Blockchain II: garantire la sicurezza

DI MAURIZIO GIAFFREDO
09/10/2025

BLOCKCHAIN SICUREZZA QUINTO ANNO SECONDO BIENNIO

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

La sicurezza della **blockchain** si basa su due principi chiave: la **crittografia a chiave pubblica/privata** e l'**integrità dei blocchi**. Ogni utente firma le proprie transazioni con una chiave privata, mentre la chiave pubblica consente di verificarne l'autenticità.

Ogni blocco, identificato da un codice **hash**, contiene l'impronta digitale del precedente, formando una catena inalterabile. Anche una minima modifica cambierebbe l'intero hash, rendendo evidente ogni tentativo di manomissione. Questo sistema distribuito rende le blockchain sicure e trasparenti, ma richiede potenti risorse di calcolo per mantenerne l'affidabilità.

Autori

MAURIZIO GIAFFREDO

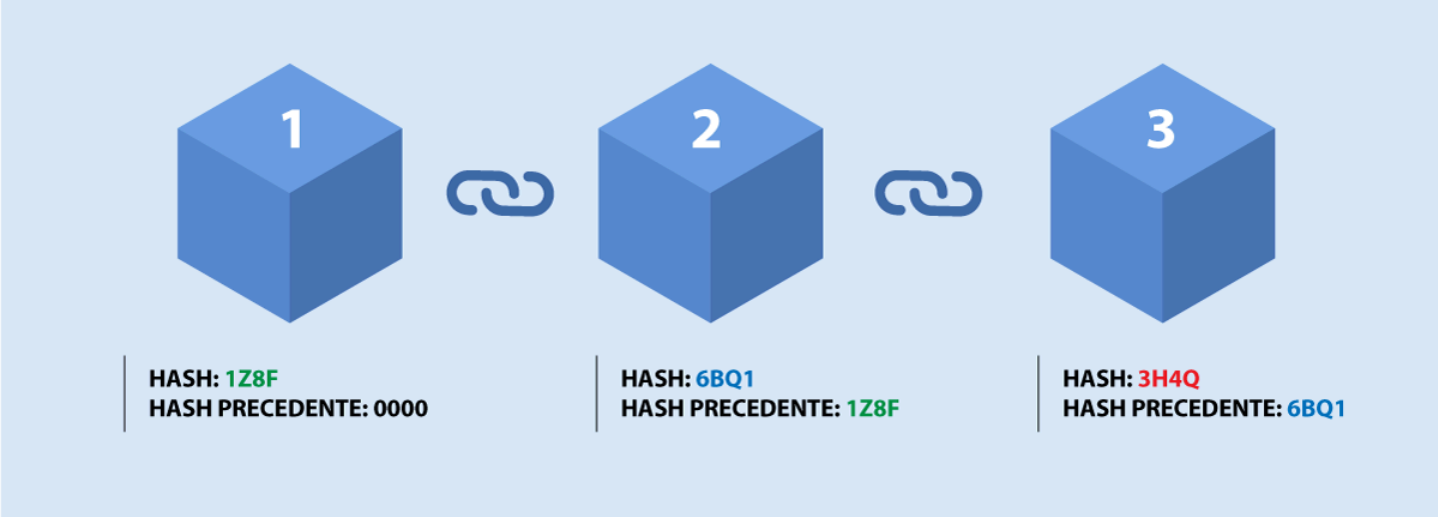
In un **recente articolo** abbiamo presentato alcune caratteristiche di base di una ***blockchain***. In questo proseguiamo idealmente il discorso e ci concentriamo su come si possa garantire la **sicurezza** delle *blockchain*, riferendoci in particolare a quella di **Bitcoin** ma premettendo che le opzioni possibili sono diverse.

CRITTOGRAFIA A CHIAVE PUBBLICA/PRIVATA

La sicurezza delle operazioni elencate nei blocchi di una *blockchain* è tendenzialmente basata su un **sistema crittografico asimmetrico**: ciascun utente inserisce le proprie transazioni nei blocchi della catena, ordinandole e poi firmandole attraverso la propria **chiave privata** (che resta segreta, in possesso del firmatario), mentre l'autenticità delle operazioni può essere verificata utilizzando la **chiave pubblica** del firmatario di una certa operazione (che è nota a tutti gli utenti della blockchain). Questo meccanismo consente pertanto di garantire l'**autenticità dell'autore** di ciascuna transazione.

INTEGRITÀ DEI BLOCCHI

Il meccanismo di identificazione e connessione dei blocchi garantisce invece la loro **integrità**: ciascuno di essi ha una propria "impronta digitale" (che si chiama **hash** ed è utilizzata come identificatore) e **"punta" al blocco che lo precede nella catena**, memorizzandone proprio l'impronta digitale stessa.



Nell'immagine, una rappresentazione dei blocchi della blockchain e del sistema di puntamento.

L'hash associato a ogni blocco si può determinare grazie a un'apposita **funzione crittografica di hash**, ovvero una funzione che preso in input il contenuto di un blocco genera rapidamente un output di lunghezza fissa, che cambia completamente se viene effettuata anche una sola minima variazione al contenuto del blocco. Inoltre, la funzione deve essere anche difficile da invertire, nel senso che deve risultare **computazionalmente intrattabile** il problema di risalire a un input che abbia generato un certo output.

Con questo stratagemma, è facile **verificare se il puntamento dei blocchi è corretto** e se i blocchi subiscono variazioni nei contenuti o nell'ordine, rendendo sostanzialmente **impossibile modificare blocchi già inseriti** nella blockchain (se non altro, senza il consenso della maggior parte degli utenti).

Ci resta ancora da capire come funziona il **meccanismo di consenso** per l'aggiunta di blocchi validi e di considerare l'**impatto ambientale** che ha avuto la nascita di Bitcoin. Di questo, però, tratteremo nel prossimo articolo.