Blockchain CheatSheet - Consenso

Tempo di Lettura: 7 m

Indice dei Contenuti

§ Fondamenti

Consenso

Definizione: Il consenso nella blockchain si riferisce al meccanismo attraverso il quale i nodi (computer indipendenti collegati in rete) concordano sullo stato di un registro distribuito. Garantisce che tutte le transazioni siano valide e irreversibili, secondo le regole definite dall'algoritmo di consenso.

Tipi

- Maggioranza = 51%
- Super-Maggioranza = +66%
- Unanimità = 100%
- Ponderato = I voti di Proof of Stake sono ponderati in base alla posta (o alla quantità di criptovaluta posseduta) di ciascun nodo.

Nodi

Definizione: Un nodo è un computer che esegue il software che supporta una specifica architettura blockchain, formando parte della rete distribuita della blockchain.

Nodi comuni

Nodo Minerario: Computer altamente specializzati e potenti che eseguono calcoli per proporre nuovi blocchi. Ricevono ricompense di mining, coprendo il costo delle loro operazioni.

Nodo Completo: Agisce come un relè tra la creazione di blocchi e la loro distribuzione. Mantengono una copia completa del registro della blockchain e convalidano tutte le transazioni e i blocchi per garantire coerenza e sicurezza.

Nodo Leggero: Agisce come un relè tra la creazione di blocchi e la loro distribuzione. Mantengono una copia completa del registro della blockchain e convalidano tutte le transazioni e i blocchi per garantire coerenza e sicurezza.

Necessità

In un sistema blockchain, che è distribuito e decentralizzato, è essenziale un meccanismo robusto poiché le parti coinvolte spesso non possono fidarsi intrinsecamente l'una dell'altra.

È necessario garantire l'integrità del registro affinché la cronologia delle transazioni sia affidabile. Questo porta alla necessità di convalidare le transazioni senza la necessità di fiducia.

Il meccanismo di consenso e le sue forme sono progettati per affrontare queste questioni.

> **Il consenso** è il processo che consente di fidarsi dell'esito di una transazione o di un blocco all'interno di una blockchain, senza la necessità di fidarsi delle parti individuali coinvolte nella transazione o dell'entità che la verifica.

---

§ Proof of Work (PoW)

Panoramica

- **Scopo**: Garantire l'immutabilità della blockchain.
- **Come viene fatto**: *Nonce* (Numeri utilizzati una sola volta) sono aggiunti alla fine dell'hash di ogni blocco per trovare un hash che soddisfi un obiettivo di difficoltà specifico, spesso richiedendo un certo numero di zeri iniziali. Questo convalida il blocco.
- **Perché**: Il sistema richiede una prova che sia stato eseguito un lavoro computazionale. Trovare un hash che soddisfi l'obiettivo di difficoltà è impegnativo e richiede molti tentativi, dimostrando che è stato eseguito un lavoro computazionale significativo.
- **Sicurezza**: Questo processo rende difficile per chiunque alterare i dati senza rifare tutto il lavoro computazionale, migliorando così la sicurezza della blockchain.

Punti di forza

- **Tempi di blocco prevedibili**: Mantiene un intervallo di tempo costante tra i blocchi.
- **Completamente decentralizzato**: Consente a qualsiasi partecipante di contribuire alla sicurezza della rete.
- **Alto costo di attacco**: La spesa per realizzare un attacco al 51% lo rende non fattibile.
- **Incensurabile e pubblico**: Le transazioni e i blocchi vengono trasmessi pubblicamente e non possono essere facilmente censurati.

Punti di debolezza

- **Alto consumo energetico**: PoW è intensivo di risorse, spesso criticato per il suo impatto ambientale.
- **Centralizzazione dei pool di mining**: Può portare a una potenziale centralizzazione, poiché pochi pool potrebbero dominare il processo di mining.

- **Non fattibile per i computer standard**: Il mining è diventato impraticabile per i computer ordinari a causa degli alti requisiti computazionali.
- **Redditività del mining variabile**: La redditività del mining può fluttuare, rendendolo talvolta meno redditizio finanziariamente.

Sistemi PoW attuali

> Per le informazioni più accurate e aggiornate, consiglio di effettuare una ricerca rapida con l'aiuto di assistenti AI per rimanere aggiornati sugli ultimi sviluppi nei sistemi PoW.

---

§ Economia

Per la maggior parte delle persone, è quasi impossibile riuscire a minare un blocco da soli a causa dei costi proibitivi dell'hardware di mining specializzato e dell'elettricità, soprattutto rispetto ai potenziali premi.

Pool

L'approccio più fattibile è unirsi a un pool di mining, che consolida la potenza di elaborazione di più minatori. Questi pool hanno tipicamente accesso a fonti di energia più economiche e a dispositivi di mining più efficienti. Come membro, riceveresti una parte delle ricompense proporzionale al tuo contributo alle risorse complessive del pool.

---

§ Proof of Stake (PoS)

Panoramica

Proof of Stake (PoS) è un meccanismo di consenso alternativo al Proof of Work (PoW), che offre un approccio diverso per raggiungere il consenso in una rete blockchain.

Definizione: Nel PoS, la "posta" si riferisce alla quantità di criptovaluta che un individuo detiene e impegna come mezzo per ottenere il diritto di partecipare al processo di creazione di nuovi blocchi. La probabilità di essere scelti per creare un blocco è tipicamente proporzionale alla quantità di posta detenuta.

Punti di forza

- **Efficienza energetica**: PoS è molto meno intensivo di energia rispetto a PoW, riducendo l'impatto ambientale.
- **Sicurezza basata sugli interessi**: Più alta è la posta di un validatore, più ha da perdere agendo in modo malizioso, allineando i suoi interessi con il benessere della rete.
- **Costo più alto di attacco**: La spesa per realizzare un attacco al 51% lo rende il più non fattibile a causa dell'interesse che si ottiene avendo più controllo.
- **Incensurabile e pubblico**: Le transazioni e i blocchi vengono trasmessi pubblicamente e non possono essere facilmente censurati.
- **Significativamente più scalabile**: I costi operativi più bassi permettono al PoS di gestire più transazioni, migliorando la scalabilità.

Punti di debolezza

- **Accumulo di ricchezza**: Premi più alti aumentano le ricompense, rischiando la centralizzazione della ricchezza e gli squilibri di potere.
- **Preoccupazioni sulla sicurezza**: PoS può essere percepito come meno sicuro rispetto a PoW perché la sicurezza basata sulla posta dipende fortemente dalle penalità economiche, non dagli sforzi computazionali.
- **Rischio di attacco Sybil**: Le alte barriere all'ingresso scoraggiano ma non eliminano gli attacchi Sybil, in cui molteplici identità fittizie influenzano la rete.
- **Problema del nulla in gioco**: I validatori possono supportare più fork della blockchain poiché farlo non comporta costi significativi, potenzialmente portando a problemi di doppia spesa.

Proof of Stake Delegato (DPoS)

DPoS mira a democratizzare il processo di staking consentendo agli stakeholder di delegare il loro potere di staking a "delegati", che convalidano le transazioni e creano blocchi per loro conto. Questo sistema può potenzialmente affrontare la centralizzazione delle ricompense diffondendo l'opportunità di guadagnare commissioni di transazione e premi per i blocchi più ampiamente tra i partecipanti.

Sistemi PoW attuali

> Per le informazioni più accurate e aggiornate, consiglio di effettuare una ricerca rapida con l'aiuto di assistenti AI per rimanere aggiornati sugli ultimi sviluppi nei sistemi PoW.

---

§ Il Problema dei Generali Bizantini

Il Problema dei Generali Bizantini illustra una sfida nel raggiungere il consenso nei sistemi distribuiti, specialmente in condizioni in cui alcuni partecipanti (o "nodi") possono agire in modo malizioso o non comunicare in modo affidabile. Il problema prende il nome da un'analogia che coinvolge generali bizantini che devono concordare un piano di battaglia tramite messaggeri, sapendo che alcuni dei generali o dei messaggeri potrebbero essere traditori.

Aspetti chiave:

- **Fiducia e coordinamento**: Garantire che tutti i generali leali (o nodi in una blockchain) raggiungano una decisione comune, nonostante la presenza di traditori che possono interrompere il consenso o inviare informazioni false.
- **Affidabilità del consenso**: La necessità di un meccanismo che garantisca l'accordo tra i partecipanti, assicurando che i messaggi non vengano alterati e che la strategia concordata (o la transazione) venga eseguita in modo coerente in tutta la rete.

Applicazione Blockchain

Nella tecnologia blockchain, questo problema è analogo al garantire che tutti i nodi nella rete concordino sulla validità e sull'ordine delle transazioni, nonostante i tentativi potenziali di alcuni partecipanti di barare o di interrompere il processo. Soluzioni come Proof of Work (PoW) e Proof of Stake (PoS) sono progettate per mitigare questi rischi richiedendo ai partecipanti di contribuire con lavoro o posta, creando barriere economiche e computazionali al comportamento disonesto.

---

§ Altri Algoritmi di Consenso

- **Tolleranza ai guasti bizantini pratica (pBFT)**: Elezione democratica di un leader che delega i nodi "shard" per la convalida.
- **Tolleranza ai guasti bizantini federata (fBFT)**: Elezioni federate di un leader che delega i nodi "shard" per la convalida.
- **Tolleranza ai guasti bizantini delegata**
- **Proof-of-Importance (PoI)**: Quanto usi la tua posta.
- **Proof-of-Elapsed-Time (PoET)**
- **Proof-of-Capacity (PoC - aka P-o-Space)**
- **Proof-of-Authority (PoA)**
- **Raft** (consenso più classico, non specifico per blockchain)

Non è provato che un particolare algoritmo di consenso sia adatto a ogni caso. Potrebbe essere molto bene il caso opposto in molte istanze.

> Gli algoritmi di consenso devono essere ottimizzati per il caso d'uso.

Suggerimenti per il seguito

Blockchain CheatSheet - Cryptoapplications

Autore: Kenneth Boldrini