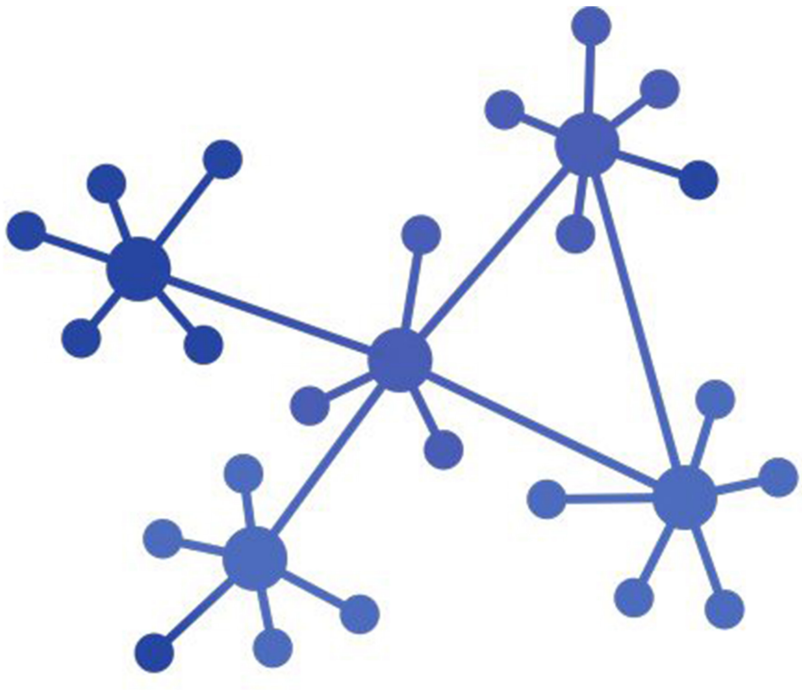
Blockchain I: la tecnologia dietro alle criptovalute

DI MAURIZIO GIAFFREDO
09/10/2025

BLOCKCHAIN CRIPTOVALUTE QUINTO ANNO SECONDO BIENNIO

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



La sicurezza delle blockchain, come quella di **Bitcoin**, si basa su due pilastri: **crittografia asimmetrica** e **integrità dei blocchi**. Ogni utente firma le proprie transazioni con una chiave privata, mentre chiunque può verificarne l'autenticità con la chiave pubblica.

I blocchi sono collegati tra loro tramite una funzione di **hash crittografico**, che genera un'identificazione univoca e cambia completamente al minimo intervento, rendendo praticamente impossibili modifiche non autorizzate. Questo sistema garantisce tracciabilità e sicurezza dei dati, ponendo le basi per la fiducia nelle reti distribuite.

Autori

MAURIZIO GIAFFREDO

Sono oramai diversi anni che si parla di **criptovalute**: il **Bitcoin**, la cui invenzione ha dato una grande spinta a tutto il settore, risale al 2009. Al cuore del loro funzionamento c'è spesso una ***blockchain***, un'architettura che può essere utilizzata in diversi contesti. In questo primo articolo ne presentiamo alcune caratteristiche.

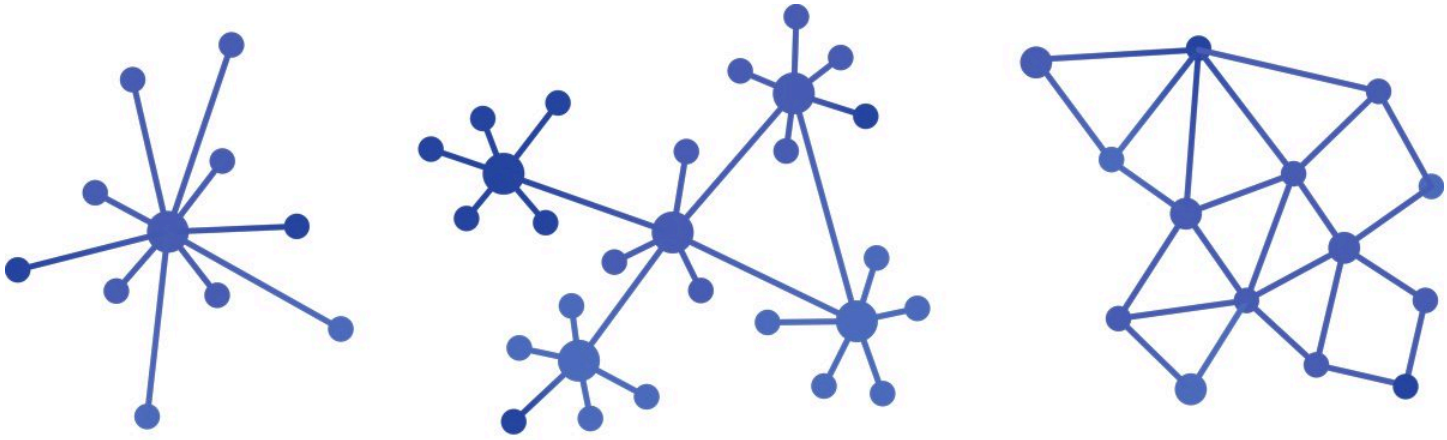
COS'È UNA BLOCKCHAIN?

L'esigenza a cui risponde una *blockchain* è quella di disporre di un **registro digitale** (nel caso delle criptovalute è l'elenco delle transazioni di denaro) che sia contemporaneamente **distribuito** e **immutabile**: per un singolo utente non deve essere possibile modificare o eliminare le voci del registro, ma in qualsiasi momento deve essere possibile leggerle e eventualmente aggiungerne alcune in coda. In questa maniera tutte le operazioni effettuate sul registro digitale sono **tracciabili**, anche se viene sempre garantito l'**anonimato** degli utenti.

Per avere una condivisione agevole del registro digitale conviene allora suddividerlo in una serie di parti, dette **blocchi**, che vengono ordinate in un'unica **catena**: la *blockchain*, appunto.

DECENTRAMENTO E DISTRIBUZIONE

Ciascun utente possiede una copia di tutti i blocchi della catena, che sono condivisi in un'apposita **rete P2P** (una rete i cui nodi hanno tutti pari ruolo). Un vantaggio immediato nel **non avere un'entità centrale** è la maggiore **trasparenza**. Inoltre, l'elevata ridondanza di una *blockchain* consente di **evitare la perdita di informazioni** e dà a chiunque accesso pressoché istantaneo a una copia dell'intero registro digitale.



Una rappresentazione grafica di alcune tipologie di struttura di una rete. Da sinistra: una rete centralizzata, una rete decentralizzata e una rete distribuita.

Dalla struttura decentrata discendono anche vantaggi più tecnici: **non si risente infatti dei malfunzionamenti di un particolare nodo**, vanificando quindi eventuali **attacchi malevoli** di tipo **DDoS** (*distributed denial-of-service*), che mirano a sovraccaricare i nodi di una rete mettendoli fuori servizio.

OLTRE LE CRIPTOVALUTE

Le criptovalute sono solo uno dei campi in cui si è utilizzata una *blockchain*, ma non è certamente l'unico. Un settore in rapida evoluzione è, solo per dirne uno, quello degli **NFT** (*non-fungible token*), utilizzati per certificare **autenticità e proprietà** e quindi impiegati, per esempio, principalmente per la **tutela della proprietà intellettuale** e del **copyright**.

Nel prossimo articolo capiremo meglio come garantire la sicurezza e come il funzionamento di una *blockchain* abbia spesso un costo elevato, sia computazionale che ambientale.