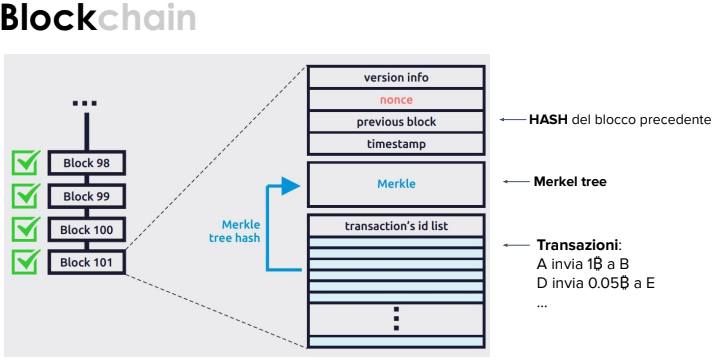
**Lezione 24/05/2024**

**Concetti di economia e finanza decentralizzata**

considera lez precedente



**Merkel tree:** insieme delle transazioni nel blocco

**Hash:** funzione non invertibile, + usata è sha256 (da 256 bit)

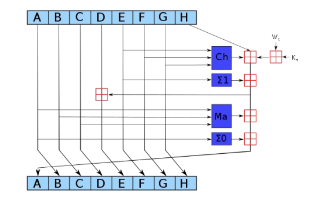
come detto da lezione precedente la funzione hash deve garantire la

**Non invertibilità:** l’algoritmo impiega troppo tempo a decodificare**,**

**Resistenza debole alle collisioni:** hash sono finiti, l’input indefinito. ci possono essere casi che nella selezione dell’hash possano essere uguali(nel caso di modifica manomissione), è pensato per essere difficile che accada

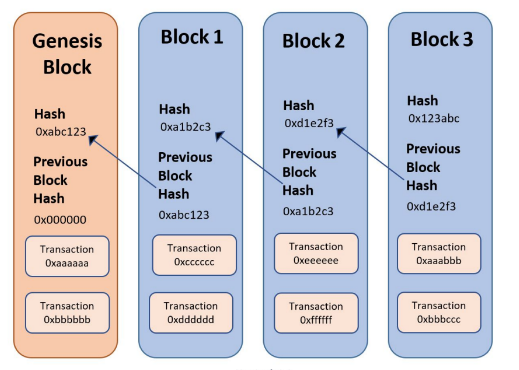
**Resistenza forte alle collisioni:** difficile trovare file diversi con stesso hash

**Processo SHA256**

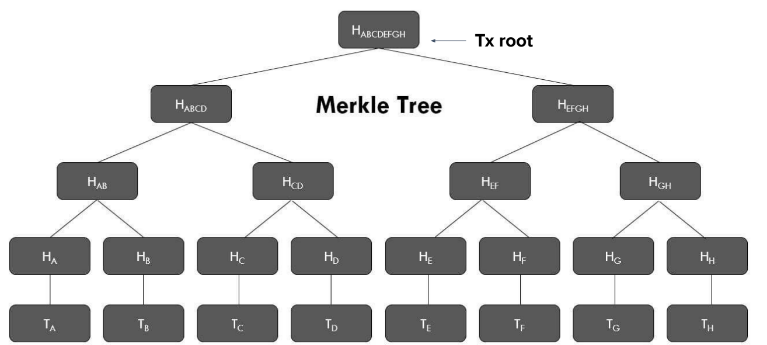
****

Il messaggio viene suddiviso in blocchi di 512 bit, Questi blocchi vengono iterati con una funzione di compressione su un insieme di 8 valori da 32 bit (A, B, C, D, E, F, G, H), Il risultato è la concatenazione di questi blocchi (8 x 32 = 256 bit), Bitcoin utilizza SHA2562 ossia SHA256(SHA256(x))

concetto della chain di block



**Merkle tree:** algoritmo che raccoglie N file transazioni, li raccoglie/elabora per far sì che si possa ottenere un solo hash



all'inizio abbiamo 8 transazioni, calcola hash di ognuno, poi inizia a fare l’hash concatenati di file(a coppie di 2). è un meccanismo ricorsivo(richiama se stessa)

**si ferma quando avremo un solo hash che verrà messo nella blocco(tx root)**

è + efficiente per la verifica di una transazione effettuata, questo è fattibile grazie al logaritmo di N hash

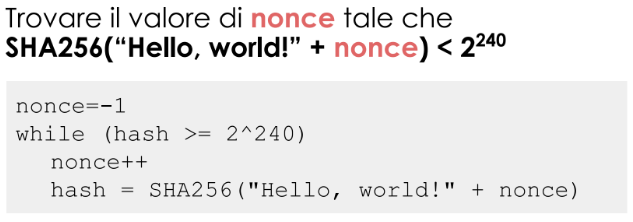
**FONTI UTILI:** <https://github.com/ezimuel/tecnologie-blockchain>

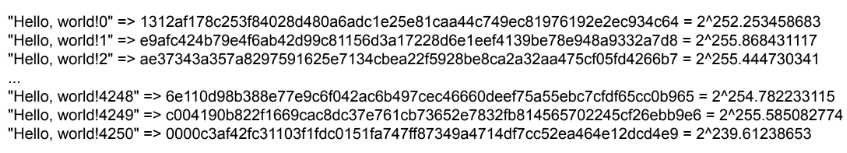
**Nonce:** risultato del **Proof Of Work** (“quiz” che chi conia monete, miner, deve risolvere)

chi indovina, vince e ottiene le monete coniate (se è il primo…?)

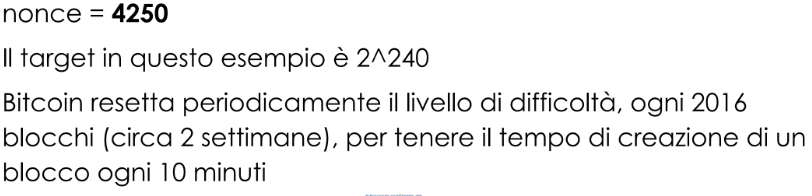
la dimostrazione è difficile da eseguire per trovare la soluzione: il nonce è la soluzione da trovare (valore che deve essere concatenato all’input risposta, in modo tale che risulti minore a un target prestabilito,)

questo è un metodo per i tentativi per calcolare i l nonce e trovare la soluzione





al 4250 indovina



con una legge di mur ogni due anni bitcoin resetta il lvl di difficoltà modo tale da tenere un tempo di creazione btc di 10 min

**Miner:** nodi che risolvono i PoW, vince = ricompensa (ma prova dopo + difficile)

curiosità le gpu hanno maggiori prob di calcolo



**Crittografia**

a chiave pubblica (cifrare persona)

a chiave privata (decifrare personale)

**Firma digitale:** chiave privata per “firmare” un dato , chiave pubblica per verificare firma

Chiave pubblica BTC: **ripemd160(SHA256(Public-key))**

**curve ellittiche: y^2 = x^3 + ax + b**

• Una curva ellittica è una funzione matematica particolarmente utilizzata in crittografia

• Una curva ellittica è la funzione y

**crittografia ellittica**

• La crittografia ellittica (ECC) utilizza le curve ellittiche su un campo Zn

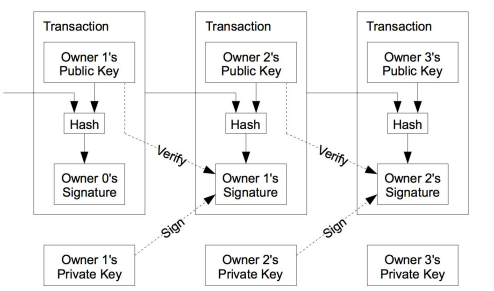
• Nelle tecnologie blockchain l’algoritmo che viene utilizzato per firmare le transazioni è l’ECDSA, Elliptic Curve Digital Signature Algorithm

**Secp256k1**

Una delle curve più utilizzate nelle tecnologie blockchain (es. Bitcoin) è la Secp256k1, dove a=0 e b=7, ossia la curva y^2 = x3 + 7

Bitcoin utilizza Z definita sul campo Z2 256−232−977, nel quale le coordinate x e y sono interi a 256-bit modulo un primo

molto grande

****