Algoritmi di consenso distribuito

Francesco Pugliese, PhD

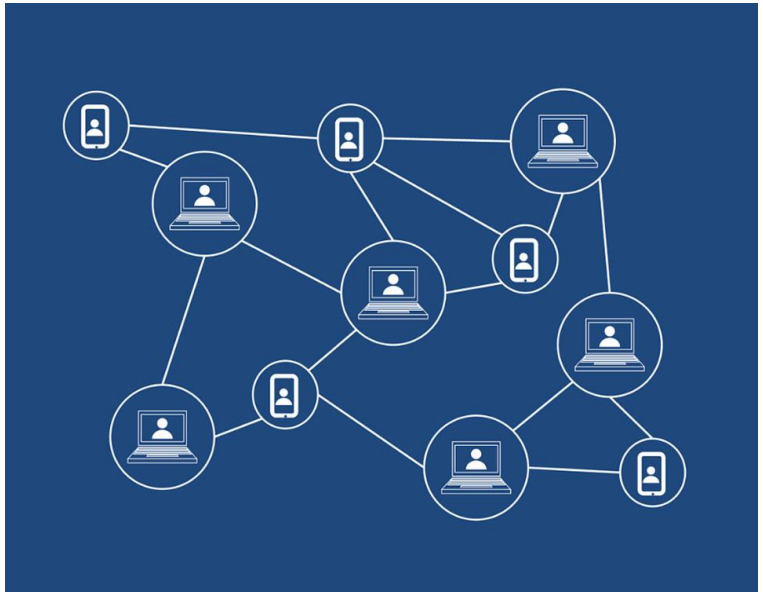
neural1977@gmail.com

Algoritmi di consenso distribuito

- Un **algoritmo di consenso** è un meccanismo che permette a utenti o dispositivi di coordinarsi in un contesto **distribuito**.

- Deve garantire che tutti gli agenti nel sistema possano concordare su una singola fonte di verità, anche se alcuni agenti falliscono.

- In altre parole, il sistema deve essere **fault-tolerant.**



Algoritmi di consenso distribuito

- ✓ In una configurazione centralizzata, una singola entità ha **potere sul sistema**. In gran parte dei casi, possono apportare modifiche come vogliono – non esiste un complesso sistema di governance per raggiungere il consenso tra diversi amministratori.

- ✓ In una configurazione decentralizzata, invece, è tutta un'altra storia. Supponiamo di avere un **database distribuito** – come facciamo a raggiungere un accordo su quali voci debbano essere aggiunte?

Algoritmi di consenso distribuito

- ✓ Superare questa sfida in un ambiente in cui sconosciuti non si fidano gli uni degli altri è stato forse lo sviluppo più cruciale per aprire la strada alle **blockchain**.

- ✓ Vediamo come gli algoritmi di consenso sono vitali per il funzionamento delle **criptovalute** e dei registri distribuiti.

Algoritmi di consenso e criptovalute

- ✓ Nelle **criptovalute**, i saldi degli utenti vengono registrati in un database – la **blockchain**.

- ✓ E' fondamentale che tutti (o, più precisamente, tutti i **nodi**) mantengano una copia **identica del database**. Altrimenti, finiremmo presto con informazioni contrastanti, compromettendo totalmente lo scopo del network di criptovaluta.

- ✓ La **crittografia a chiave pubblica** garantisce che gli utenti non possono spendere le **monete** di altri, ma deve comunque esserci una singola fonte di verità su cui i partecipanti al network si basano, per riuscire a determinare se i fondi sono già stati spesi.

Funzionamento degli Algoritmi di consenso

- ✓ Per prima cosa, chiediamo agli utenti che vogliono aggiungere **blocchi** (chiamiamoli validatori) di fornire una **stake**.
- ✓ La **stake** è una qualche sorta di valore che il validatore deve mettere in gioco, con l'obiettivo di dissuaderlo dall'agire in modo disonesto. Se imbroglia, perderà la sua posta in gioco.
- ✓ Esempi di questa stake includono potenza computazionale, criptovaluta o persino reputazione.

Funzionamento degli Algoritmi di consenso

- ✓ Perché i **validatori** dovrebbero rischiare le proprie risorse? Beh, c'è anche una ricompensa in palio. Questa consiste solitamente nella **criptovaluta nativa** del protocollo ed è composta dalle commissioni pagate da altri utenti, unità di criptovaluta appena generate o entrambi.

L'ultimo elemento di cui abbiamo bisogno è la **trasparenza**. Dobbiamo essere in grado di scoprire quando qualcuno sta imbrogliando. Idealmente, dovrebbe essere costoso produrre **blocchi** ma economico per chiunque verificarli. Ciò garantisce che i **validatori** sono tenuti sotto controllo dagli utenti regolari.

Tipi di Algoritmi di consenso

- La **Proof of Work** è il padrino degli algoritmi di consenso **blockchain**. E' stato implementato per la prima volta in **Bitcoin**, ma il concetto è in circolazione da ben prima. Nella Proof of Work, i **validatori** (denominati miner) elaborano tramite **hash** i dati che vogliono aggiungere fino a quando non producono una soluzione specifica.

- Una hash è una stringa apparentemente casuale di lettere e numeri generata dall'elaborazione di dati attraverso una funzione di hash. Tuttavia, elaborando gli stessi dati nella stessa funzione, si otterrà lo stesso output. Cambiando anche un solo dettaglio, però, porterà a una hash completamente differente.

Bibliografia

https://academy.binance.com/it/articles/what-is-a-blockchain-consensus-algorithm