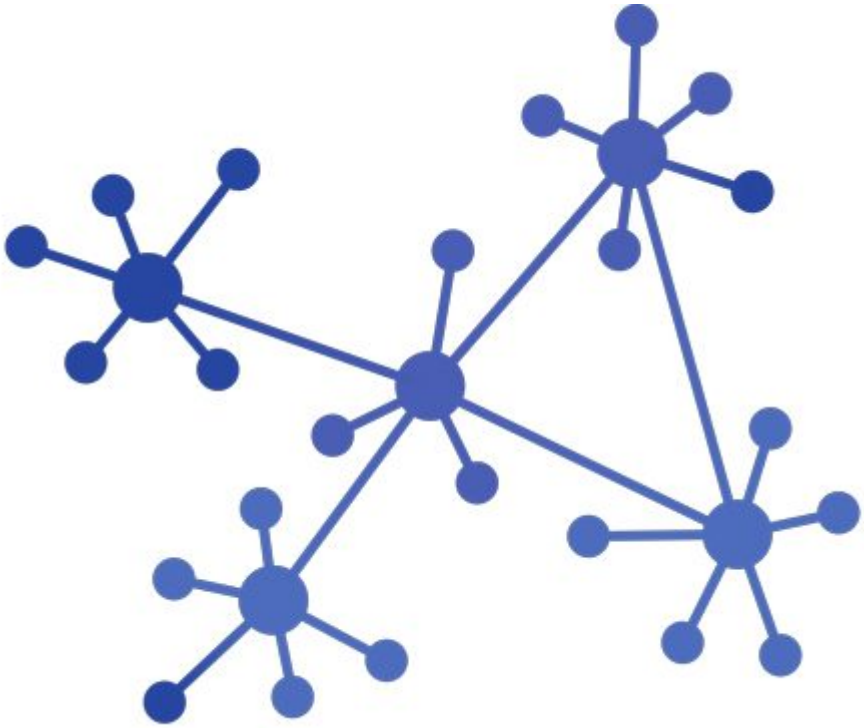
News



Blockchain I: la tecnologia dietro alle criptovalute

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.

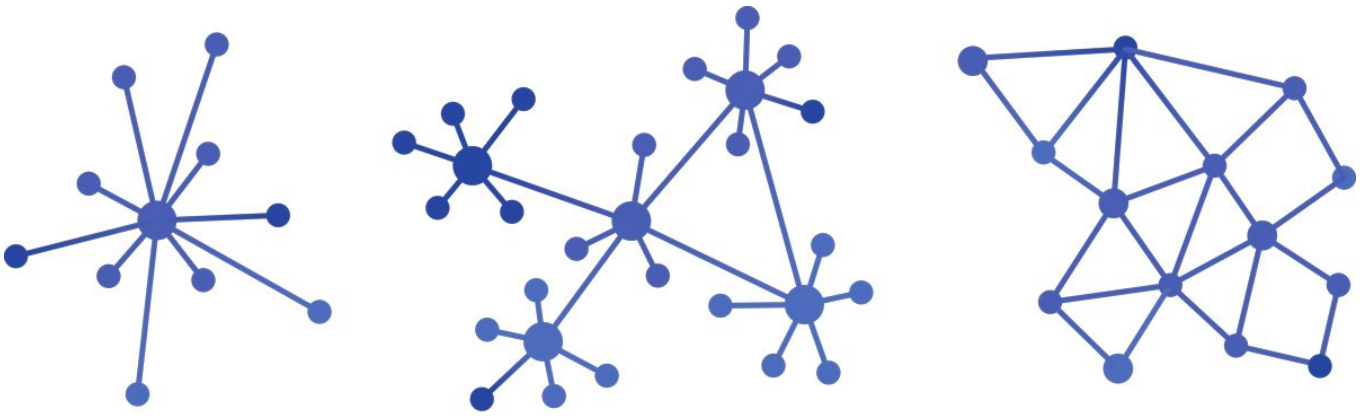
Per avere una condivisione agevole del registro digitale conviene allora suddividerlo in una serie di parti, dette **blocchi**, che vengono ordinate in un'unica **catena**: la blockchain, appunto.

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.

Rizzoli EDUCATION

News



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.

APPROFONDIMENTI

- But how does bitcoin actually work?
  Un video di 3Blue1Brown che illustra come funzionino le criptovalute, compreso il meccanismo delle *blockchain*.
- Tutto quello che faremo con la blockchain
  Un articolo del 2018 in cui si presentano alcune possibili applicazioni delle *blockchain*.