ALCARAZ Hugo
BAUMEL Baptiste
EL KADOURI Soufiane
SERVILLAT Fabien

M1 SICOM

MINING

(Blockchain)

TABLE DES MATIÈRES

1. Qu’est-ce que le minage ?

- Le minage désigne la validation d'un bloc par un des membres du réseau.
- Un bloc est un groupe d’opérations, qui vont être groupées entre elles, et mises à la suite de la chaîne de blocs, constituant ainsi un nouveau maillon à cette chaîne.
- Un bloc est simplement l’agglomération de plusieurs opérations valides. Par exemple, si Bob envoi 5 Bitcoins à Alice alors qu’il n’en possède qu’un, c’est au moment de la création de ce bloc (donc au minage) que les opérations sont confirmées ce qui ne sera pas le cas dans cet exemple-là.
- Le minage est une question d’argent et de temps c’est donc un investissement ce qui représente des risques car tout ce qui est engagé financièrement peut-être perdu.
- Le minage de bitcoins a été le premier minage de crypto-monnaie que les gens ont connu mais aujourd’hui il y a plus de 800 crypto-monnaies qui peuvent être minées et échangées.

2. Le principe du minage.

Dans un cas classique (Bitcoin et tous ses dérivés), le principe est le suivant :

- N’importe quel nœud (membre) du réseau peut proposer un nouveau bloc, et donc miner,
- Le mineur agrège toutes les opérations en attente, non encore incluses dans un bloc et donc non-présentes dans la blockchain,
- Il vérifie la validité de toutes ces opérations (les comptes sont suffisamment approvisionnés, l’opération est dûment signée par les personnes autorisées, etc.),
- Il groupe les opérations dans un même bloc,
- Il soumet le bloc au réseau,
- Le réseau étudie la validité du bloc, dans la forme (respect du protocole informatique) et dans le fond (validité des transactions saisies),
- Le réseau accepte le nouveau bloc et tous les membres l’ajoutent à leur copie locale de la blockchain

La rémunération du mineur

- Soit par les utilisateurs du système monétaire qui payent des frais de transaction qui peuvent choisir de manière libre. Plus ils définissent des frais élevés, plus leurs opérations seront passées rapidement puisque les mineurs priorisent les opérations les plus rémunératrices.

- Soit en créant de la monnaie à chaque bloc. Dans le cas du Bitcoin, ce montant est généré par création monétaire diminue exponentiellement au fil du temps. De ce fait le dernier Bitcoin sera miné en 2140.

Les différents types d'algorithmes de minages :

- DAGGER-HASHIMOTO / ETHASH
- EQUIHASH
- NEOSCRYPT
- LYRA2Z
- CRYPTONIGHT
- NIST5
- XEVAN

Qui fait du minage ?

- Amoureux de hardware,
- Personnes voulant faire vivre la blockchain,
- Personnes voulant gagner de l'argent

Le mining en groupe permet de résoudre un problème (trouvé le nonce) plus rapidement que seul et chaque mineur est récompensé proportionnellement à sa participation.

Détails techniques (Exemple):

- Création d'un hash à partir d'un bloc d'une transaction déjà existante (La taille du bloc est limitée à 1 Méga-octet)
- Générer une entête de bloc en hash (Exemple : 93ef6f358fbb998c60802496863052290d4c63735b7fe5bdaac821de96a53a9a)
- Déterminer le nonce qui devra être inférieur au proof-of-work (Exemple : 0787a6fd6e0782f7f8058fbef45f5c17fe89086ad4e78a1520d06505acb4522f)
- Ajouter le bloc à la chainblock
- Vérification par rapport à la chainblock de l'authenticité du bloc

3. Pourquoi tout le monde ne fait pas de "Mining" ?

Afin de créer un bloc valide dans une blockchain, il faut résoudre une problématique mathématique très complexe. La solution ne peut être résolue que par "force brute" c'est-à-dire, tester les solutions une à une jusqu'à obtenir la solution.

Le minage de nouveau bloc est dûe à:

- La chance, car la solution peut-être résolu dans un cas très rapidement ou dans l'autre cas après plusieurs dizaines de minutes. Le temps de création d'un bloc est très variable.
- La puissance de calcul du mineur. Plus celui-ci dispose de ressources importantes et plus celui-ci trouvera la solution rapidement.
- Afin de s'adapter à l'augmentation de la puissance de calcul des mineurs, le protocole est conçu pour augmenter ou diminuer la difficulté des problèmes mathématiques pour répondre à des besoins et maintenir un temps moyen entre les blocs. (Exemple : 10 Minutes pour le Bitcoin, 12 secondes pour Ethereum).

4. Lien avec UBER.

Dans le cas des blockchains, les mineurs doivent résoudre des problèmes mathématiques complexes le plus rapidement possible pour obtenir la récompense. Le chauffeur d'Uber, dans son cas, reçoit une notification d'alerte pour lui informer qu'un ou plusieurs client veulent se déplacer grâce au système du Uber. Celui-ci doit répondre oui ou non à la demande du client pour empocher la récompense.
Que ce soit pour le chauffeur ou le mineur, dans les deux cas, ils sont conscient des risques à prendre :

Le mineur n'a pas la vie facile

- Facture d'électricité (Le minage du Bitcoin consomme plus que 159 pays)

- Risque technologique (une carte graphique qui ne fonctionne plus)
- Risque de marché (montée de la difficulté, cartes invendables)

- Risque monétaire (fluctuation des monnaies)
- Risques financiers opérationnels (plateforme fonctionne plus, vente impossible, hack d'une plateforme / d'un compte sur une plateforme)

Le mineur peut perdre des mois de travail et de dur labeur en seulement quelques secondes.

Le chauffeur Uber

- Facture
- Assurance
- Risque du marché (augmentation du prix de l'essence)
- Risque de dégradation (vol ou accident)
- Risque de bouchon
- Risque de concurrence
- Risque de perte du permis

Minage pour le TP Uber

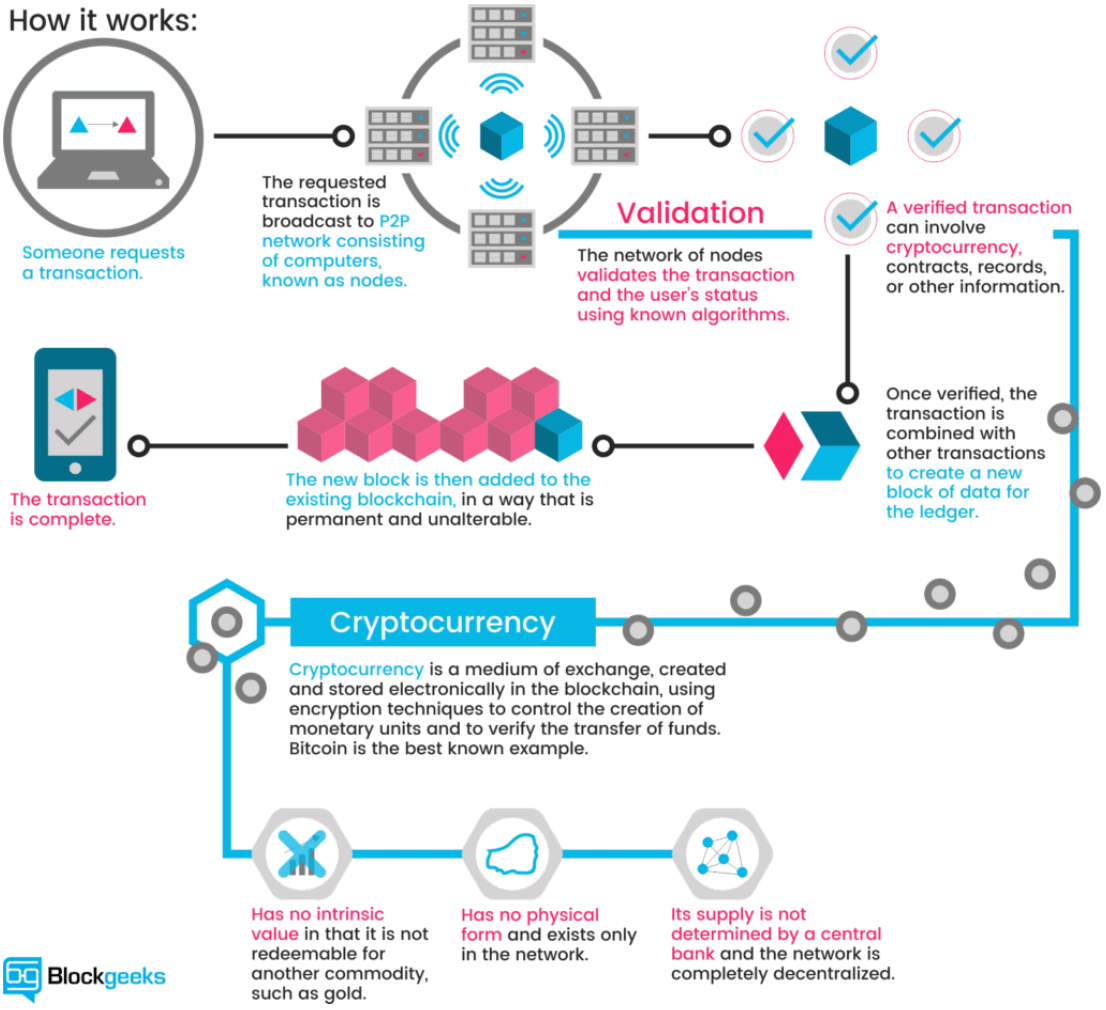
Le minage va permettre la vérification des blockchains et ainsi garantir l'authenticité des transactions des trajets Uber.

De plus, miner dans le système Uber va permettre de gagner une petite somme d'argent utilisable pour payer les trajets. Ainsi, plus on mine, plus on garantie la sécurité des trajets et plus on gagne de quoi faire des trajets.

Le système devra être sécurisé car des données personnelles (lieux, noms, prénoms, voiture, horaire, système de paiement) transitent, mais devra également être rapide :

- Il faudrait utiliser un hash puissant mais rapide.
- Il faut aussi limiter le nombre de bloc qui vont être créé pour ne pas surcharger les capacité de stockage. En effet, plus il y aura de blocs, plus la taille de la chaîne sera grosse.

5. Schéma explicatif du minage



6. Sources

- https://maniabook.argentmania.com/business/bitcoin-mining/articles/mining-comment-a-marche
- https://crypto-monnaie.pro/minage-crypto-monnaie/
- https://www.magelan-software.eu/quest-ce-que-le-minage/
- https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1207718-miner/
- https://fr.wikipedia.org/wiki/Minage_de_cryptomonnaie
- https://forum.hardware.fr/hfr/Discussions/Societe/mining-monnaies-debutant-sujet_107766_1.htm

- https://medium.com/@JB_Pleynet/le-minage-expliqu%C3%A9-aux-non-initi%C3%A9s-b511b5a33117
- https://medium.com/la-baleine/le-minage-pour-qui-comment-e8aaf7d6fa4
- https://medium.com/@mycoralhealth/code-your-own-blockchain-mining-algorithm-in-go-82c6a71aba1f