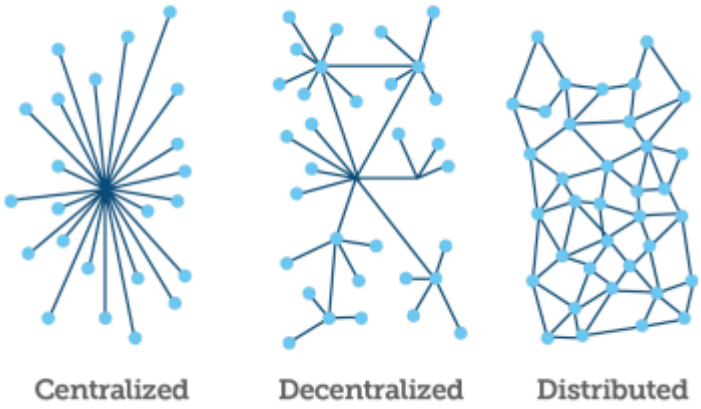
La BlockChain (catena di blocchi) è un registro informatico aperto.

Ogni utente che partecipa al registro è connesso con tutti gli altri e detiene una copia di una sorta di libro mastro, chiamato blockchain. Nella blockchain sono registrate tutte le transazioni di tutti gli utenti di sempre, da quando quella catena è stata usata per la prima volta. Per far ciò la blockchain è aperta e consultabile da chiunque la utilizzi.

È autosufficiente, decentralizzata, non richiede un'autorità che ne approvi le operazioni perché sono le sue stesse operazioni, per il modo in cui sono fatte, a essere autolegittimate.
Ciò è possibile perché ogni singola transazione risiede all'interno di una catena di blocchi che dall'ultima risale alla prima assoluta, e perché ogni utente della catena è sempre a conoscenza di tutte le altre operazioni che vengono fatte dagli altri utenti (con i Bitcoin, per esempio, questo serve a evitare che qualcuno usi lo stesso Bitcoin per pagare due cose diverse).



Ogni transazione sulla catena genera un blocco che a sua volta suggerisce un nodo a cui agganciare il prossimo blocco (la prossima transazione). Ogni modifica di un blocco, che non sia una transazione, ha ripercussioni su tutti i blocchi precedenti, distruggendo così la stessa catena. Non si può manomettere una cosa del genere.

Il primo sistema a "blocchi di hash" risale al 1991 ma il tipo più utilizzato oggi è quello descritto e realizzato da Satoshi Nakamoto, lo pseudonimo dietro l'inventore (o gli inventori) del Bitcoin, ideato nel 2008 in un libro bianco e implementato l'anno dopo.
vedi anche: Cosa sono i Bitcoin