Fonctionnement de la Blockchain

Adrian Bonnet

Grenoble INP - Esisar

22 10 2021

Sommaire

Structures de données décentralisées

- Table de hachage distribuée
  - *exemple* : torrent
  - partage de données décentralisé (*seeders* et *leechers* via un client de torrent)
  - coordination centralisée des torrents (hébergeur)
- Blockchain
  - *exemple* : cryptomonnaies
  - partage de données décentralisé (entre les nœuds)
  - coordination décentralisée

Blockchain

- Un **registre** (*ledger*) qui permet de stocker des données : liste de transactions (cryptomonnaies), liste de certificats
- Pour ajouter des données, il faut les envoyer à un **nœud** qui va les vérifier et demander à les ajouter à la Blockchain
- Fonctionnement en **liste chaînée**

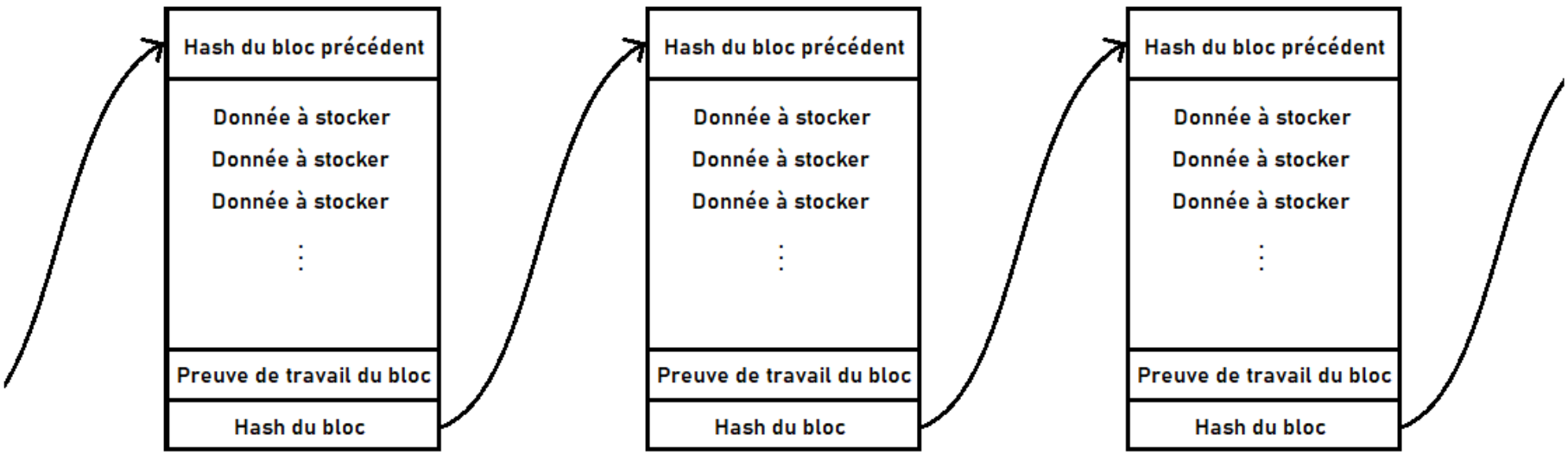

FIGURE 1 – Enchaînement des blocs dans la Blockchain

Partage des informations

- Lorsqu'un nouveau bloc est ajouté, il faut que tous les nœuds qui participent à la Blockchain le reçoivent
- Peu importe comment est faite la diffusion du bloc
  - de pair à pair via une liste de diffusion
  - par un serveur centralisé qui redistribue les informations
  - avec des pigeons voyageurs et des transcripteurs si vous voulez
- Il faut qu'à tout instant, la Blockchain soit identique sur chaque nœud qui participe

Consensus

- Lorsqu'un bloc est ajouté, s'il ne fait pas consensus dans la Blockchain, il y aura un **fork** qui permettra de ne pas le prendre en compte
- Il faut arriver à maintenir une forme de **consensus** dans la Blockchain, pour choisir qui peut écrire un bloc, punir les nœuds frauduleux et récompenser les autres (utilisation des cryptomonnaies)

Méthodes de consensus :

- Preuve de **travail** (PoW) : premier nœud à résoudre un challenge cryptographique (casser un hash) gagne le droit d'écrire le prochain bloc et empoche une récompense
  - problème de gaspillage de ressources
- Preuve d'**enjeu** (PoS) : les nœuds possèdent une mise importante dans la cryptomonnaie, le gagnant est choisi parmi ceux qui ont la plus grande mise
  - problème d'enrichissement des riches

Non-répudiation

Pour supprimer des données inscrites dans la Blockchain, il faut :

- soit attendre que tous les nœuds considèrent le bloc comme trop ancien (aucun contrôle) et le suppriment
- soit faire un fork de la Blockchain, donc toutes les données inscrites dans la Blockchain après nos données seraient perdues
    - (irréalisable en pratique, car le fork favorisé est toujours le plus long)

Aparté Bitcoin

Qu'est-ce que cela veut dire d'**avoir** des Bitcoin ?

Pour aller plus loin

- 3Blue1Brown - Blockchain
  - plus approfondi sur la PoW, mais ne parle pas de la PoS