Sistemi Cooperativi e Reti Sociali

Lezione 5

Daniele Margiotta, Gabriele Prestifilippo, Luca Squadrone

Maggio 2019

Indice

Capitolo 1

Introduzione

Nel contesto delle criptovalute, gli algoritmi di consenso costituiscono un elemento cruciale per ogni network blockchain, in quanto hanno il compito di mantenere l'integrità e la sicurezza di questi sistemi distribuiti. Il primo algoritmo di consenso per criptovalute creato è la Proof of Work (PoW), progettata da Satoshi Nakamoto e implementata su Bitcoin per garantire la Byzantine Fault Tolerance.

Capitolo 2

Algoritmo del consenso

Un algoritmo di consenso può essere definito come il meccanismo attraverso cui un network blockchain raggiunge il consenso. Le blockchain pubbliche (decentralizzate) sono sviluppate come sistemi distribuiti e, dato che non si basano su un'autorità centrale, i nodi distribuiti devono concordare sulla validità delle transazioni. Ecco dove entrano in gioco gli algoritmi di consenso. Essi garantiscono che le regole del protocollo vengano seguite e che tutte le transazioni avvengano correttamente, facendo in modo che le monete possano essere spese solo una volta.

2.1 Qual è l'Importanza degli Algoritmi di Consenso nelle Criptovalute?

Gli algoritmi di consenso sono di vitale importanza per mantenere l'integrità e la sicurezza del network di una criptovaluta. Forniscono un mezzo ai nodi distribuiti per raggiungere il consenso su quale versione della blockchain è quella reale. Concordare l'attuale stato della blockchain è essenziale per il corretto funzionamento di un sistema economico digitale.
L'algoritmo di consenso Proof of Work è considerato una delle migliori soluzioni al Problema dei Generali Bizantini, che ha reso possibile la creazione di Bitcoin come sistema Byzantine Fault Tolerance. Questo significa che la blockchain di Bitcoin è estremamente resistente agli attacchi, come il 51% attack (o majority attack). Non solo perché il network è decentralizzato, ma anche grazie all'algoritmo PoW. I costi elevati associati al processo di mining rendono molto difficile e improbabile che i miner investano le proprie risorse per ostacolare il network.

2.2 Proof of Work (PoW)

La PoW è il primo algoritmo di consenso creato. Viene utilizzato da Bitcoin e tante altre criptovalute. L'algoritmo Proof of Work è una parte essenziale del mining process.
Il mining PoW implica diversi tentativi di hashing, quindi una maggiore potenza di calcolo risulta in un maggior numero di tentativi al secondo. In altre parole, i miner con un hash rate maggiore hanno più probabilità di trovare una

soluzione valida per il blocco successivo (ovvero la block hash). L'algoritmo di consenso PoW consente ai miner di convalidare un nuovo blocco e aggiungerlo alla blockchain solo se i nodi distribuiti del network raggiungono il consenso e concordano che la block hash fornita dal miner è una proof of work valida.

2.3 Probblema dei generali Bizantini

Si tratta di un problema informatico che consiste nel trovare un accordo comunicando tramite messaggi fra le diverse parti del network.
Questo problema è stato teorizzato dai matematici Leslie Lamport, Marshall Pease e Robert Shostak nel 1982, i quali crearono la metafora dei generali.
La blockchain nasce con lo scopo di eliminare la fiducia verso terze parti durante una transazione. Per essere tale essa ha bisogno di un meccanismo che sostituisca un ente centrale. L'obbiettivo è far sì che tutti siano concordi sull'ordine cronologico delle transazioni, e quindi è fondamentale introdurre un algoritmo di consenso, che permetta appunto, di "mettere d'accordo" i diversi attori del network.

2.3.1 La metafora

Diversi generali, durante un assedio, sono sul punto di attaccare una città nemica. Essi sono dislocati in diverse aree strategiche, e possono comunicare solo mediante messaggeri di fiducia al fine di coordinare l'attacco decisivo. Tra questi messaggeri però è altamente probabile, se non addirittura certo, che vi siano dei traditori. Questo problema risiede dunque, nella facoltà di portare avanti l'attacco nonostante il rischio di tradimento. Ciò che è conosciuto come consenso decentralizzato.
Il messaggio che può arrivare può essere nel migliore dei casi coordinato: attaccare o ritirarsi.
Oppure, come è più logico che avvenga, il messaggio non sarà coordinato, quindi arriveranno entrambi gli ordini: **attaccare e ritirarsi**.
Il problema che affligge i generali bizantini è lo stesso che devono affrontare i sistemi di elaborazione distribuiti. Come raggiungere un consenso su una rete distribuita in cui alcuni nodi possono essere difettosi o volontariamente corrotti?

2.3.2 Bitcoin

Nel caso specifico di Bitcoin, il sistema deve essere in grado di mantenere la sua affidabilità nel caso in cui una minoranza dei componenti invii informazioni errate o dannose per eludere la verifica della **doppia spesa**.
Questo problema è molto difficile da risolvere, ma Satoshi Nakamoto, con la blockchain di Bitcoin offre una soluzione pratica e funzionale combinando crittografia asimmetrica, sistemi peer to peer e Proof of Work. Facendo in modo che tutti i partecipanti della rete possano concordare e condividere in modo rapido e sicuro ogni messaggio trasmesso.
Nelle sue mail Nakamoto spiega come la "chain della proof of work" offre una soluzione al problema dei generali bizantini. Illustra come un certo numero di generali pronti ad attaccare il re debbano coordinarsi sull'istante in cui sfer-

rare l'attacco. Non è importante quale istante scegliere in particolare, ma è determinante che sia **sincronizzato**.
E' stato stabilito che il momento dell'attacco verrà stabilito dal primo ente che decide il momento dell'attacco, e sarà ritenuto valido per tutti. Ma siccome il network non è istantaneo, può succedere che due generali annuncino due differenti orari per l'attacco in modo quasi simultaneo. Con il risultato che alcuni recepiranno il primo orario e altri il secondo. Per risolvere questo problema si utilizza la catena della prova di lavoro. Quando un generale riceve un messaggio deve risolvere un problema estremamente difficile. Il primo che lo risolve, lo comunica agli altri partecipanti. Se qualcuno stava lavorando su un orario di attacco diverso, dovrà sostituirlo con quello che ha appena ricevuto, perché questa catena è quella più lunga, con più lavoro, dunque ritenuta valida.

Capitolo 3

Confirmation

Tutti le blockchain pubblicihe fanno uso di blockchain Confirmation. Quando una transazione viene trasmessa per la prima volta alla blockchain, inizia con 0 conferme, il numero aumenta quando viene aggiunto un successivo blocco al primo.
Le conferme di Blockchain sono vitali in quanto sono un modo di verificare e legittimare le informazioni che diventeranno immutabili. Se una transazione è considerata fraudolenta, verrà respinta dalla blockchain: questo si verifica nel caso che dopo il primo blocco contenente la transazione effettuata venga inserito in coda un altro blocco contenente una contraddizione.
In media, gli scambi di criptovaluta richiedono un minimo di 6 conferme fino a quando una transazione non viene accettata.

3.1 Perchè 6 blocchi per la conferma?

Consideriamo 100 peer nella rete Bitcoin, e consideriamo 51 di questi **"onesti"** ed i restanti 49 **"non onesti"**.
Per poter essere sicuri che l'algoritmo del consenso funzioni ci serve sapere che i "non onesti" lavorino tanto quanto gli "onesti", per far questo si introduce il **Delay time**.
Il delay time impedisce a qualsiasi disonesto di poter eseguire più operazioni di seguito, questo ritardo sono i 10 minuti di tempo per poter costruire un nuovo blocco.
Per far si che ci sia Trust nella rete e necessario essere sicuri (w.h.p.) che un blocco malevolo sia riconosciuto prima di poter confermare un blocco intero di transazioni.
Sappiamo che trovare una collissione in uno stesso blocco è $1/m$ (m sono i peer) e quella di non trovarlo sono $1 - 1/m$. Se colleghiamo 2 blocchi allora la probabilità di non trovare collisioni diventa $(1 - 1/m)^2$, dopo che viene fatto per ogni peer (ricostruendo la catena) la probabilità diventa $(1 - 1/m)^m$ che è circa $1/e$. Dopo aver ricostruito la catena quindi, il numero di blocchi affinché riesca a trovare una collisione è "e", con 3 passi quindi con alta probabilità puoi raggiungere la collisione.
Quindi in teoria servirebbero 3 blocchi per poter confermare una transazione, ma se ne aspettano 6 perchè se con 3 blocchi i peer "benevoli" costruiscono l'intera

catena, anche i peer "malevoli" costruiscono la propria con 3 blocchi. Quindi dopo 6 blocchi (3+3) sono sicuro che troverò (se esistente) un'incongruenza e in quel caso potrò stroncare il blocco contenente il double spending.

3.2 Problemi

Questo ci mostra come ogni peer della rete Bitcoin ha un problema, che l'algoritmo del consenso ha un problema, e cioè che esistono le **Miner Farm**, strutture equipaggiate con tutte le apparecchiature necessarie ad estrarre ("minare") Bitcoins o altre criptovalute. Sono degli intermediari software tra i miner comuni, che possono quindi (grazie alla potenza di calcolo che hanno a disposizione) rompere lo schema del consenso, rendendo tutto il modello a **Controllo Centralizzato**.