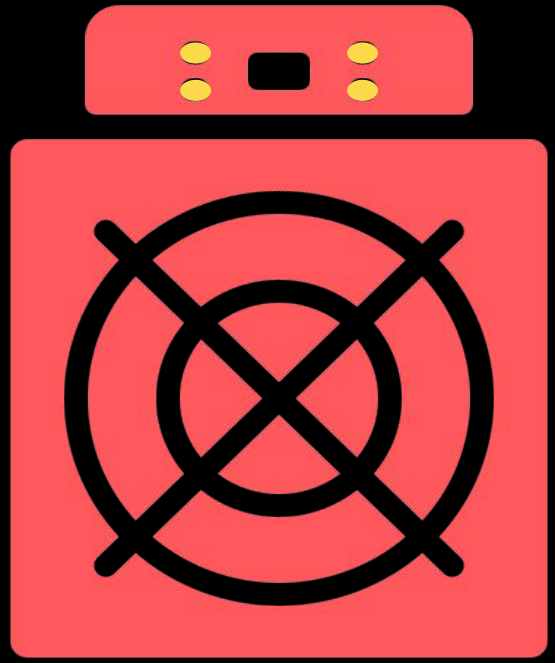
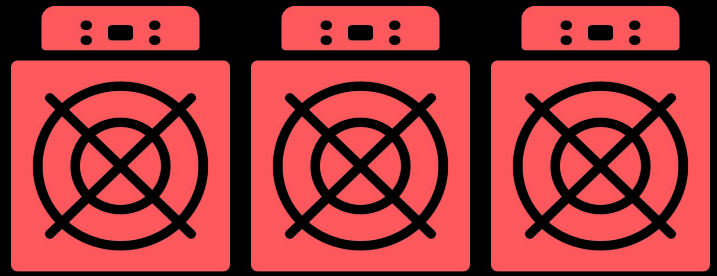
FONDAMENTI DI PROOF OF WORK

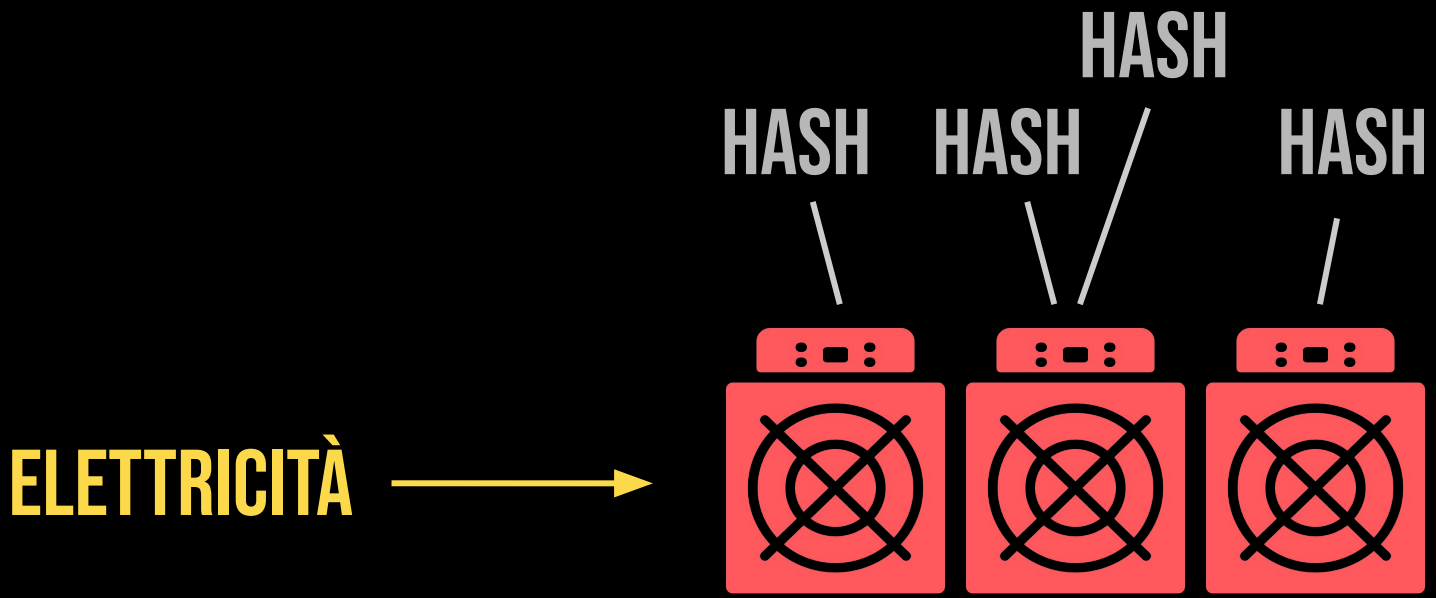


ELETTRICITÀ



@ANILSAIDSO

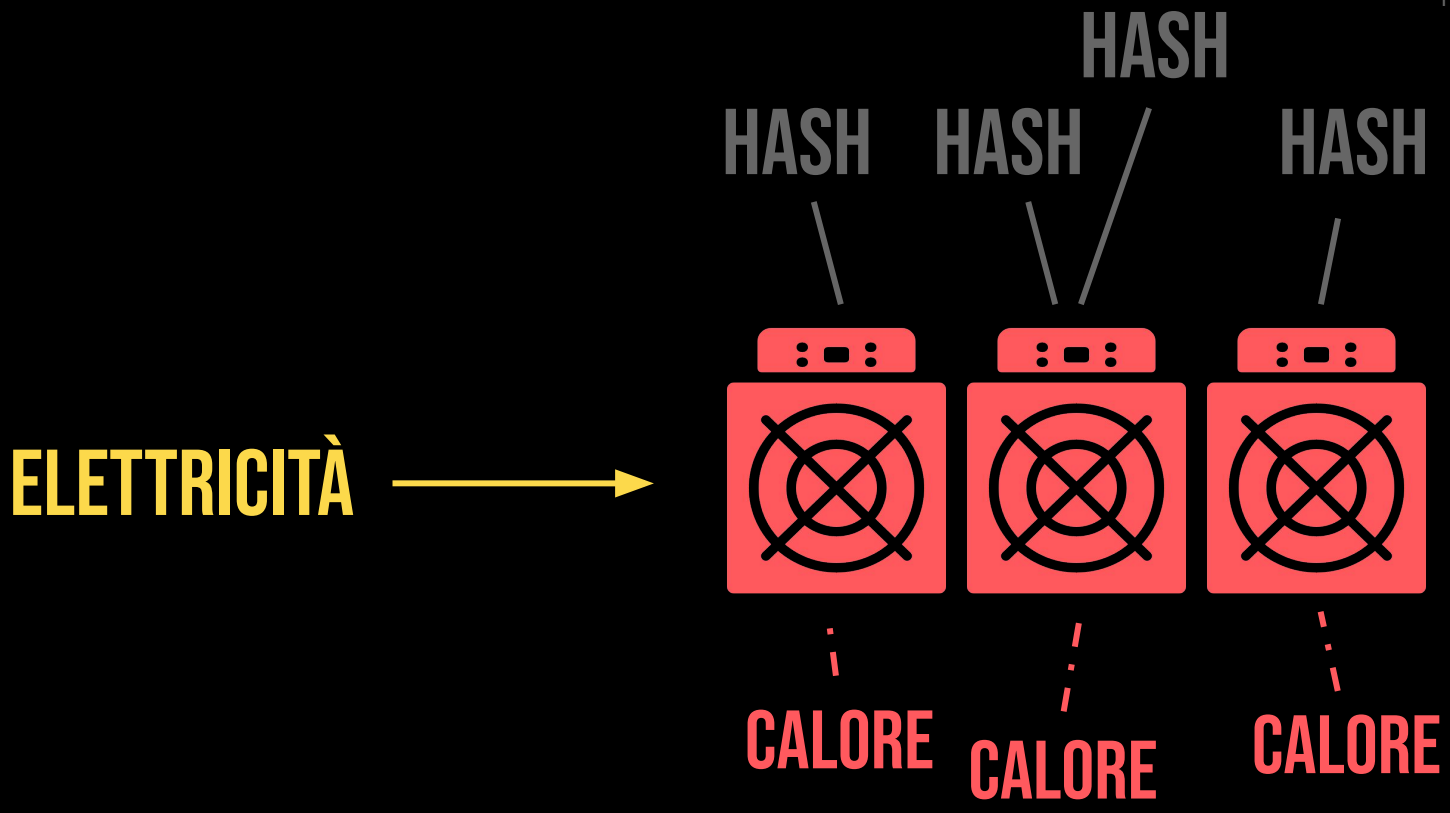
I *miner* (minatori) consumano elettricità fornita da una rete elettrica o generata direttamente da una fonte energetica presente in loco.



Anche se "miner" è un termine che rende bene l'idea, queste apparecchiature sono in realtà impegnate nel processo di "hashing" dei dati con l'obiettivo di ottenere un determinato *output* (risultato).

HASHING *(verbo)*

Utilizzare un algoritmo per effettuare la conversione di un dato in una stringa univoca di lunghezza fissa.



Come sottoprodotto della produzione di *hash*, i *miner* sviluppano calore.

1ª Legge TERMODINAMICA

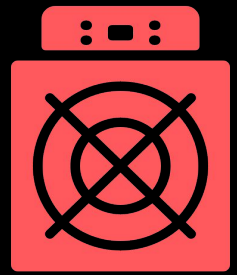
Nei sistemi isolati, l'energia non può essere creata né distrutta. Può essere solo trasformata.

I miner utilizzano energia computazionale (convertendo l'elettricità in hash) e sviluppano calore come prodotto secondario.

HASH

26A03CAD6CEF052E
5772286E18D7986D
E1B3D2D9F959C56D
FCE04CA7B469449E

ELETTRICITÀ



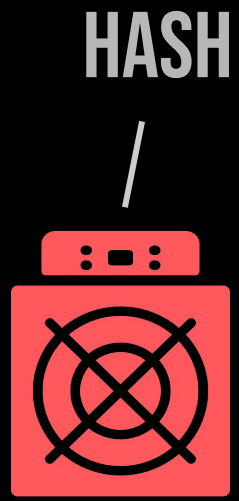
@ANILSAIDSO

I *miner* cercano un numero casuale (chiamato "nonce") che produca un *hash* che soddisfi l'attuale livello di difficoltà (numero di zeri iniziali).

NONCE *(nome)*

Un numero casuale generato per produrre un risultato che soddisfi determinate caratteristiche (ad esempio, gli zeri iniziali) quando viene combinato con i dati esistenti.

ELETTRICITÀ



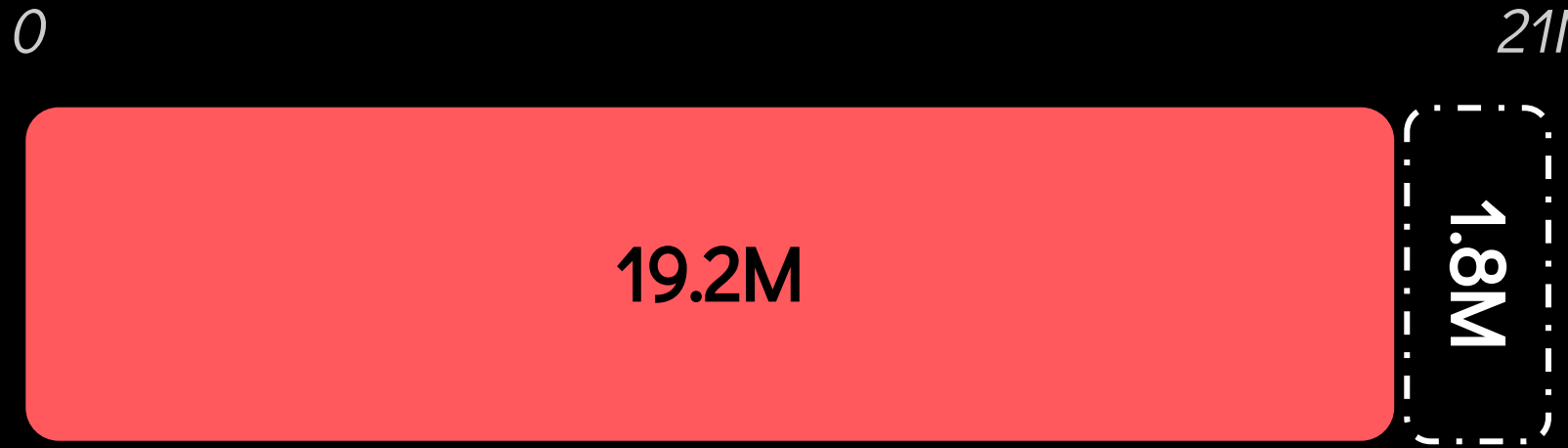
0000000000000000
000 77D7E94EA7787
80E2D6138D4E38EB
091932E6C6CA4004

VINCITORE!

@ANILSAIDSO

Il vincitore ha il diritto di reclamare le spese di transazione e di ottenere dei nuovi bitcoin. Per farlo, propone un nuovo blocco alla rete includendo in esso una transazione autopagante denominata "coinbase".

PER COSA COMPETONO I MINER?



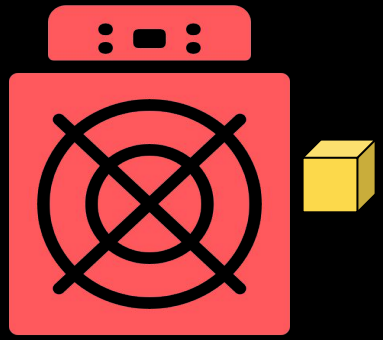
COMMISSIONI DI TRANSAZIONE
dalla supply circolante

BITCOIN RIMANENTI
emessi con i nuovi blocchi

BLOCK SUBSIDY *(nome)*

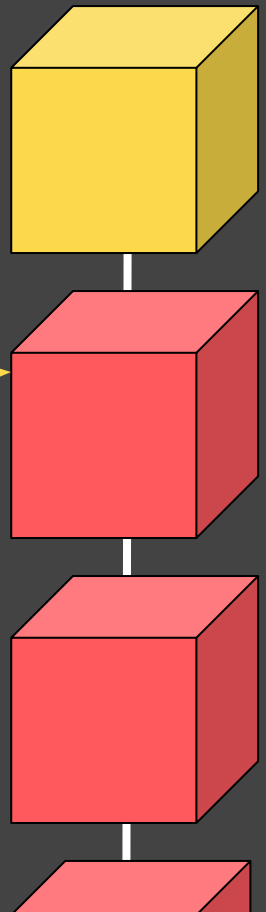
La quantità predeterminata di bitcoin che il miner vincente è autorizzato a "coniare" attraverso il nuovo blocco.

50BTC	25BTC	12.5BTC	6.25BTC	3.125BTC



Il blocco proposto viene trasmesso alla rete e, se valido, si propaga formando la nuova estremità della catena.

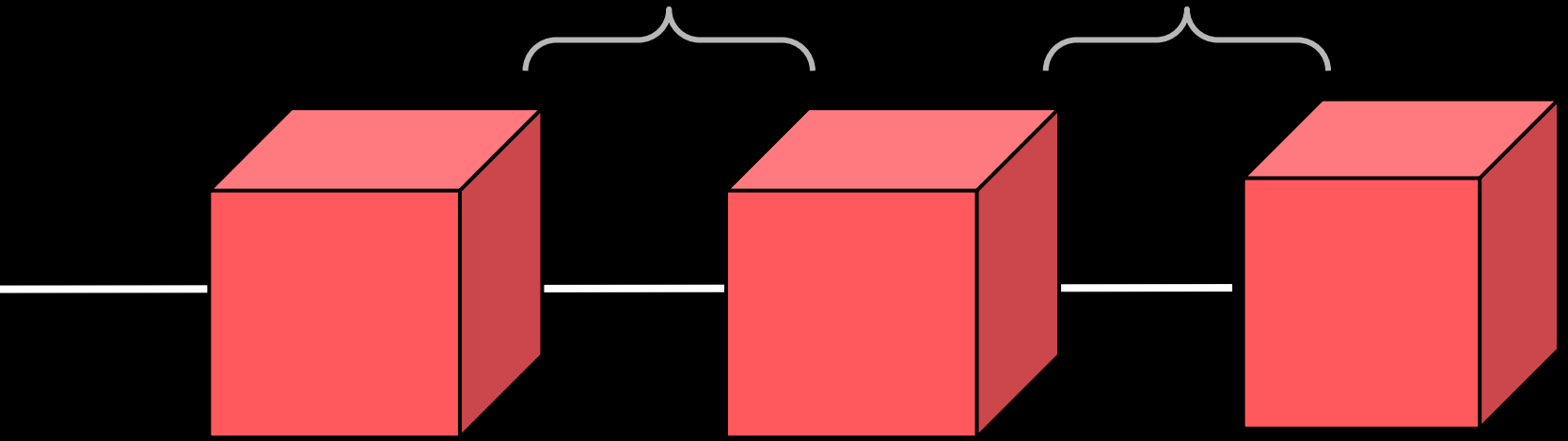
ESTREMITÀ DELLA CATENA



BLOCCO PROPOSTO

BLOCCO CONFERMATO

INTERVALLI DI 10 MINUTI
(IN MEDIA)



La produzione di blocchi è programmata per avvenire a intervalli regolari. Se i tempi si allontanano troppo dall'intervallo desiderato di 10 minuti, il livello di difficoltà viene regolato verso l'alto o verso il basso.

DIFFICOLTÀ *(nome)*

Misura la probabilità di trovare un nuovo blocco in base a determinati parametri.

00000000000000000000 77D7E94EA778780E2D6138D4E38EB091932E6C6CA4004

“Bitcoin è solida immutabilità storica garantita dalla legge della termodinamica.

Abbiamo solo bisogno di un libro mastro immutabile basato sulla proof-of-work.”

—ANDREAS ANTONOPOULOS

Anil

@anilsaidso

Anil è un educatore indipendente che crea risorse altamente visive su Bitcoin.