Bitcoin e criptovalute

Cos’è la criptovaluta?

E’ un’unità di valore digitale movimentata on line

Criptovaluta → Crittografia che gioca un ruolo fondamentale per garantire sicurezza, immutabilità

La Blokchain è l’infrastruttura sulla quale si muove la criptovaluta

Fornisce sicurezza e decentralizzazione alla criptovaluta

Impedisce la contraffazione (crittografia) e il doble spending (poter spendere la stessa unità di valore più di una volta due volte)

E’ open source ossia è un protocollo chiunque può provare a sviluppare qualcosa.

Sistema centralizzato

- Prevede intermediari finanziari (banca, circuito della carta di credito, paypall ecc)
  - Es. Se devo fare un bonifico a qualcuno cosa succede? Inserisco sull'online banking la di disposizione del bonifico, la banca verifica e lo approva, lo manda all'altra banca che a sua volta lo approva e lo accredita sul conto della persona cui ho mandato il bonifico.

Approvazione della mia banca

Approvazione della sua banca

Tempo e costi e se ci sono dei disservizi di sistema non posso effettuare l'operazione.
Se effettuo un cross border (cambio della valuta) → ulteriori costi

SISTEMA INEFFICIENTE

Sistema decentralizzato

Insieme di nodi distribuiti nel mondo;

Noi comunicando con quei nodi (rete bitcoin- protocollo bitcoin) inviamo la transazione, il protocollo lo valida ed arriva direttamente all'altra persona senza istituti finanziari e senza conti bancari

I bitcoin sono di mia proprietà non devo chiedere a nessuna banca l'autorizzazione di poterli usare

Vantaggi di un sistema decentralizzato

- Tempi brevi;
- Minori costi non ci sono intermediari ma solo il network;
- Sempre fruibile perché per determinati nodi off line ce ne saranno altri on line tramite i quali posso effettuare le mie operazioni;
- E' Bordeless ossia se la transazione la mando in America,in Cina o nel paese accanto al mio non cambia nulla sono sempre bitcoin
- Non dobbiamo chiedere il permesso a nessuno
- E' sicuro grazie all'uso della crittografia

Blockchain

E’ un **registro distribuito** su vari nodi;

Ogni nodo (computer) eseguono un software che le collega con il network bitcoin;

Ogni nodo possiede tutto lo storico della Blockchain (dalla nascita dei bitcoin ad oggi) a seconda della categoria di nodi

Se nella Blockchain mancano 100 nodi ci devono essere dei nodi che possiedono lo storico delle transazioni

Le nuove transazioni vengono sincronizzate in tempo reale

Ogni nodo può validare la transazione

Consenso ditribuito → se ho i bitcoin che occorrono per la transazione non sono un tuo conoscente ma validi la transazione

Blockchain

- La blockchain è composta da moltissimi nodi non ad per es. 5 poiché sarebbe un sistema quasi centralizzato;

- Deve essere **trasparente** ossia tutti possono leggere quello che c'è scritto dentro (vedo un adress quale transazione ha fatto). **Immutabile** ossia la mia transazione non può esserere variata da nessun altro

Cos’è il Bitcoin

E’ la prima criptovaluta creata, la più sicura e la più decentralizzata.

Creata da Satoshi Nakamoto (nessuno sa chi e cosa sia) nel 2008 e non ha un capo

Nasce in piena crisi economica nel periodo dove le banche rischiavano la bancarotta;

Nasce il alternativa al denaro **FIAT** che è imposto e controllato da politiche monetarie al contrario il bitcoin è controllato da un algoritmo, dalla decentralizzazione ossia dalla community

Come funziona Bitcoin?

Occorre un wallet per interagire ossia un software che mi permette di ricevere, inviare e conservare bitcoin;

Questo viene permesso tramite l'utilizzo di due chiavi una **CHIAVE PUBBLICA** e la **CHIAVE PRIVATA**

Il wallet va pensato non come un portafoglio che contiene del denaro ma un contenitore di chiavi che mi permette di ricevere, conservare ed inviare bitcoin;

La chiave pubblica è ricavabile dalla chiave privata tramite un algoritmo crittografico **ECDSA** Crittografia a chiave ellittica;

Se all'algoritmo fornisco la chiave privata lui mi restituisce la chiave pubblica e non il contrario.

Come funziona Bitcoin?

Se voglio ricevere bitcoin devo dare a terzi la mia chiave pubblica ossia l'address che è derivato dalla chiave pubblica

Chi ha la chiave pubblica non può spendere i miei bitcoin perché non ha la mia chiave privata

La chiave privata va custodia

Non si può craccare un wallet ossia non posso arrivare alla chiave privata

Esempio di transazione con Bitcoin

- Ricevo Bitcoin sulla mia chiave pubblica;
- Spendo i miei bitcoin sulla chiave privata;
- Il network controlla che tu abbia realmente i bitcoin che vorresti spendere (controllano lo storico);
- Se sono in possesso dei bitcoin richiesti transazione ok altrimenti ko;
- Una volta inviata la transazione va in coda nella Blokchain;
- Quando arriva il mio turno finisco in un blocco, il mio blocco viene validato, viene reso immutabile e propagato agli altri nodi della rete

Cosa da valore ai Bitcoin?

- Lo utilizzo perché è sicuro, non utilizza intermediari, è nativo online e Bordeless;
- E’ una riserva di valore digitale e non materiale;
- Non devo pagare nessuno affinchè mi conservi i bitcoin;
- Strumento finanziario sul quale investire creano domanda e portano via liquidità;
- Il valore del Bitcoin dipende dal rapporto tra domanda e offerta di monete sul mercato: maggiore è la domanda di mercato a parità di offerta totale, più alto sarà il suo valore e quindi il suo prezzo. Viceversa, nel caso di minore domanda, il suo valore diminuirà. Il valore del Bitcoin dipende solo dal mercato
- Alcune piattaforme per comprare e vendere bitcoin sono per es. Coinbase, Kraken, Bitstamp e Bitfinex