on ajoute à cela la réduction des frais de transactions et une compétitivité attrayante, il est évident que la masse critique d'utilisateur sur la plateforme serait très rapidement atteinte.

- 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.

- De plus le Proof of Stack qui se développe beaucoup de nos jours, qui est en partie la validation des blocs de la chaine par consensus de détenteur de cryptomonnaie ciblée (exemple pour la blockchain Ethereum il faut détenir de l'ETH, bien que cette dernière soit entrain de transiter vers son état final de PoS).Ce développement est en partie lié aux coûts de calcul à effectuer, soit le prix de l'électricité, bien que cette technique de validation est moins solide que celle du Proof of Work comme la blockchain Bitcoin. C'est ici qu'avec notre solution, nous proposons une blockchain plus que solide grâce au Proof of Work généré par accélération quadratique, en enlevant quasiment complètement la donnée du prix de l'électricité de l'équation étant donné que faire tourner un moteur graphique Quantique est très peu couteux en électricité.

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.

Répondons par les points écris dans ce document aux questions posées dans le brief de présentation fait par Mr. Maxime HAVEZ.

1- Pourquoi puis-je l'utiliser ?

Vous pourrez utiliser cette solution afin de proposer à vos clients, une solution pour placer leurs capitaux d'une manière la plus sure possible tout en gagnant des bénéfices conséquents en cas de Holding, ou même de leur proposer des contrats exclusifs s'ils font partis des personnes qui ont envie d'allouer de la puissance de calcul à la Blockchain. De part les frais de gestion, litiges et fraudes ainsi que des transactions à faible coût et à grande vélocité, vos clients pourront bénéficier d'un service à moindre coût. Emettant une toute nouvelle Cryptomonnaie, au vu des réglementations qui seront passés d'ici le temps, le blanchiment d'argent sera quasiment impossible. De plus c'est un moyen de faire fonctionner une banque de manière inclusive, équilibrée et solidaire.

2- Quelles sont les limites ?

La principale limite que nous voyons au déploiement de ce projet de manière décentralisée, et par conséquent reposant sur une certaine confiance de la sécurité du marché, sera une limite impliquant le déploiement à grande échelle des ordinateurs quantiques, ou tout du moins leurs mises en location pour pouvoir participer à du cloud mining, et ainsi faire dégager un bénéfice non négligeable aussi à vos clients qui ne voudraient pas opter pour l'investissement dans une machine quantique.

Après pour ce qui est du côté quantique, les limites seront à très long terme, l'optimisation du réseau et donc l'implémentation du QKD (DB84) sur l'intégralité de l'infrastructure, afin de rendre les transactions sécurisées par la physique quantique, et pouvoir ce passer de l'algorithme de Shor.

3- Quelles sont les opportunités ?

Les opportunités de la solution sont multiples. Tout en sécurisant des revenus journaliers à vos clients, en leur proposant une sécurité maximale à moindre coût qu'ils soient de gestion ou transactionnel, dans un environnement décentralisé, et accessible à tous via le cloud mining. Le tout dans une solution écoresponsable et s'inscrivant dans la chartre de protection de la nature des plus grandes entreprises du monde. De plus un allègement vraiment conséquent de la fonction de contrôle de la banque que ce soit pour le blanchiment d'argent, ou encore les diverses fraudes et litiges, simplifiant la gestion du process et réduisant son fond de roulement global. Dégageant des fonds pour investir dans d'autre projets ou l'allouer afin de développer votre réseau de communication et déployer des personnes qualifier afin d'expliquer à vos clients de quoi il en retournera pour eux et de la chance que vous leurs accorderez d'être partit prenante d'une si belle infrastructure.

Conclusion sur le Start 404 :

Ce fût une incroyable expérience de partage et d'apprentissage et ceux dans quelques domaines que cela soit, c'est une manière vraiment intelligente de mêler différentes compétences les unes avec les autres et de voir quels projets peut en ressortir. En espérant avoir pu vous aider à apporter une solution concrète au problème que développeront les nouvelles technologies de demain. Merci à vous pour l'organisation.

Cordialement l'équipe des CryptoBabies.

Document réalisé le 09/05/2021 par l'équipe du Hackathon CryptoBabies composé de 4 membres :

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