Blockchain III: la proof-of-work e i suoi limiti

DI MAURIZIO GIAFFREDO
09/10/2025

BLOCKCHAIN PROOF-OF-WORK QUINTO ANNO SECONDO BIENNIO

ITE AFM-RIM , SCIENTIFICO S.A. , TE SIA , TT INFORMATICA

La **proof-of-work** è il meccanismo di consenso che regola l'aggiunta dei blocchi nella blockchain di Bitcoin. I **miner** competono nella risoluzione di problemi matematici complessi, garantendo sicurezza e integrità della rete in cambio di una ricompensa.

Tuttavia, questo sistema presenta limiti significativi: alto consumo energetico, lentezza nelle transazioni e rischio di centralizzazione dovuto alla concentrazione della potenza di calcolo. Inoltre, l'energia impiegata genera un notevole impatto ambientale. Per ovviare a questi problemi, si stanno diffondendo modelli alternativi come la **proof-of-stake**, più sostenibili e meno dispendiosi

Autori

MAURIZIO GIAFFREDO

In un **recente articolo** e poi in un **articolo successivo**, abbiamo presentato alcune caratteristiche di base di una ***blockchain*** e cercato di affrontare il tema della **sicurezza** sia nei suoi aspetti **crittografici** che in quelli di **integrità dei blocchi**, facendo riferimento al funzionamento di **Bitcoin**.

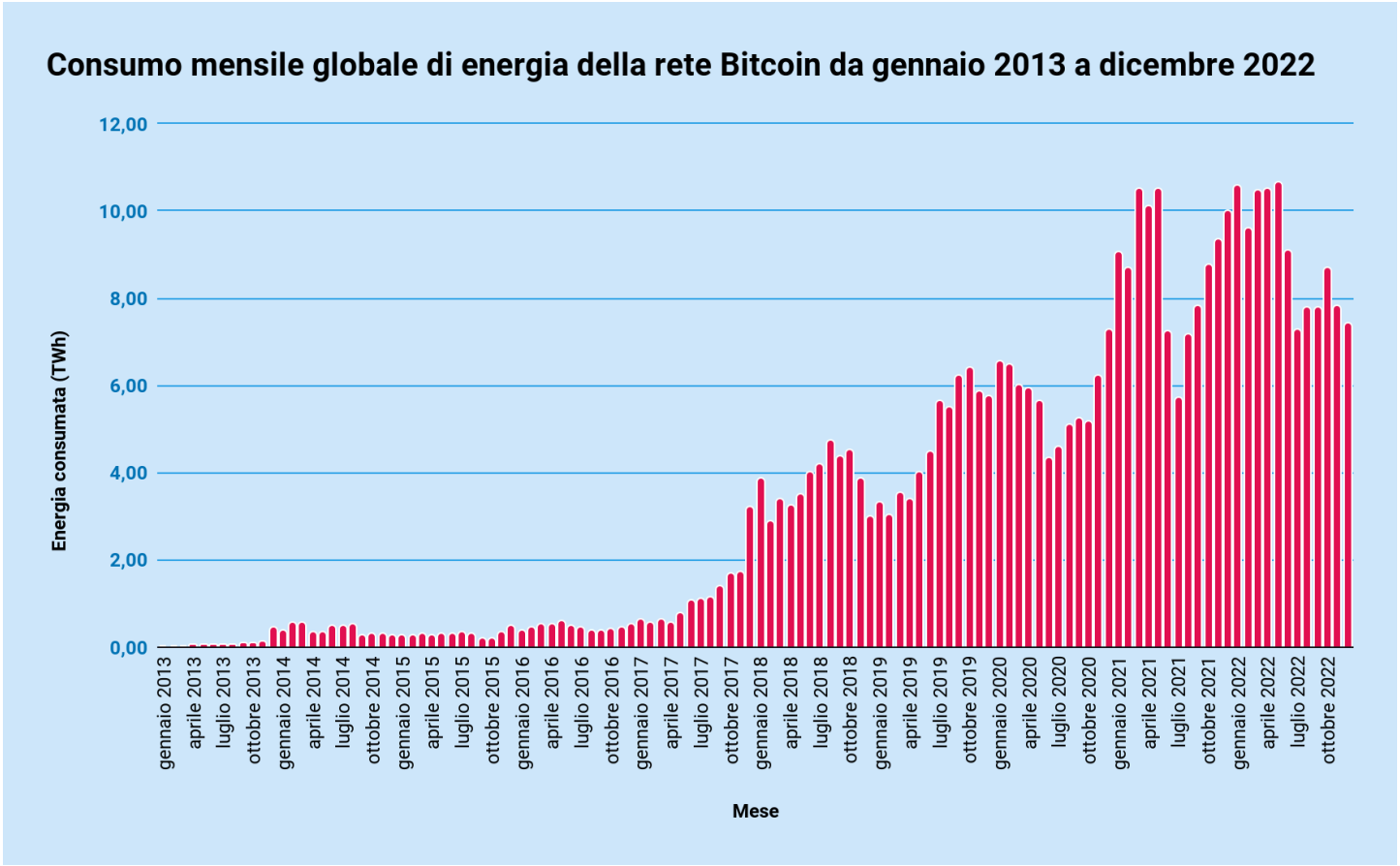
In questo articolo concludiamo il discorso, avendo in sospeso da discutere il **meccanismo di consenso** per l'aggiunta dei blocchi.

MINER E PROOF-OF-WORK

Come già detto, in una rete distribuita come quella costituita dagli utenti di una *blockchain*, manca un'autorità centrale che certifichi la validità delle operazioni. Si rende dunque necessario disporre di un **meccanismo intrinseco** che regoli i potenziali conflitti per l'inserimento di nuovi blocchi alla catena.

Nel caso di Bitcoin, i nodi deputati a questa operazione sono i cosiddetti ***miner***. Per vedere accettato un blocco da loro composto, i *miner* competono nella risoluzione di un problema matematico che ha un **elevato costo computazionale**: aggiungere un numero alla fine del blocco in modo tale che il suo codice hash inizi con una certa quantità prestabilita di zeri. Il successo in questa operazione costituisce la cosiddetta ***proof-of-work*** (letteralmente: "prova di lavoro"), per la quale i *miner* ricevono una piccola ricompensa in caso di accettazione del blocco.

Questo consente una **protezione della *blockchain* dagli attacchi del tipo *DoS*** (*Denial of Service*), che risultano inefficaci, ma anche una **maggiore equità** tra i nodi della rete: tutto ciò che conta è la capacità di calcolo a disposizione, non la quantità di Bitcoin che si possiede.



*Un grafico che riporta il consumo globale di energia della rete Bitcoin negli ultimi dieci anni (fonte: **CBECI**). I consumi annuali di elettricità della rete Bitcoin sono maggiori di quelli di interi paesi (come ad esempio la Finlandia).*

NON È TUTTO ORO QUELLO CHE LUCCICA

La *proof-of-work* presenta diversi svantaggi:

- è teoricamente **vulnerabile ad attacchi al 51%**, ovvero a monopolizzazioni della rete da parte di soggetti che potrebbero controllare la maggioranza delle risorse di calcolo e dunque modificare i blocchi senza aver bisogno del consenso degli altri;
- **rallenta moltissimo l'aggiunta di transazioni** (si consideri che la rete Bitcoin registra circa 7 transazioni al secondo, contro le 1700 della rete VISA);
- conferisce **maggiore potere a chi ha a disposizione una grossa potenza di calcolo e hardware ad hoc**, dunque favorisce chi ha la possibilità di fare grossi investimenti;
- i calcoli fatti per la *proof-of-work* non sono riutilizzabili per altri scopi (scientifici, economici, ecc.) e dunque costituiscono un **grosso spreco**;
- il **consumo di energia** causato dal mining è alto e si traduce in un **importante costo economico** oltre che in un **elevato costo ambientale**; un **report della casa bianca** stima che le criptovalute siano responsabili dello **0,3% delle emissioni**

annuali globali di gas serra.

Per cercare di superare questi problemi, negli anni si sono proposti meccanismi di consenso alternativi. I meccanismi più quotati oggi sono la ***proof-of-stake*** e la ***delegated proof-of-stake***, sulle quali alcuni restano comunque scettici.

Ma questa è un'altra storia, che forse racconteremo in futuro.