La forza dei numeri

Bitcoin è costruito intorno a importanti funzioni matematiche, che si legano a numeri tanto grandi da superare di gran lunga i trilioni cui è tanto legata anche la finanza.

Thomas Zara, Managing Partner di Arkadia Digital Advisory.

Nel mondo Bitcoin vi sono diversi motti diventati famosi se non addirittura virali. I più mainstream sono senz'altro: *Don't Trust... verify!*, ossia: *Non ti fidare verifica!* (è tutto su blockchain) e *Not your keys... not your coins!*, che sta a significare: *Se non sei in possesso delle tue chiavi private (depositati sugli Exchanges), i bitcoin non sono veramente tuoi!*

Ce n'è un altro però, meno noto e di derivazione latina, che approfondendo lo studio di Bitcoin cattura l'attenzione, *Vires in numeris*, ossia *La forza nei numeri.*

Bitcoin è matematica ed è costruito sui numeri grandi e sull'impossibilità teorica di indovinarli. Tali numeri sono molti ordini di grandezza superiori a quanto si sia abituati anche solo ad immaginare. Capirne la grandezza è essenziale per comprendere l'essenza. Milioni, miliardi o trilioni, sono i numeri più grandi del sentire comune. Del resto, un miliardo di secondi corrisponde a circa 32 anni.

Bitcoin utilizza la matematica e la crittografia per rimuovere la necessità di doversi affidare ad autorità e istituzioni centrali. Le parti effettuano transazioni tra di loro, in modalità peer to peer, senza bisogno di fidarsi perché funzioni, matematiche ne garantiscono autenticità e immutabilità, nonché l'impossibilità di effettuare double spending.

Il numero di indirizzi che Bitcoin è in grado di generare è pari a 2^256, un numero talmente enorme che è paragonabile al numero di atomi che compongono l'universo. Il protocollo Bitcoin utilizza, tra le altre, la funzione di hashing "Ssa256", un algoritmo crittografico non invertibile per garantire l'integrità delle informazioni memorizzate in un blocco.

Il termine *hash*, significa 'sminuzzare' e la funzione di hash fa proprio questo, ossia trasforma dati e testo, in una stringa alfanumerica con lunghezza predefinita. Per 'non invertibile' si intende invece che da un input si può ottenere un output, ma dal medesimo output è impossibile a risalire all'input originario (unidirezionalità).

Quando un miner propone un nuovo blocco (con un insieme di nuove transazioni effettuate) da inserire nella blockchain, affinché esso venga accettato dai nodi validatori, deve provare di aver svolto un lavoro risolvendo un problema matematico proposto, che ha una complessità variabile a seconda della 'difficoltà' che è direttamente proporzionale, all'aumentare della potenza di calcolo (hashpower) presente nella rete di mining.

> «Il numero di indirizzi che Bitcoin è in grado di generare è pari a 2^256, un numero talmente enorme che è paragonabile al numero di atomi che compongono l'universo. Tra le altre funzioni utilizza anche l'altrettanto chiave hashing "Ssa256"»

Il testo complessivo di questo blocco (lettere e numeri che lo compongono), è composto dall'hash del blocco precedente, dall'hash delle nuove transazioni raccolte dal miner e da un numero casuale.

Cambiando a ogni tentativo il numero casuale, il miner genera ogni volta un hash diverso ed effettua quest'operazione fino a quando lui, o un altro miner prima di lui, non genera un hash che sia inferiore alla difficoltà prevista dal protocollo.

La 'Proof of work' consiste pertanto nella ricerca di un valore che, una volta sottoposto ad hash, restituisca un altro hash che inizi con un certo numero di zero bit. Il lavoro di calcolo richiesto cresce in maniera esponenziale all'aumentare del numero di zero bit richiesti (1, 2, 3...) e quindi al coefficiente di difficoltà della rete. Una volta individuato tale numero, la dovuta verifica da parte di ogni altro partecipante alla rete richiede pochi millisecondi, eseguendo un unico hash.

Fa sorridere pensare come, la metafora per antonomasia, ossia di 'trovare un ago in un pagliaio', si adatti perfettamente.

Vi è però un'evidente asimmetria tra il trovare la soluzione richiesta e il verificarne la correttezza. Trovare un ago in un pagliaio è chiaramente difficile e richiede molto 'lavoro' (qui potenza computazionale) ma una volta trovato, verificare che l'ago non sia una pagliuzza è molto facile.

La blockchain di bitcoin rappresenta pertanto un sistema di convalida indipendente e decentralizzato, il consenso su cui i nodi della rete convergono permette anche di avere una marcatura temporale degli eventi (time stamping). Il consenso, è il modo in cui Bitcoin esprime il tempo.

Il sistema degli incentivi, che fa leva sull'interesse economico personale dei miner, influenza l'ordine univoco in cui tali eventi si sono verificati, che sono quindi inseriti nei blocchi, indipendentemente da quando sono avvenute le transazioni. Il tutto avviene in maniera decentralizzata dove chiunque può minare o convalidare un blocco e decidere di andarsene.

Sovranità monetaria decentralizzata attraverso la matematica...