Criptovalute e algoritmi di consenso – parte 1

Author : Luca Dinardo

Date : 12 Marzo 2019

Da qualche anno a questa parte siamo costantemente bombardati di informazioni relative all'andamento economico delle principali criptovalute, tramite qualunque mezzo di comunicazione a disposizione dell'essere umano. Al contrario di quanto si è spesso portati a pensare, in modo superficiale ed errato, le criptovalute non rappresentano soltanto un mezzo per "guadagnare soldi facili" (affermazione che di per sé risulta già molto discutibile).

Sono importanti perché sono diventate, di fatto, **un elemento fondamentale nel processo di evoluzione del nostro mondo digitale**. E quello che spesso si dimentica è che l'aspetto tecnologico è il fattore principale che guida questa rivoluzione.

Le criptovalute sono uno strumento utilizzabile dagli utenti di tutto il mondo per lo scambio di "valore" in maniera istantanea, tramite un'infrastruttura decentralizzata che, sfruttando la rete internet (ma non solo), permette di non avere più delle singole entità centralizzate (ad esempio banche o governi) come autorità di controllo e gestione delle transazioni.

Ma questo, sul piano tecnologico, come è possibile? Com'è possibile che milioni di utenti possano coesistere in questo spazio virtuale e utilizzare le criptovalute per effettuare transazioni senza necessità di affidarsi a un'entità centrale?

Alla base di tutto, ciò che rende davvero una criptovaluta decentralizzata è **l'algoritmo di consenso** utilizzato per gestire e validare le transazioni: gli utenti si "accordano" secondo dei criteri di equità e seguono regole ben definite che consentono l'esecuzione, tramite l'utilizzo della tecnologia blockchain, di transazioni immutabili, definitive e impossibili da contraffare, "premiando" economicamente coloro che facciano un corretto utilizzo del network e penalizzando eventuali tentativi di abuso.

Algoritmi di consenso e Byzantine Fault Tolerance (BFT)

Un algoritmo di consenso deve poter risolvere quello che, in letteratura, è definito il problema dei generali bizantini [1]: deve esser possibile raggiungere un consenso "globale" in situazioni

in cui è possibile la presenza di errori (siano essi in buona o in cattiva fede) da parte delle entità coinvolte nella decisione. Il problema consiste nel trovare un accordo tra entità diverse, nel caso in cui siano presenti informazioni discordanti, allo scopo di mantenere intatta l'integrità, l'operatività e la consistenza della rete distribuita.

Proof Of Work, Proof Of Stake e gli altri algoritmi di consenso

Senza voler entrare, almeno per ora, troppo nel dettaglio tecnico, vengono di seguito descritti alcuni dei principali algoritmi di consenso utilizzati dalle più note criptovalute. Ad oggi, il più adottato è il cosiddetto "Proof Of Work", su cui Bitcoin prima, Ethereum e molte altre criptovalute dopo, sono basati.

Il concetto di Proof Of Work viene reso pubblico dapprima nel 1993 da Cynthia Dwork e Moni Naor e poi, nel 1999, da Markus Jakobsson. Nel **White Paper originale di Bitcoin** [2], pubblicato da un utente rimasto anonimo sotto lo pseudonimo di Satoshi Nakamoto, viene descritto il funzionamento dell'algoritmo di consenso e del network di Bitcoin. Nel documento si descrive la modalità di esecuzione e di approvazione delle transazioni effettuate all'interno della rete *peer-to-peer*, che avvengono senza la necessità di fare affidamento a un'entità centrale. Semplificando, il network di bitcoin si basa sul lavoro computazionale effettuato da alcuni nodi della rete che, per pubblicare nuovi blocchi di informazioni all'interno di un registro distribuito e verificare/validare le transazioni effettuate dai vari nodi del network, competono per risolvere un problema matematico con difficoltà sempre crescente, a fronte di una ricompensa economica. La combinazione di questi fattori porta all'assunto che il network sia intrinsecamente resistente a operazioni di "double-spending" da parte di nodi appartenenti alla rete, fintanto che questi non riescano a controllare almeno il 51% del totale dell'hash power impiegato da tutti i nodi partecipanti.

Ad oggi è possibile constatare come, nel corso dei primi 10 anni di vita di Bitcoin, **nessuno sia mai riuscito a comprometterne realmente la sicurezza in questo modo**.

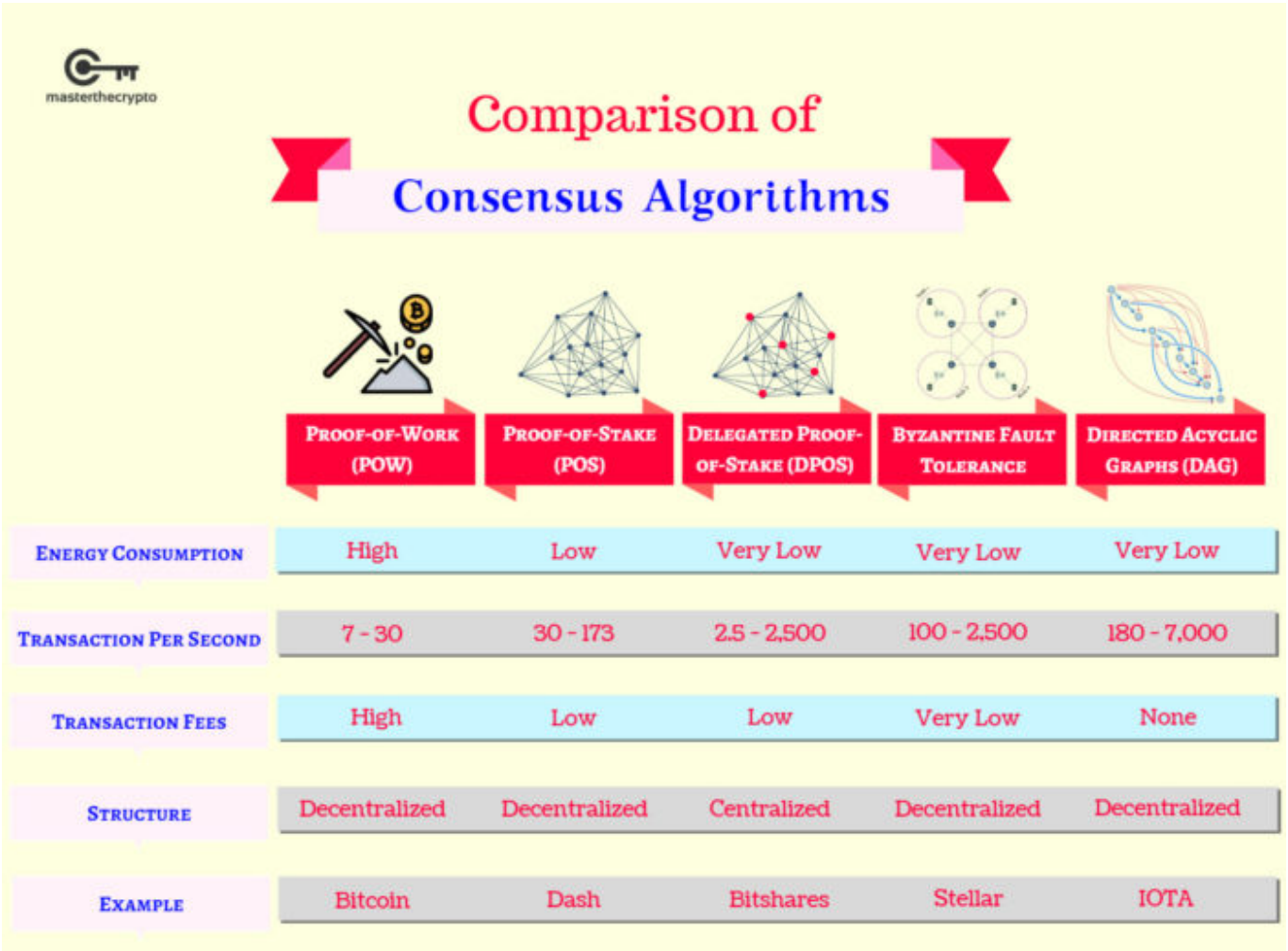
L'alternativa più nota al Proof Of Work **è rappresentata dal Proof Of Stake**, al quale Ethereum sta pianificando di passare in futuro, con l'applicazione dell'update denominato Casper [3].

Lo scopo primario, anche in questo caso, è validare le transazioni e raggiungere il consenso all'interno della rete ma, in questo caso, tale processo non viene effettuato tramite la risoluzione di problemi matematici e la generazione di nuove monete, assegnate come ricompensa ai miners. Con il PoS, il nodo preposto per la creazione del nuovo blocco di transazioni da pubblicare sul registro distribuito, viene scelto in modo deterministico sulla base dello *stake* (quantità di coins) "bloccato" e messo a disposizione per tale scopo.

Per fare un esempio concreto, se un nodo detiene e "blocca" 10 coins e un altro nodo ne blocca 100, quest'ultimo avrà 10x le possibilità di essere "eletto" dal network come creatore del successivo blocco di transazioni. La sua ricompensa sarà esclusivamente legata alle *fee* generate dalle transazioni effettuate sul network. Come detto, infatti, **non vi è alcuna nuova creazione di *coins***, che sono già tutte distribuite in origine, durante la fase di lancio del progetto e della criptovaluta.

Questo meccanismo di consenso risulta esser decisamente più economico rispetto al Proof Of Work, in quanto permette di risparmiare sui costi dell'hardware e dell'elettricità necessaria per alimentare la rete. In compenso però, in determinate condizioni, tale meccanismo potrebbe finire per favorire coloro che posseggono già grossi capitali, aumentandone le possibilità di vincere le varie assegnazioni con stake sempre più grossi e quindi, alla lunga, potenzialmente creare un fattore di centralizzazione del network su un numero ristretto di entità. Costringere i nodi a mantenere bloccate le *coin* (come definito nelle versioni più recenti di PoS), d'altra parte, permette di avere una garanzia sul rispetto delle regole dei vari nodi ed evita attacchi di tipo "nothing at stake" [4]. Come deterrente per comportamenti scorretti, da protocollo, è definito che i nodi possano veder perso l'intero stake messo a disposizione, qualora venga accertato abbiano intrapreso attività non lecite.

Diversi **altri algoritmi ibridi** e con logiche diverse sono nati nel corso del tempo. Alcuni progetti di criptovalute hanno optato per l'utilizzo di algoritmi di consenso PoW ASIC-based, altri GPU-based, altri hanno preferito optare per il Delegated Proof Of Stake (un numero limitato di nodi scelti in base allo stake a disposizione ed al "comportamento" tenuto nel corso del tempo) o altri meccanismi ibridi PoW-PoS, etc. Sono anche nati progetti che stanno provando ad utilizzare meccanismi di consenso completamente diversi, come il Proof Of Authority (PoA) , Proof Of Weight (PoWeight) , i Directed Acyclic Graphs (DAGs) etc.



Nessuna di queste soluzioni è perfetta - ci sono pregi e difetti in ognuna di esse - ma, sintetizzando, possiamo affermare che, per essere considerato un buon meccanismo di consenso, questo deve poter garantire a una criptovaluta le seguenti caratteristiche:

- **Decentralizzazione**: per evitare attacchi di 51% (o simili) e per garantire l'assenza di entità centrali che possano controllare le transazioni.
- **Sicurezza**: l'algoritmo deve essere resistente a eventuali attacchi di varia natura che possano essere intrapresi contro la rete.
- ***Fault Tolerance***: in qualunque caso di fault di uno o più nodi, la rete deve continuare ad essere in grado di funzionare correttamente.
- **Incentivi alla partecipazione**: devono esser presenti degli incentivi (economici) forti che spingano gli utenti a comportarsi in maniera corretta piuttosto che in maniera illecita.

Riferimenti bibliografici

[1] "The Byzantine Generals Problem" LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE SRI International - https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.

[2] "Bitcoin: A Peer-to-Peer Electronic Cash System" Satoshi Nakamoto - https://bitcoin.org/bitcoin.pdf.

[3] "Casper: What Will the Upgrade Bring to the Ethereum's Network?" - https://cointelegraph.com/news/casper-what-is-known-about-the-new-ethereums-network-upgrade.

[4] "Understanding Proof of Stake: The Nothing at Stake Theory" - Julian Martinez https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027.

Articolo a cura di **Luca Dinardo**