Creazione di Bitcoin

scritto da Alberto De Luigi | 2 Maggio 2016
< Pagina precedente Pagina successiva >

2.1 La Coinbase Transaction

Quando il miner **crea un nuovo blocco**, non solo crea uno "spazio" virtuale per registrare le transazioni, ma attua anche **una "coinbase transaction", che genera nuovi bitcoin**.

La coinbase è una transazione presente in ogni blocco (una sola per blocco) che come output trasferisce bitcoin al miner, pur non avendo un tradizionale input e una signature script. Al posto del parametro "Scriptsig" (signature script) c'è un parametro "coinbase", che può essere scelto arbitrariamente dal miner. Per esempio, nella prima transazione coinbase del primo blocco della storia compare, fra gli altri dati, la scritta: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

Inizialmente venivano generati 50 bitcoin per blocco, ma ogni quattro anni circa questa quantità viene dimezzata (i primi tre dimezzamenti sono nel 2012, 2016, 2020). Sia i bitcoin di nuova generazione che le commissioni pagate dalle transazioni costituiscono un output che non è spendibile come input prima che la blockchain abbia aggiunto altri 100 blocchi al blocco appena creato **-> Vedi i dettagli in una finestra separata**.

Non è necessario includere delle transazioni in un blocco oltre alla coinbase transaction, il cui inserimento è invece obbligatorio. Un miner può inserirla come unica transazione nel blocco e in quel caso verrebbe creato l'hash della Merkle root partendo dalla coinbase e una copia di se stessa. Ovviamente, se le transazioni hanno delle commissioni, il miner ha tutta convenienza a inserirle nel blocco: può comunque decidere arbitrariamente di inserire o meno una

transazione, sia che paghi una commissione o no.

Viene creato un blocco ogni circa 10 minuti. Per creare un blocco il miner deve risolvere un enigma matematico. Tale enigma ha un coefficiente di difficoltà (**il target**) che varia in modo tale da mantenere la frequenza di creazione di blocchi in tutto il mondo di 1 ogni 10 minuti. Se per esempio un blocco è stato creato in 9 minuti e 40 secondi, la difficoltà aumenterà, se è stato creato in 11 minuti, diminuirà. Se più (meno) potenza di calcolo viene adoperata dai miner, e quindi si trovano blocchi più (meno) frequentemente, il coefficiente viene aumentato (diminuito). Il target non è altro che un numero all'interno della funzione, che più è piccolo più rende difficoltosa la soluzione dell'enigma.

Il target è un numero molto lungo (256 bit), ma se per ipotesi fosse molto più breve, per esempio solo «1000», significa che l'enigma viene risolto quando il risultato dell'operazione matematica è un numero positivo inferiore a 1000. Quindi un nuovo blocco viene creato se il risultato è uguale o inferire a 999. Più il target è basso, meno possibilità ci sono di trovare la soluzione. Ad esempio se il target fosse 1, il blocco verrebbe creato solo con un risultato x tale che $0 \leq x < 1$

2.2 La creazione di un blocco

La creazione di un blocco avviene solo quando l'hash di un particolare algoritmo (il Block Hashing Alghoritm) risulta inferiore al target:
se hash<target allora il blocco è valido.

Più potenza di calcolo si dispone, più hash al secondo vengono effettuati e perciò maggiore è la probabilità di trovare **in modo del tutto casuale** l'hash giusto. Scoprire un blocco è una sorta di gara fra minatori, che gareggiano per conquistare le commissioni sulle transazioni e il "premio" per la creazione del blocco, ovvero il "coinbase". Statisticamente vince chi ha

più potenza di calcolo a disposizione.

Dato che **i bitcoin possono essere al massimo 21 milioni** (è una delle «consensus rules» del protocollo, non un vincolo matematico), quando saranno stati tutti creati non ci sarà più un premio dato dalla coinbase transaction. I minatori gareggieranno quindi solo per le commissioni sulle transazioni.

L'elenco che segue è l'insieme degli elementi (detti "block header") che vengono elaborati dalla funzione di hash per produrre l'hash voluto:

1.La Merkle root: l'hash finale di tutte le transazioni. Per calcolarla, un miner raccoglie tutte le transazioni che vuole fino al tetto massimo di 1mb per blocco. Può anche non inserire alcuna transazione, eccetto la coinbase, che sarà sempre la prima del blocco. Se un miner sta cercando un hash valido per un blocco che include una data transazione e un altro miner scopre prima di lui un blocco al cui interno ha inserito la stessa transazione, allora Bob dovrà modificare il suo Merkle tree senza includere quella transazione. In caso contrario la transazione sarà inclusa in due blocchi diversi e uno dei due non sarà riconosciuto dagli altri nodi (**vedi approfondimento sul double spending in una finestra separata**). È uso che i minatori riservino 50 Kb di ogni blocco per le transazioni che presentano un ouput non speso da molto tempo. Il restante spazio è occupato dalle transazioni in ordine di commissione per byte, con le transazioni più remunerative (per il miner) aggiunte prima e così via in sequenza, finché tutto lo spazio nel blocco viene occupato.

2.L'hash del blocco precedente. Tutti i blocchi sono così concatenati, ciascuno includendo in sé l'hash di tutti gli elementi del blocco precedente.

3.La versione del software utilizzato quando l'hash viene calcolato.

4.Il timestamp: l'ora in cui l'hash viene calcolato. È generalmente aggiornato ogni pochi secondi. Dal momento che vengono provati molti hash al secondo, molti tentativi riportano lo stesso orario.

5. Il target: è un numero sotto al quale l'hash del blocco dovrà trovarsi per essere ritenuto valido.

Dato che l'hash è una stringa composta da un numero fisso di cifre, per risultare in un numero inferiore al target dovrà iniziare con una serie di zeri. Dunque se l'hash del blocco inizierà con un numero di zeri consecutivi sufficientemente lunga, allora il blocco è considerato valido. Altrimenti è necessario calcolare, ancora in modo del tutto casuale, un altro hash. Se cambia anche solo una singola cifra fra tutti gli elementi di partenza per la creazione dell'hash, questo sarà modificato completamente. Per questo motivo le prove vengono svolte in modo del tutto casuale modificando generalmente un solo parametro per volta, il Nonce.

6. Il Nonce: è il parametro modificato a piacere dal miner per trovare in modo casuale un hash che stia al di sotto del target

Il nonce è una sequenza di 32 bit (4 bytes). Il miner prova ogni combinazione in 32 bit finché l'hash risultante non sia inferiore al target. Dato che un bit può essere 0 o 1, vi sono 2^32 possibili Nonce da provare, ovvero circa 4 miliardi e 294 milioni. Se, come generalmente accade, nessuno dei 4 miliardi di hash risultanti è inferiore al target, si modifica un altro dato da inserire nell'algoritmo, come il timestamp o la merkle root, e si riprovano da capo tutte le possibili combinazioni di Nonce, finché non viene trovato un hash del blocco che inizia con un numero sufficiente di zeri. Da notare che la coinbase non richiede un signature script definito e si potrà quindi inserire un valore casuale che il miner può utilizzare come Nonce aggiuntivo.

Qui un riassunto degli elementi del Block Hashing Algorithm:

Elemento	Descrizione	Aggiornato quando..	Peso (Bytes)
Merkle root	L'hash finale di tutte le transazioni	Una nuova transazione viene inclusa nel blocco da creare	32
Hash del Blocco precedente	Hash di (Versione, Target, Nonce ecc.....)	Un nuovo blocco viene creato	32
Versione	La versione di software utilizzata	Il software Bitcoin viene aggiornato	4
Timestamp	L'ora in cui viene effettuato l'hash	Ogni pochi secondi	4
Target	Il coefficiente di difficoltà	La difficoltà viene aggiustata (~10 minuti)	4
Nonce	un numero di 32 bit	Ciascun hash viene calcolato	4

Clicca su "Pagina successiva" per andare alla sezione Criticità e idee, altrimenti torna alla transazione bitcoin

< Pagina precedente Pagina successiva >