II Mining

Valerio Vaccaro

Monday 4th March, 2024

Meme

* entro la fine del corso capirete tutti i meme.

Riassunto

- Strutture dati blocco ed header
- Altezza e block id
- Merkle tree
- Blocco 0 e coinbase
- Testnet/signet/regtest
- ...

Mining

da "Mastering Bitcoin"

"Lo scopo del mining non è la creazione di nuovi bitcoin. Questo è un sistema di incentivi. Il mining è il meccanismo con cui la sicurezza di bitcoin è decentralizzata."

La scelta del nome mining non è particolarmente felice, il mining si occupa di:

- Gestire l'emergenza di un nuovo consenso senza autorità centrale
- Rendere costosa/impossibile la modifica delle storia di Bitcoin
- Consolidare le transazioni
- Creare nuova moneta

L'economia del miner

Costi:

- Corrente elettrica
- Hardware specializzato per il mining
- Gestione e manutenzione

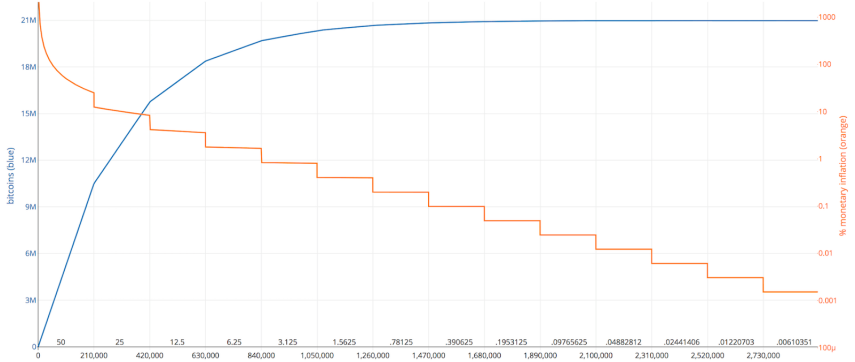
Ricavi:

- Premio (attualmente 6,25 BTC)
- Somma delle fee pagate da tutte le transazioni incluse

I ricavi sono spendibili dopo 100 blocchi, se il blocco è considerato non-valido i ricavi non potranno essere mai spesi.

L'economia di Bitcoin

Ogni 210.000 blocchi il premio si dimezza.



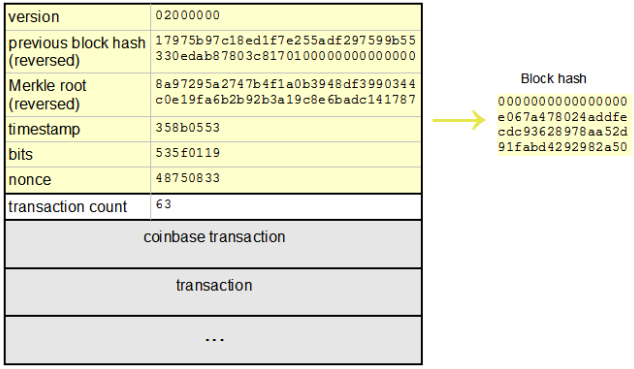
Nel 2140 (circa) saranno generati tutti i 21 milioni di Bitcoin.

L'economia di Bitcoin

I Bitcoin sono in un numero finito.
Perché?
"L'emissione limitata e decrescente crea un approvvigionamento monetario fisso che resiste all'inflazione. A differenza di una moneta fiat, che può essere stampata in numeri infiniti da una banca centrale, il bitcoin non può mai essere gonfiato con la stampa"
– Mastering Bitcoin

Costruzione del blocco

Per minare un nuovo blocco dobbiamo prima costruirlo.



Selezione delle transazioni

Il primo step è cercare la lista delle transazioni che includeremo nel nuovo blocco. Validate le transazioni scegliamo il mix in modo da:

- Riempire lo spazio del blocco il più possibile
- Massimizzare la somma delle fee pagate da tutte le transazioni scelte

Che è una variate del "Problema dello zaino" e quindi NP-completo.

Selezione delle transazioni

Poi dobbiamo aggiungere la coinbase che è una transazione speciale che ha le seguenti caratteristiche:

- Può avere zero fee
- Può non avere input (cioè generare nuova moneta)
- Può avere uno o più output la cui somma sia inferiore o uguale al premio più la somma delle fee pagate dalle transazioni

Fee

Le fee non sono in consenso quindi un blocco può contenere transazioni che non pagano fee, il miner normalmente scarterà queste transazioni. Probabilmente anche la mempool le scarterà per una protezione da attacchi DOS.

Selezione delle transazioni

Spesso la coinbase al posto degli input ha dei dati (random o meno) che aiutano l'attività di mining (questo spazio è normalmente chiamato extra nonce).

Extra Nonce

Visto che il campo Nonce dell'header è di dimensioni troppo piccole per il mining viene utilizzato anche il campo extra nonce per generare diversi template di transazione su cui effettuare il mining.

Costruzione dell'header

Name	Type	Bytes	Description
`version`	int32_t	4	Version number
`previous hash`	char[32]	32	Hash of the previous block header in internal byte order
`merkle root`	char[32]	32	Merkle root of the transactions included in the block formatted in internal byte order
`time`	uint32_t	4	Epoch timestamp of the block
`bits`	uint32_t	4	Encodes the network target difficulty
`nonce`	uint32_t	4	Dedicated number to be updated to generate unique hashes

Costruzione dell'header

- Mettiamo la versione a 2
- Copiamo il block id del blocco precedente
- Calcoliamo il merkle tree di tutte le transazioni (coinbase compresa) e copiamo il merkle root
- Copiamo il timestamp dal nostro computer (assicuriamoci sia aggiornato)
- Copiamo il target (o ricalcoliamolo se necessario)
- Poniamo nonce a zero

Target

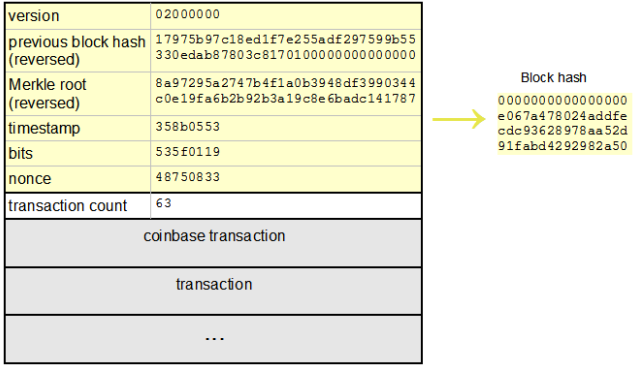
0x181bc330 →	0x1bc330	*	256	^	(0x18	-	3)
nBits In Big-Endian Order	Significand (Mantissa)		Base		Exponent		Bytes In Significand

Result: 0x1bc330000000000000000000000000000000000000000000

Converting nBits Into A Target Threshold

Mining

Occorre trovare un nonce (in generale un header) il cui hash sia minore del target (o più facile da ricordare con un certo numero di zeri).



Ottimizzazione

L'header di un blocco è grande 80 byte, SHA256 lavora a blocchi di 64 byte.
Il nonce si trova oltre i primi 64 byte quindi potremmo:

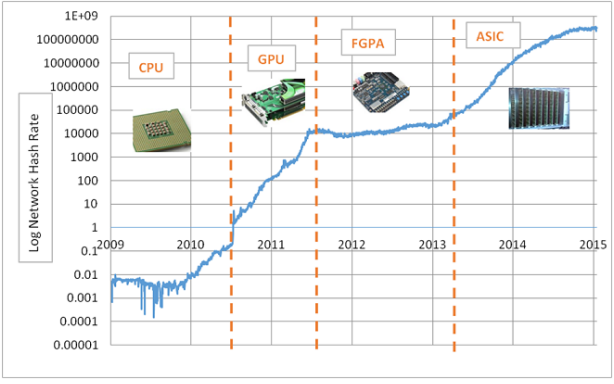
- Calcolare SHA256 dei primi 64 byte SENZA finalizzare e memorizzare il risultato come S
- Applicare ad S il nonce e finalizzare SHA256
- Ripetere il punto precedente per tutti i valori di nonce

Abbiamo velocizzato di parecchio il mining per Bitcoin.

Solomining vs. pool

Fino ad ora abbiamo visto come fare minig in solitaria ovvero senza collaborare con altri (solomining). Se il nostro hashrate è basso potremmo dover aspettare anni per trovare la soluzione ad un blocco.
Le pool nascono per aggregare il lavoro da più miner e fornire pagamenti a scadenze regolari (o al raggiungimento di un certo target).
In cambio le pool si prendono una percentuale e forniscono dei servizi web con cui istruire il proprio miner.

Evoluzione tecnologica del mining



Il mining ricerca:

- Energia a prezzo inferiore (di qualsiasi tipo)
- Nuove tecnologie che riescano ad effettuare mining ad un costo inferiore

Pausa

Nerdminer

Nerdminer: 80K hashes per second

https://github.com/BitMaker-hub/NerdMiner_v2

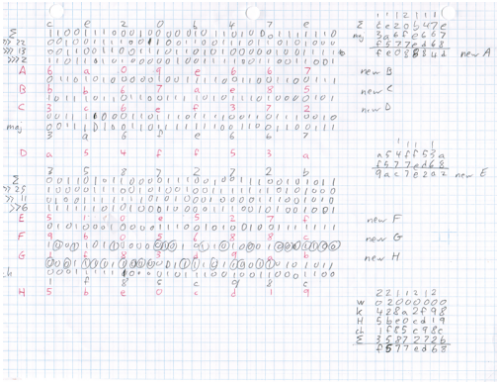
Bitaxe

Bitaxe: 300G hashes per second

https://github.com/skot/bitaxe

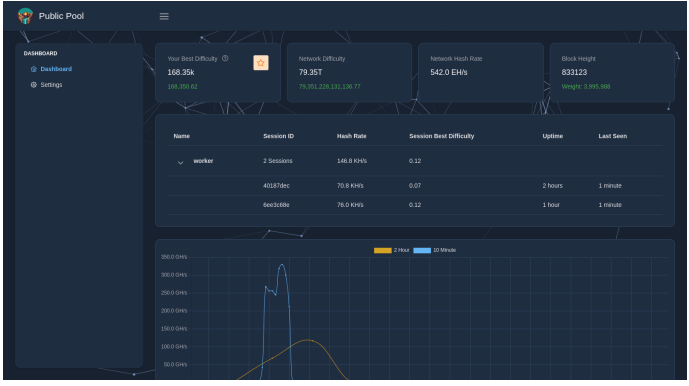
Mining manuale

Mining Bitcoin with pencil and paper: 0.67 hashes per day



https://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

Pool



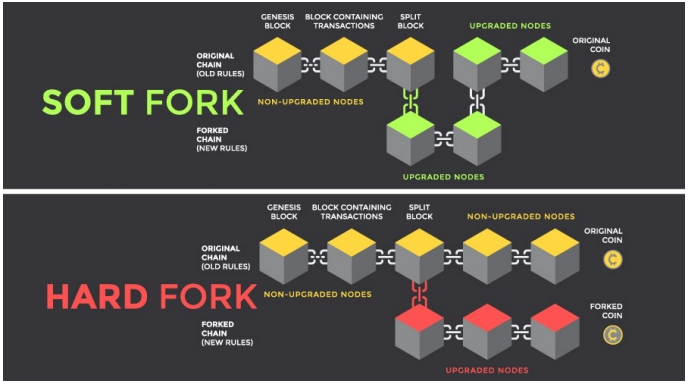
https://web.public-pool.io/#/app/bc1q79qgpy5sc7n3fkmmc2920ycrhrt7e2fm6t7rw4

Come cambiare le regole di consenso?

Le regole del consenso determinano la validità delle transazioni e dei blocchi e possono essere modificate (mai retroattivamente) ma:

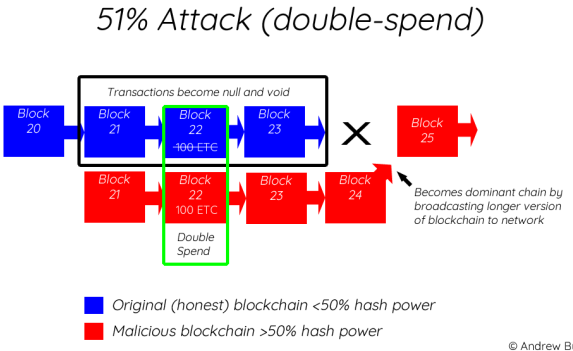
- Le modifiche richiedono una forte convergenza di tutti gli attori
- Sono più semplici in caso di bug
- Le nuove funzionalità vengono testate per anni prima di essere consolidate
- La tendenza è quella di non cambiare più il protocollo (ossificazione)
- Possono generare hardfork ovvero lo split definitivo della catena

Hardfork vs. softfork



Perché avere il 51 per cento dell'hashing power è pericoloso?

Un attacco al cinquantun per cento si verifica quando un singolo miner o un gruppo di miner prende il controllo della maggioranza.



Se il problema sono le pool ...

Allora stratum v2 potrebbe risolverlo.
Stratum v2 è un nuovo protocollo che sposta parte delle decisioni dalla pool ai singoli miner, un attacco controllando il cinquantun per cento dei singoli miner è più difficile.

Bibliografia

- Andreas M. Antonopoulos, "Mastering Bitcoin", 2015
- Adam Back, "Hashcash-a denial of service counter-measure", 2002
- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
- Hal Finney, "Reusable Proofs of Work", 2004

Altre risorse

Tra le altre risorse utili mi piace citare:

- Ovviamente BitPolimi che ha organizzato queste lezioni.
- Satoshi Spritz - eventi serali a scadenze regolari per parlare di Bitcoin (a Milano ci incontriamo ogni mercoledì dalle 18).
- Ventuno - Podcast, raccolta di libri e materiali su Bitcoin.
- Officine Bitcoin - lezioni su telegram da 30 minuti per la risoluzione di problemi pratici.

Domande


BEH... EHM... SAREBBE A DÌ... CHE RISPETTO A STA COSA, CIOÈ, NE LA MISURA IN CUI... EHM... SE ANNAMO, SE FA PE' DÌ, A SVILUPPÀ UN DISCORSO SU LE STRUTTURE, CIOÈ, SUL CONTENUTO, TRA VIRGOLETTE...
AHO', MA CHE VOR DÌ?


"That's all Folks!"