Block

Transaction data is permanently recorded in files called **blocks**. They can be thought of as the individual pages of a city recorder's recordbook (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a linear sequence over time (also known as the block chain). New transactions are constantly being processed by miners into new blocks which are added to the end of the chain. As blocks are buried deeper and deeper into the blockchain they become harder and harder to change or remove, this gives rise of bitcoin's Irreversible Transactions.

Contents

Block structure

Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

Description

Each block contains, among other things, the current time, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle - the answer to which is unique to each block. New blocks cannot be submitted to the network without the correct answer - the process of "mining" is essentially the process of competing to be the next to find the answer that "solves" the current block. The mathematical problem in each block is extremely difficult to solve, but once a valid solution is found, it is very easy for the rest of the network to confirm that the solution is correct. There are multiple valid solutions for any given block - only one of the solutions needs to be found for the block to be solved.

Because there is a reward of brand new bitcoins for solving each block, every block also contains a record of which Bitcoin addresses or scripts are entitled to receive the reward. This record is known as a generation transaction, or a coinbase transaction, and is always the first transaction appearing in every block. The number of Bitcoins generated per block starts at 50 and is halved every 210,000 blocks (about four years).

Bitcoin transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. Miners get incentive to include transactions in their blocks because of attached transaction fees.

The difficulty of the mathematical problem is automatically adjusted by the network, such that it targets a goal of solving an average of 6 blocks per hour. Every 2016 blocks (solved in about two weeks), all Bitcoin clients compare the actual number created with this goal and modify the target by the percentage that it varied. The network comes to a consensus and automatically increases (or decreases) the difficulty of generating blocks.

Because each block contains a reference to the prior block, the collection of all blocks in existence can be said to form a chain. However, it's possible for the chain to have temporary splits - for example, if two miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another. The peer-to-peer network is designed to resolve these splits within a short period of time, so that only one branch of the chain survives.

The client accepts the 'longest' chain of blocks as valid. The 'length' of the entire block chain refers to the chain with the most combined difficulty, not the one with the most blocks. This prevents someone from forking the chain and creating a large number of low-difficulty blocks, and having it accepted by the network as 'longest'.

Common Questions about Blocks

How many blocks are there?

Current block count (http://blockexplorer.com/q/getblockcount)

What is the maximum number of blocks?

There is no maximum number, blocks just keep getting added to the end of the chain at an average rate of one every 10 minutes.

Even when all 21 million coins have been generated?

Yes. The blocks are for proving that transactions existed at a particular time. Transactions will still occur once all the coins have been generated, so blocks will still be created as long as people are trading Bitcoins.

How long will it take me to generate a block?

No one can say exactly. There is a generation calculator that will tell you how long it **might** take.

What if I'm 1% towards calculating a block and...?

There's no such thing as being 1% towards solving a block. You don't make progress towards solving it. After working on it for 24 hours, your chances of solving it are equal to what your chances were at the start or at any moment. Believing otherwise is what's known as the Gambler's fallacy [1] (http://en.wikipedia.org/wiki/Gambler's_fallacy).

It's like trying to flip 53 coins at once and have them all come up heads. Each time you try, your chances of success are the same.

Where can I find more technical detail?

There is more technical detail on the block hashing algorithm page.

See Also

- Protocol rules - "block" messages
- Format of the BDB-style block files (https://bitcointalk.org/index.php?topic=101514.0)

Retrieved from "https://en.bitcoin.it/w/index.php?title=Block&oldid=66453"

- This page was last edited on 13 May 2019, at 16:48.
-