

Block chain

From Bitcoin

A **block chain** is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency. With this information, one can find out how much value belonged to each address at any point in history.

Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block. Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known. Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. These properties are what make double-spending of bitcoins very difficult. The block chain is the main innovation of Bitcoin.

Honest generators only build onto a block (by referencing it in blocks they create) if it is the latest block in the longest valid chain. "Length" is calculated as total combined difficulty of that chain, not number of blocks, though this distinction is only important in the context of a few potential attacks. A chain is valid if all of the blocks and transactions within it are valid, and only if it starts with the genesis block.

For any block on the chain, there is only one path to the genesis block. Coming from the genesis block, however, there can be forks. One-block forks are created from time to time when two blocks are created just a few seconds apart. When that happens, generating nodes build onto whichever one of the blocks they received first. Whichever block ends up being included in the next block becomes part of the main chain because that chain is longer. More serious forks have occurred after fixing bugs that required backward-incompatible changes.

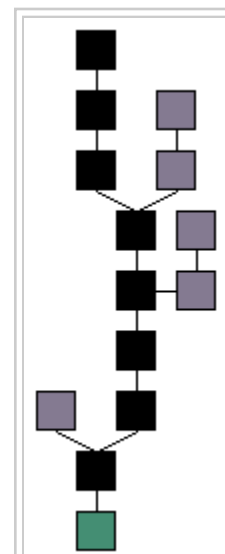
Blocks in shorter chains (or invalid chains) are not used for anything. When the bitcoin client switches to another, longer chain, all valid transactions of the blocks inside the shorter chain are re-added to the pool of queued transactions and will be included in another block. The reward for the blocks on the shorter chain will not be present in the longest chain, so they will be practically lost, which is why a network-enforced 100-block maturation time for generations exists.

These blocks on the shorter chains are often called "orphan" blocks. This is because the generation transactions do not have a parent block in the longest chain, so these generation transactions show up as orphan in the listtransactions RPC call. Several pools have misinterpreted these messages and started calling their blocks "orphans". In reality, these blocks have a parent block, and might even have children.

Because a block can only reference one previous block, it is impossible for two forked chains to merge.

It's possible to use the block chain algorithm for non-financial purposes: see Alternative chain.

The block chain is broadcasted to all nodes on the networking using a flood protocol: see Block chain download.



Blocks in the main chain (black) are the longest series of blocks that go from the genesis block (green) to the current block. Purple blocks are blocks that are not in the longest chain and therefore not used.

See Also

- [BlockChain.info](#) - Utility site and EWallet provider of similar name

Retrieved from "https://en.bitcoin.it/w/index.php?title=Block_chain&oldid=37883"

Categories: [Technical](#) | [Vocabulary](#)

- This page was last modified on 18 May 2013, at 18:16.
- This page has been accessed 141,352 times.
- Content is available under [Creative Commons Attribution 3.0](#).