Blockchain CheatSheet - Consensus

Temps de lecture : 7 min

Table des Matières

§ Fondamentaux

- Consensus
- Nœuds
- Besoins

§ Proof of Work (PoW)

- Vue d'Ensemble
- Forces
- Faiblesses
- Systèmes PoW Actuels

§ Économie

- Pools

§ Proof of Stake (PoS)

- Vue d'Ensemble
- Forces
- Faiblesses
- Proof of Stake Décentralisé (DPoS)
- Systèmes PoW Actuels

§ Le Problème des Généraux Byzantins

- Application Blockchain

§ Autres Algorithmes de Consensus

§ Fondamentaux

Consensus

Définition : Le consensus dans la blockchain fait référence au mécanisme par lequel les nœuds (ordinateurs indépendants connectés dans un réseau) s'accordent sur l'état d'un grand livre distribué. Il garantit que toutes les transactions sont valides et irréversibles, conformément aux règles définies par l'algorithme de consensus.

Types

- Majorité = 51%
- Super-Majorité = +66%
- Unanimité = 100%
- Pondéré = Les votes de Proof of Stake sont pondérés en fonction du stake (ou de la quantité de crypto-monnaie détenue) par chaque nœud.

Nœuds

Définition : Un nœud est un ordinateur qui exécute un logiciel supportant une architecture blockchain spécifique, formant une partie du réseau distribué de la blockchain.

Nœuds Communs

Nœud de Minage : Ordinateurs hautement spécialisés et puissants qui effectuent des calculs pour proposer de nouveaux blocs. Ils reçoivent des récompenses de minage, couvrant les coûts de leurs opérations.

Nœud Complet : Sert de relais entre la création de blocs et leur distribution. Ils maintiennent une copie complète du grand livre de la blockchain et valident toutes les transactions et les blocs pour garantir la cohérence et la sécurité.

Nœud Léger : Sert de relais entre la création de blocs et leur distribution. Ils maintiennent une copie complète du grand livre de la blockchain et valident toutes les transactions et les blocs pour garantir la cohérence et la sécurité.

Besoins

Dans un système blockchain, qui est distribué et décentralisé, un mécanisme robuste est essentiel, car les parties impliquées ne peuvent souvent pas se faire confiance

intrinsèquement. Il est nécessaire d'assurer l'intégrité du grand livre afin que l'historique des transactions soit fiable. Cela conduit à la nécessité de valider les transactions sans avoir besoin de confiance.

Le mécanisme de consensus et ses formes sont conçus pour aborder ces problèmes.

> **Consensus** est le processus qui permet de faire confiance au résultat d'une transaction ou d'un bloc au sein d'une blockchain, sans avoir besoin de faire confiance aux parties individuelles impliquées dans la transaction ou à l'entité qui la vérifie.

---

§ Proof of Work (PoW)

Vue d'Ensemble

- **Objectif** : Assurer l'immutabilité de la blockchain.
- **Comment cela se fait** : Les *Nonces* (nombres utilisés une seule fois) sont ajoutés à la fin du hash de chaque bloc pour trouver un hash qui répond à un objectif de difficulté spécifique, nécessitant souvent un certain nombre de zéros en tête. Cela valide le bloc.
- **Pourquoi** : Le système nécessite une preuve que du travail computationnel a été effectué. Trouver un hash qui répond à l'objectif de difficulté est difficile et nécessite de nombreuses tentatives, montrant que du travail computationnel significatif a été réalisé.
- **Sécurité** : Ce processus rend difficile pour quiconque de modifier les données sans refaire tout le travail computationnel, renforçant ainsi la sécurité de la blockchain.

Forces

- **Temps de Bloc Prédictibles** : Maintient un intervalle de temps constant entre les blocs.
- **Entièrement Décentralisé** : Permet à tout participant de contribuer à la sécurité du réseau.
- **Coût Élevé d'Attaque** : Le coût d'une attaque à 51% le rend peu réalisable.
- **Non Censurable et Public** : Les transactions et les blocs sont diffusés publiquement et ne peuvent pas facilement être censurés.

Faiblesses

- **Consommation Énergétique Élevée** : Le PoW est gourmand en ressources et est souvent critiqué pour son impact environnemental.
- **Centralisation des Pools de Minage** : Peut conduire à une potentielle centralisation, car quelques pools pourraient dominer le processus de minage.

- **Non Réalisable pour les Ordinateurs Standards** : Le minage est devenu impraticable pour les ordinateurs ordinaires en raison des exigences computationnelles élevées.
- **Rentabilité Variable du Minage** : La rentabilité du minage peut fluctuer, ce qui le rend parfois moins avantageux financièrement.

Systèmes PoW Actuels

> Pour obtenir les informations les plus précises et à jour, je recommande de faire une recherche rapide à l'aide d'assistants IA pour rester informé des derniers développements dans les systèmes PoW.

---

§ Économie

Pour la plupart des individus, il est presque impossible de miner un bloc avec succès seul en raison des coûts prohibitifs du matériel de minage spécialisé et de l'électricité, surtout par rapport aux récompenses potentielles.

Pools

La méthode la plus pratique est de rejoindre un pool de minage, qui regroupe la puissance de traitement de plusieurs mineurs. Ces pools ont généralement accès à des sources d'énergie moins chères et à des équipements de minage plus efficaces. En tant que membre, vous recevez une partie des récompenses proportionnelle à votre contribution aux ressources globales du pool.

---

§ Proof of Stake (PoS)

Vue d'Ensemble

Le Proof of Stake (PoS) est un mécanisme de consensus alternatif au Proof of Work (PoW), offrant une approche différente pour atteindre le consensus dans un réseau blockchain.

Définition : Dans le PoS, le "stake" fait référence à la quantité de crypto-monnaie qu'un individu détient et engage pour obtenir le droit de participer au processus de création de nouveaux blocs. La probabilité d'être choisi pour créer un bloc est généralement proportionnelle au montant de stake détenu.

Forces

- **Efficacité Énergétique** : Le PoS est beaucoup moins énergivore par rapport au PoW, réduisant l'impact environnemental.
- **Sécurité Basée sur l'Intérêt** : Plus un validateur a de stake, plus il risque en agissant de manière malveillante, alignant ainsi ses intérêts avec le bien-être du réseau.
- **Coût d'Attaque le Plus Élevé** : Le coût d'une attaque à 51% rend cela le moins réalisable en raison de l'intérêt que l'on obtient en ayant plus de contrôle.
- **Non Censurable et Public** : Les transactions et les blocs sont diffusés publiquement et ne peuvent pas facilement être censurés.
- **Significativement Plus Scalable** : Les coûts opérationnels plus bas permettent au PoS de traiter plus de transactions, améliorant la scalabilité.

Faiblesses

- **Accumulation de Richesse** : Les stakes plus élevés augmentent les récompenses, risquant une centralisation de la richesse et des déséquilibres de pouvoir.
- **Problèmes de Sécurité** : Le PoS peut être perçu comme moins sécurisé que le PoW, car la sécurité repose fortement sur les pénalités économiques, et non sur les efforts computationnels.
- **Risque d'Attaque Sybil** : Les barrières à l'entrée élevées dissuadent mais ne suppriment pas les attaques Sybil, où plusieurs identités fictives influencent le réseau.
- **Problème du Nothing-at-Stake** : Les validateurs peuvent soutenir plusieurs forks de la blockchain, car cela n'entraîne aucun coût significatif, ce qui peut entraîner des problèmes de double dépense.

Proof of Stake Décentralisé (DPoS)

Le DPoS vise à démocratiser le processus de staking en permettant aux parties prenantes de déléguer leur pouvoir de staking à des "délégués", qui valident les transactions et créent des blocs en leur nom. Ce système peut potentiellement résoudre la centralisation des récompenses en répartissant plus largement la possibilité de gagner des frais de transaction et des récompenses de blocs parmi les participants.

Systèmes PoW Actuels

> Pour obtenir les informations les plus précises et à jour, je recommande de faire une recherche rapide à l'aide d'assistants IA pour rester informé des derniers développements dans les systèmes PoW.

---

§ Le Problème des Généraux Byzantins

Le Problème des Généraux Byzantins illustre une difficulté à atteindre un consensus dans les systèmes distribués, surtout dans des conditions où certains participants (ou "nœuds") peuvent agir de manière malveillante ou échouer à communiquer de manière fiable. Le problème est nommé d'après une analogie impliquant des généraux byzantins qui doivent s'entendre sur un plan de bataille par l'intermédiaire de messagers, sachant que certains des généraux ou des messagers pourraient être des traîtres.

Aspects Clés :

- **Confiance et Coordination** : Assurer que tous les généraux loyaux (ou nœuds dans une blockchain) prennent une décision commune, malgré la présence de traîtres qui pourraient perturber le consensus ou envoyer de fausses informations.
- **Fiabilité du Consensus** : Le besoin d'un mécanisme garantissant un accord entre les participants, assurant que les messages ne sont pas modifiés et que la stratégie convenue (ou la transaction) est exécutée de manière cohérente à travers le réseau.

Application Blockchain

Dans la technologie blockchain, ce problème est comparable à garantir que tous les nœuds du réseau se mettent d'accord sur la validité et l'ordre des transactions, malgré les tentatives potentielles de certains participants de tromper ou de perturber le processus. Des solutions telles que Proof of Work (PoW) et Proof of Stake (PoS) sont conçues pour atténuer ces risques en exigeant des participants qu'ils contribuent par leur travail ou leur stake, créant ainsi des barrières économiques et computationnelles contre les comportements malhonnêtes.

---

§ Autres Algorithmes de Consensus

- **Tolérance aux Pannes Byzantines Pratiques (pBFT)** : Élection démocratique d'un leader qui délègue les nœuds "shard" pour la validation.
- **Tolérance aux Pannes Byzantines Fédérées (fBFT)** : Élections fédérées d'un leader qui délègue les nœuds "shard" pour la validation.
- **Tolérance aux Pannes Byzantines Décentralisée**
- **Proof-of-Importance (PoI)** : À quel point vous utilisez votre stake.
- **Proof-of-Elasped-Time (PoET)**
- **Proof-of-Capacity (PoC - aussi connu sous le nom de P-o-Space)**
- **Proof-of-Authority (PoA)**
- **Raft** (consensus plus classique, non spécifique à la blockchain)

Il n'est pas prouvé qu'un algorithme de consensus particulier soit adapté à chaque cas. Dans de nombreux cas, cela pourrait bien être le contraire.

> Les algorithmes de consensus doivent être adaptés au cas d'utilisation.

Suggestions pour la suite

Blockchain CheatSheet - Cryptoapplications

Auteur : Kenneth Boldrini