Sistemi Cooperativi e Reti Sociali

Daniele Margiotta, Gabriele Prestifilippo, Luca Squadrone

Giugno 2019

Indice

1 Introduzione **2**

2 Algoritmi del consenso **3**
2.1 Proof of Work (PoW) 3
2.2 Proof of Stake (PoS) 3
2.2.1 Proof od Work vs Proof of Stake 4
2.2.2 Conclusioni confronto 5
2.3 Proof of Authority (PoA) 5
2.3.1 Di cosa ha bisogno la PoA 6
2.3.2 Proof of Authority vs Proof of Stake 6
2.3.3 Critiche PoA 6

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, un secondo algoritmo del consenso è la **Proof of Stake** (PoS) sviluppato nel 2011 come alternativa alla PoW della piattaforma Ethereum ed un terzo algoritmo del consenso è la **Proof of Authority** (PoA) termine proposto nel 2017 dal co-fondatore ed ex-CTO di Ethereum Gavin Wood.

Capitolo 2

Algoritmi 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 Proof of Work (PoW)

Nelle blockchain con un consenso Proof of Work puro (come Bitcoin), solo i miner possono aggiungere blocchi alla catena, impiegando hardware in grado di indovinare efficientemente la risposta a un dato problema matematico. Ogni volta che un miner trova una risposta valida, può creare un blocco che verrà accettato dal network. Mentre i miner possono scegliere di partecipare al mining di qualsiasi catena, il network accetterà come legittima soltanto quella con la maggior Proof of Work accumulata (cioè il maggior numero di hash, o tentativi). Questo significa che i miner sono incentivati a lavorare sulla catena più lunga, e quando vedono un nuovo blocco valido, cercheranno di trovare la soluzione che permette loro di costruire su quel nuovo blocco.
La difficoltà nel riscrivere la blockchain è ciò che le consente di agire da registro per transazioni finanziarie. Quando una transazione risulta in un blocco che invia monete a uno wallet, e diversi blocchi sono stati costruiti su quel blocco (conferme), diventa molto poco probabile che quel blocco (e transazione) venga riscritto.

2.2 Proof of Stake (PoS)

Il meccanismo di consenso Proof of Stake è un metodo alternativo per decidere chi può aggiungere nuovi blocchi e verificare l'attuale stato della blockchain. Invece di miner che competono per risolvere un problema, con la proof of stake, il produttore del blocco successivo, o forger, viene determinato attraverso un

processo basato sul numero di monete conservate in wallet (letteralmente "stake", posta in gioco). Questo processo confida nel fatto che chi ha più da perdere prenderà decisioni responsabili per se stesso e quindi la totalità del network.
Il consenso Proof of Stake elimina la necessità di un processo di mining dispendioso in termini di energia, ma la mancanza di un investimento energetico significativo crea un altro problema, a volte indicato come "nothing at stake" (niente in gioco). Nel caso di un fork, i forger PoS (il termine "forging" viene in genere usato al posto di "mining") sono incentivati a lavorare su entrambe le catene perché il forging su una catena extra costa molto poco e possono ricevere le ricompense su entrambe le catene. Questo scenario rappresenta un problema per il network in quanto dovrebbe esistere soltanto una catena, e concordare sullo stato di quella singola catena è l'obiettivo del meccanismo di consenso.
La Proof of Stake ha un ulteriore problema per quanto riguarda la distribuzione di token. I miner PoW sostengono costi significativi (hardware, elettricità) e devono in genere vendere una notevole porzione delle monete ricevute per coprire queste spese. Di conseguenza, molte di queste monete possono essere acquistate sul mercato, invece di essere accumulate dai miner. I forger Proof of Stake hanno costi operativi molto bassi, quindi non hanno la stessa pressione a vendere le monete ricevute per il mantenimento del network. Le entità in possesso di grandi somme che partecipano alla Proof of Stake tendono ad aumentare la propria quota di monete in circolazione attraverso le ricompense per i blocchi e le commissioni di transazione dagli utenti del network. Questa struttura è stata paragonata al feudalesimo, il network è effettivamente posseduto e operato dai possessori di monete, e gli utenti pagano loro affitti per poterlo usare. Esiste in genere un limite minimo al di sotto del quale non è possibile partecipare direttamente al processo della Proof of Stake.

2.2.1 Proof od Work vs Proof of Stake

- La Proof of Work è migliore per la condivisione della valuta. Sebbene i miner vengano pagati per il loro lavoro, il costo associato alla convalida in genere richiede loro di vendere anziché conservare la loro moneta come accade invece nella PoS. Ciò crea una distribuzione più uniforme sul mercato. Per un miner infatti accumulare non è vantaggioso come lo è per uno Staker, quindi c'è una maggiore ricompensa per l'acquisto e la vendita piuttosto che per l'accumulare.

- Consenso del SPV (Simplified Payment Verification): in un sistema proof of work se avviene un fork nella catena a causa di problemi nel consenso, è più facile determinare quale catena abbia il maggior supporto dei data mining. Gli utenti della rete seguiranno in genere la catena più lunga, in questo modo si crea una blockchain con meno probabilità di double spending.

- La Proof of Work contiene il quantitativo della valuta emessa in quanto può modificare la difficoltà della prova, con la Proof of Stake invece non esiste alcuna cooperazione tra tecnologia e mercati per regolare e mantenere una fornitura deflazionistica. L'estrazione di moneta è determinata dal quantitativo di soldi nel Wallet degli Staker, rimuovendo completamente il costo dell'attività mineraria, senza lasciare spazio a un meccanismo di

mercato per emergere e regolare l'inflazione. Teoricamente, quindi, la crescita dell'offerta di monete PoS rimane costante, indipendentemente dal suo valore e dalla redditività dello staking.

- Necessità di hardware: i miner sono in costante ricerca di hardware che migliori le prestazioni in rapporto al consumo di energia, a differenza delle controparti del PoS che non utilizzando hardware non possono migliorare in velocità.
- Sicurezza: la sicurezza del consenso PoS non deriva da un lavoro fisico come nella PoW e quindi la Pos ha bisogno di meccanismi aggiuntivi per affrontare i problemi di sicurezza della rete.
- Rich get Richer: a differenza della PoW, dove il miner viene pagato per fare il lavoro, nella PoS, più possiedi la valuta, più soldi guadagni. Il protocollo PoS poi pesa i voti degli Staker in base al peso del loro Wallet, ciò significa che un gruppo di "ricchi" può controllare l'intera rete.

2.2.2 Conclusioni confronto

La realtà è che mentre Proof of Stake gestisce alcuni dei problemi posti dal meccanismo Proof of Work, crea diversi nuovi problemi completamente diversi. Nel mondo delle criptovalute, la Proof of Work è il protocollo più comune. Nel mondo Bitcoin, la prova del lavoro è l'unico protocollo. Nel mondo PoS, la maggior parte delle criptovalute utilizza attualmente una combinazione di entrambi.

2.3 Proof of Authority (PoA)

La Proof of Authority (PoA) è un algoritmo di consenso basato sulla reputazione che introduce una soluzione pratica ed efficiente per i network blockchain (soprattutto quelli privati). Il termine è stato proposto nel 2017 dal co-fondatore ed ex-CTO di Ethereum Gavin Wood.
L'algoritmo di consenso PoA fa uso del valore delle identità. Ciò significa che i convalidatori dei blocchi mettono in stake la propria reputazione al posto delle monete. Di conseguenza, le blockchain PoA sono protette dai nodi di convalida che vengono selezionati arbitrariamente come entità affidabili.
Il modello Proof of Authority si basa su un numero limitato di convalidatori, fattore che lo rende un sistema altamente scalabile. I blocchi e le transazioni sono verificati da partecipanti pre-approvati, che fungono da moderatori del sistema.
L'algoritmo di consenso PoA può essere applicato in un gran numero di scenari ed è considerato un'opzione valida per le applicazioni logistiche. Per quanto riguarda le catene di fornitura, ad esempio, la PoA è ritenuta una soluzione efficace e adeguata.
Il modello Proof of Authority consente alle imprese di mantenere la propria privacy e allo stesso tempo avvalersi dei vantaggi della tecnologia blockchain. Microsoft Azure è un altro esempio di compagnia che applica la PoA. In poche parole, la piattaforma Azure fornisce soluzioni per network privati, con un sistema che non richiede una valuta nativa come il 'gas' di ether, dato che il network non ha bisogno di mining.

2.3.1 Di cosa ha bisogno la PoA

Sebbene le condizioni possano variare da sistema a sistema, l'algoritmo di consenso PoA dipende solitamente da:

- **Identità valide e affidabili**: i convalidatori devono confermare le proprie identità reali.
- **Difficoltà nel diventare un convalidatore**: un candidato deve essere disposto a investire denaro e mettere in gioco la propria reputazione. Un processo rigoroso riduce il rischio di selezionare convalidatori dubbi e incentiva un impegno a lungo termine.
- **Uno standard per l'approvazione dei convalidatori**: il metodo per selezionare convalidatori deve essere uguale per tutti i candidati.

2.3.2 Proof of Authority vs Proof of Stake

Alcuni considerano la PoA come una versione modificata della PoS, che fa uso dell'identità invece delle monete. A causa della natura decentralizzata di gran parte dei network blockchain, a volte la PoS non è adatta per certe attività e imprese. Al contrario, i sistemi PoA possono rappresentare una soluzione migliore per le blockchain private viste le prestazioni notevolmente migliori.

2.3.3 Critiche PoA

L'impressione del meccanismo PoA è che rinuncia alla decentralizzazione. Si potrebbe quindi dire che il modello introdotto da questo algoritmo di consenso è solo uno sforzo per rendere più efficienti i sistemi centralizzati. Sebbene questo renda la PoA una soluzione attraente per le grandi aziende con esigenze logistiche, suscita una certa esitazione - soprattutto nell'ambito delle criptovalute. I sistemi PoA offrono un'elevata capacità di elaborazione, ma la possibilità di censura e blacklisting mettono in dubbio la loro immutabilità.
Un'altra critica frequente riguarda le identità dei convalidatori PoA, le quali sono visibili a chiunque. La risposta a questo argomento è che solo individui stabiliti in grado di occupare questa posizione cercherebbero di diventare convalidatori (come partecipante noto al pubblico). Nonostante questo, conoscere le identità dei convalidatori potrebbe potenzialmente portare a manipolazione da parte di terzi. Per esempio, se un competitore vuole ostacolare un network basato sulla PoA, potrebbe influenzare convalidatori noti per farli agire in modo disonesto e compromettere il sistema dall'interno.