**Tecnologie di blockchain**

**lezione 2**

Ripasso lezione 1

Concetti: registro, blockchain, funzioni hash; (P2P)algoritmo gossip, Merkle Tree

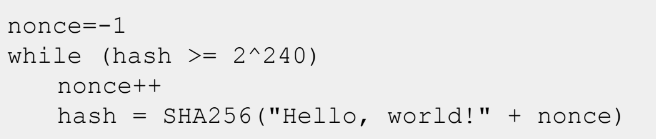
**Algoritmo di consenso**

**Proof of Work (PoW):** operazione/metodo computazionalmente difficile da risolvere,

**Nonce:** esempio di PoW, valore da concatenare all’input per ottenere hash < target (fattibile in maniera incrementale)

se è risolto problema e premiato (concorrenza tra miner nel mondo)

es di pow input=”Hello, World".



il target è il valore 2^240 adesso

il lvl difficoltà è resettato da BTC ogni 2016 blocchi(2 settimane), per tenere il tempo di creazione di un blocco ogni 10 min

**Miner:**  nodi che risolvono i PoW, risolto = ricompensa, costa energia e componenti

es bitmain (NB poolmining)

**Concetti di crittografia**

Per garantire l’autenticità e il non ripudio dei dati memorizzati in una blockchain si utilizza la crittografia a chiave pubblica

Ogni utente genera una coppia di chiavi: privata e pubblica

La crittografia a chiave pubblica può essere utilizzata sia per proteggere (cifrare) che per autenticare informazioni (firmare)

**Firma digitale**

La chiave privata viene utilizzata per firmare un dato

La chiave pubblica viene utilizzata per verificare la firma

In Bitcoin, un indirizzo è calcolato con l’hash della chiave pubblica, in particolare: *ripemd160(SHA256(Public-key))*

**Curve ellittiche:** funzione usata per controllo crittografia

da num reali a numeri finiti si fa con **crittografia ellittica,** si da uso di algoritmi di firma digitale che usano curve ellittiche (es ECDSA per transazioni)

curva + usata è la Secp256k1

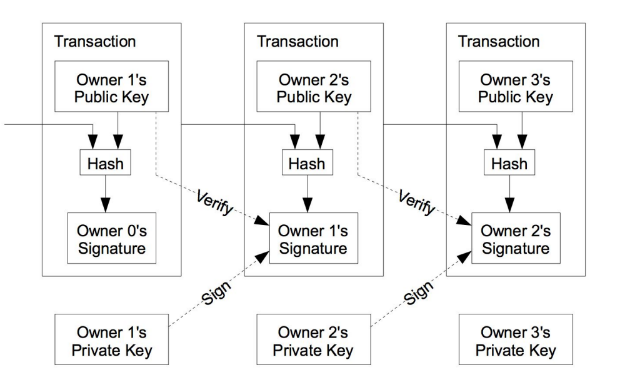
le curve sono di tipo simmetrico(rif alla somma di due punti) check grafico

formula: ***y^2 = x^3+ ax + b***

**sicurezza ECC:** Avendo definito la somma di due punti è possibile chiedersi il seguente problema: dati due punti P e Q di una curva ellittica trovare il numero intero k tale che P=Q∗k

è computazionalmente difficile (tempi umani lunghi), su questo si basa la sicurezza dei sistemi ECC

**Firma delle transazioni**

****