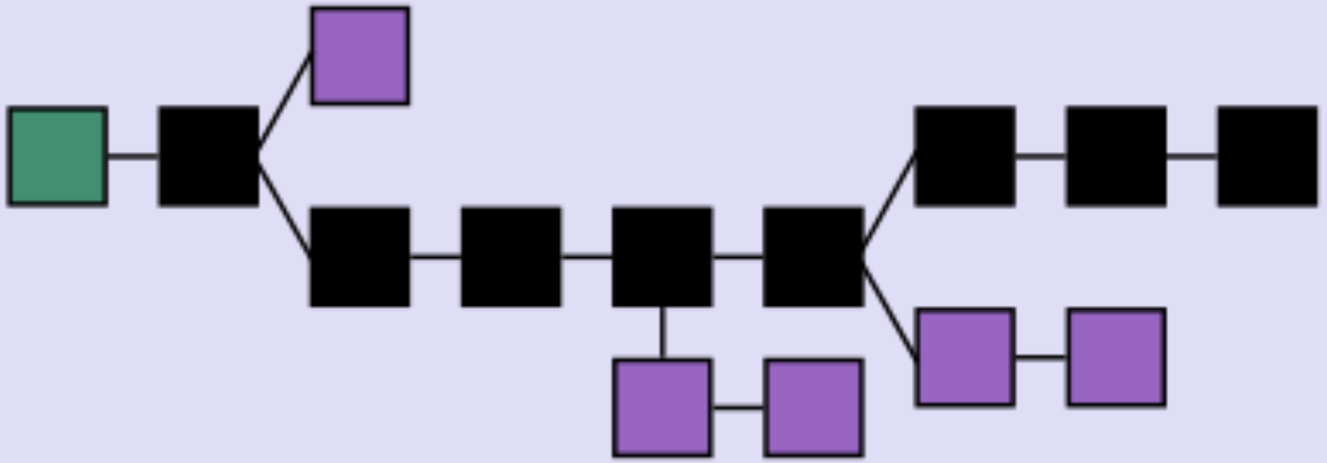
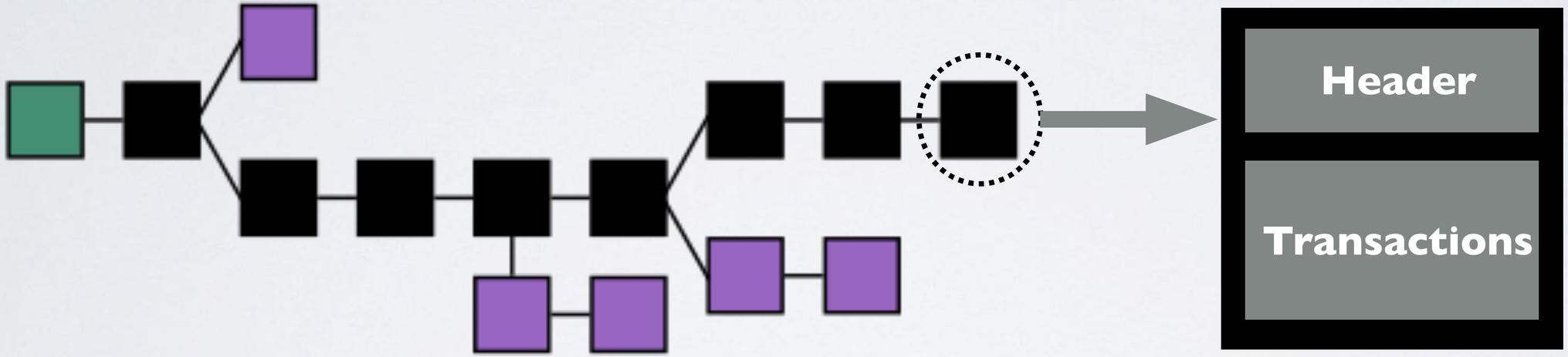
BLOCKCHAIN TUTORIAL 24

Blockchain & Miners



BLOCKCHAIN

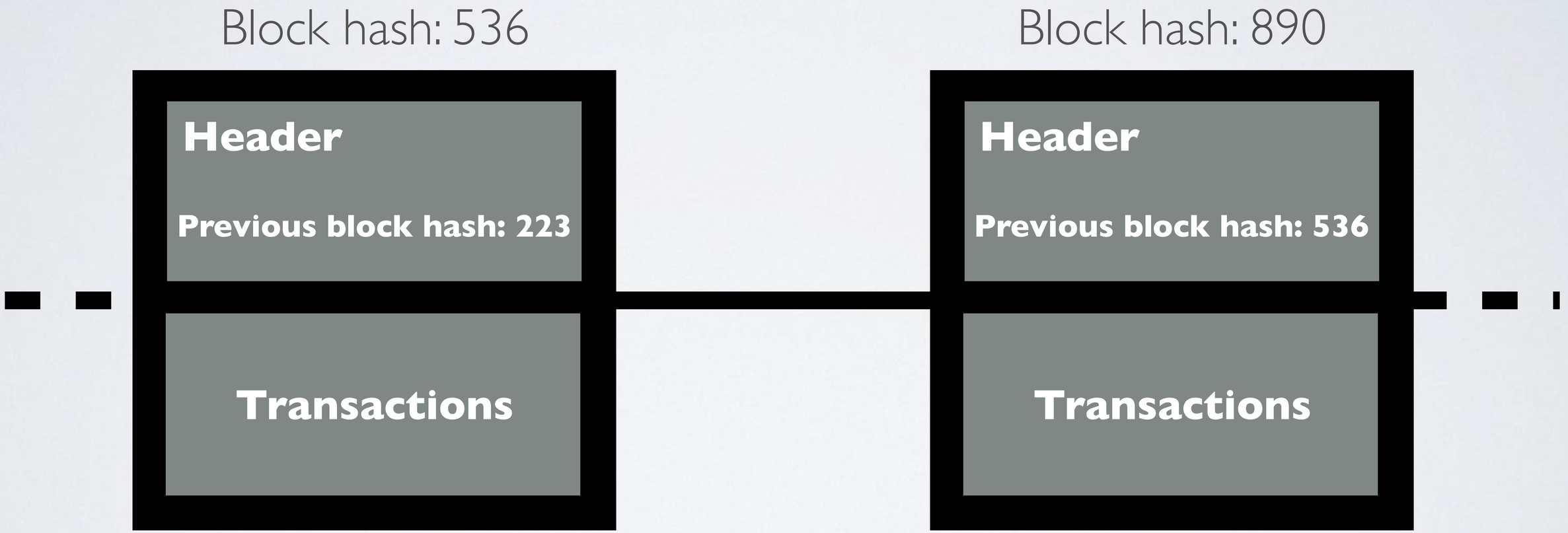
- A Blockchain ledger is visualised as a series of blocks which are connected with each other.



- Each block is made of a header, containing metadata such as its previous block hash, merkle root hash and nonce, followed by a list of transactions.

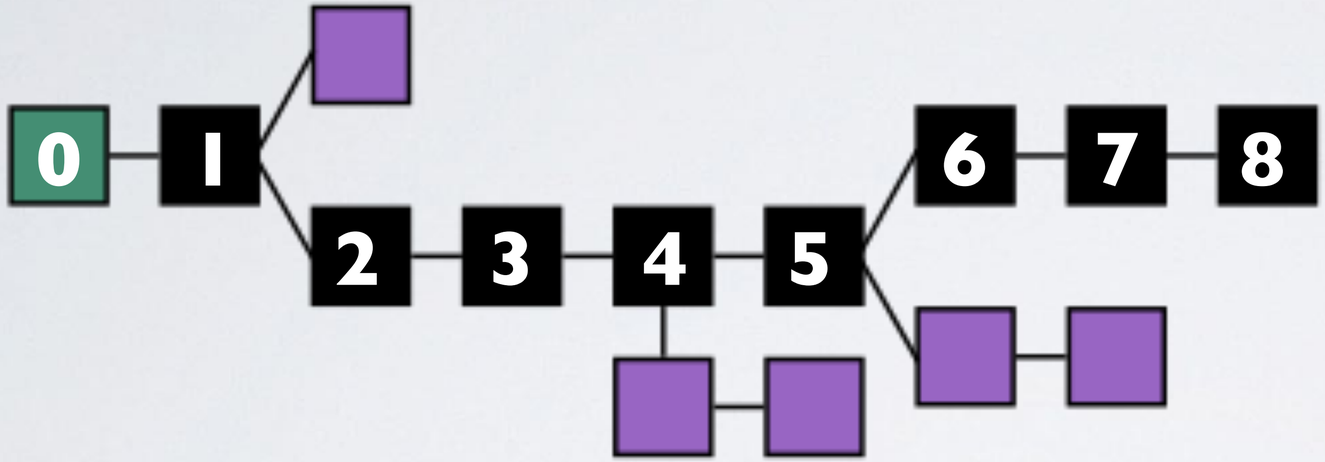
BLOCKCHAIN

- The blocks are "connected" with each other by referencing its "parents block hash".



BLOCKCHAIN

- All blocks in the main chain are numbered, starting with 0, 1, 2…



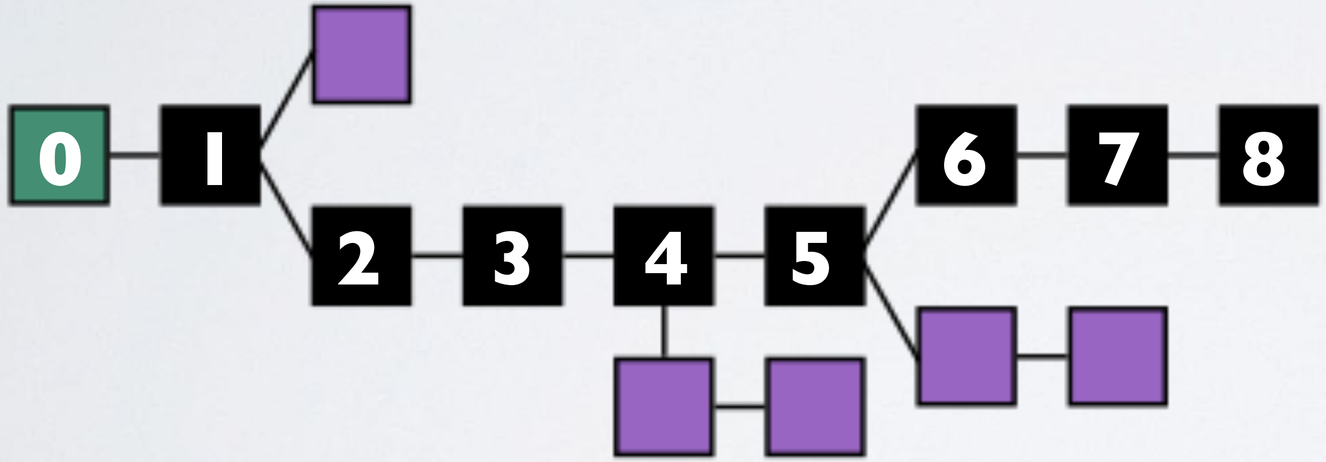
- The green block is the first block created and is called the genesis block and has block number 0.

- The "purple blocks" which forms a short but invalid chain are blockchain forks which occur quite regularly. These side forks are also called orphaned forks.

BLOCKCHAIN

- Bitcoin blocks are created every 10 minutes on average.
  Ethereum blocks are created every 17 seconds on average.

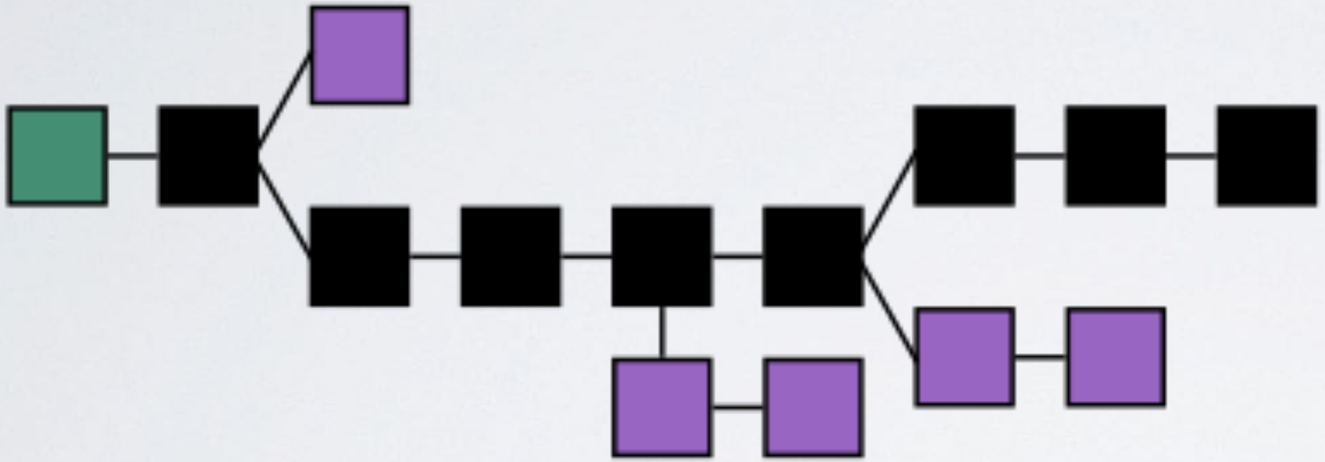
- The block height is the number of blocks in the chain between it and the genesis block minus 1.

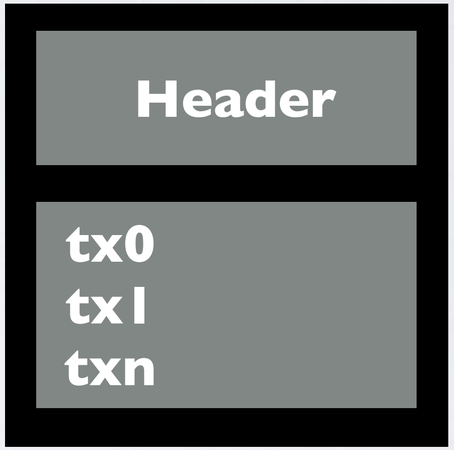


- Blocks on side forks can have the same block height as blocks on the main chain.

BLOCKCHAIN

- Special nodes on the peer-to-peer network are creating these blocks. These nodes are called miners.





- All miners are collecting all transactions which people are sending to each other over the network and only valid transactions are relayed to other nodes. Each miner takes a number of these collected transactions and put them in a newly formed "block". This list of transactions are numbered tx0, tx1, tx2,…txn.

BLOCKCHAIN

- The first transaction (tx0) is called the coinbase transaction. This is the transaction where the miner assigns a block reward to his own address. This is how Bitcoins are created. For Bitcoin miners the block reward is 12.5 BTC in 2017. When the genesis block was created in 2009 the block reward was 50 BTC.

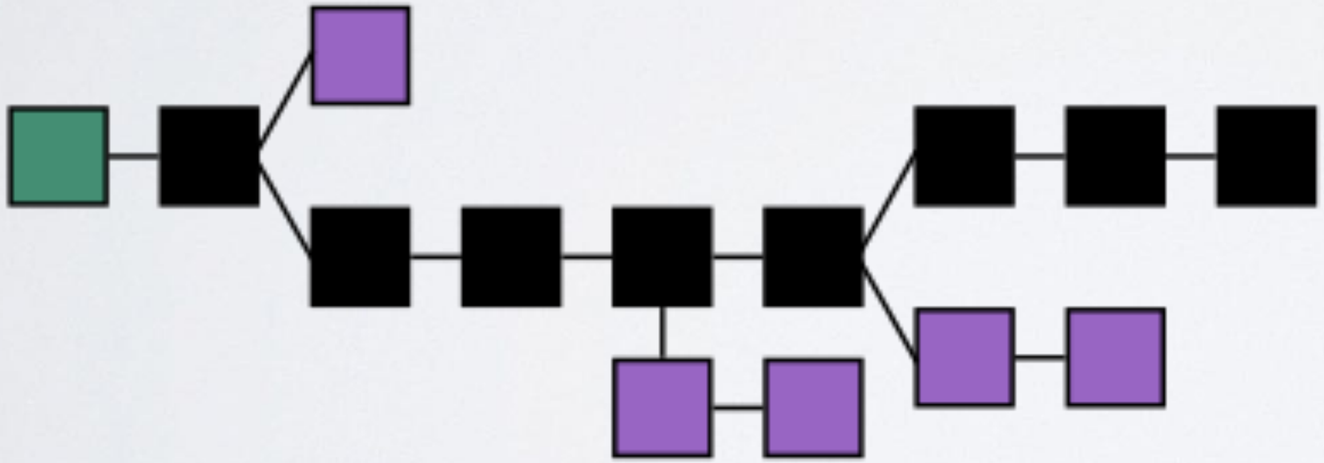
- For Bitcoin, every 210,000 blocks, the block reward will be halved. Once there have been 64 halvings, the block reward will be 0. There will be a maximum of 21 million Bitcoin in circulation in the year 2140.

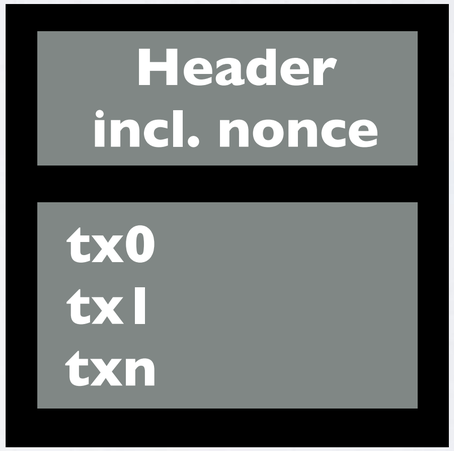
- The other Bitcoin transactions (tx1, tx2..) are ordinary transactions where Bitcoins are transferred from the owner address to a recipient address. Each transaction requires a small transaction fee. This fee will continue to increase as an incentive for the miners to create new blocks because the block reward will continue to be lowered.

BLOCKCHAIN

- When the miner has constructed a block, he has to solve a hash puzzle applied on his list of transactions.

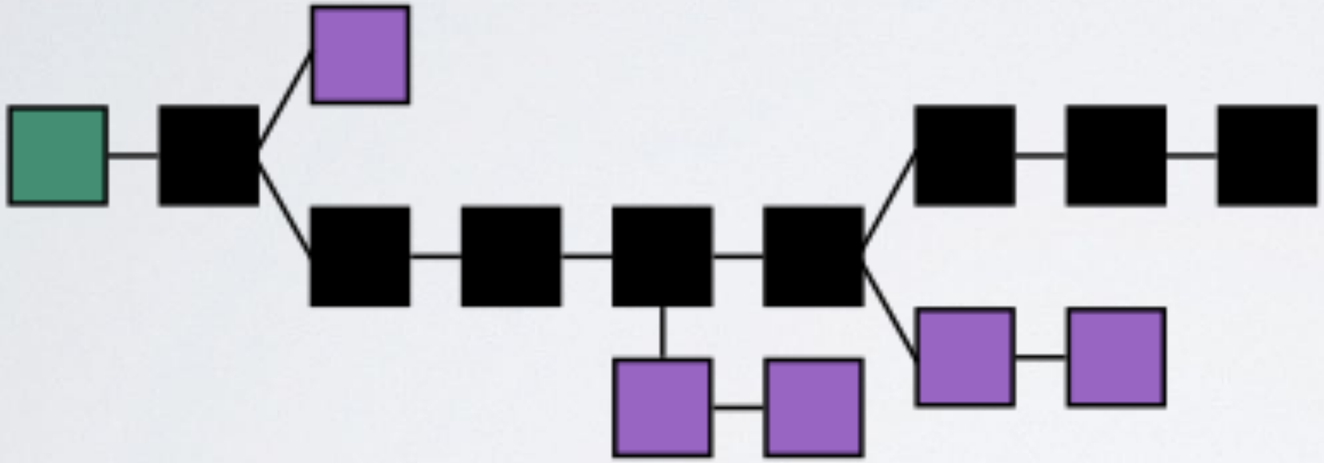
- The miner who has first solved the hash puzzle is allowed to broadcast his block on the network. The block also includes the solution to the puzzle, also called the nonce, in the block header.

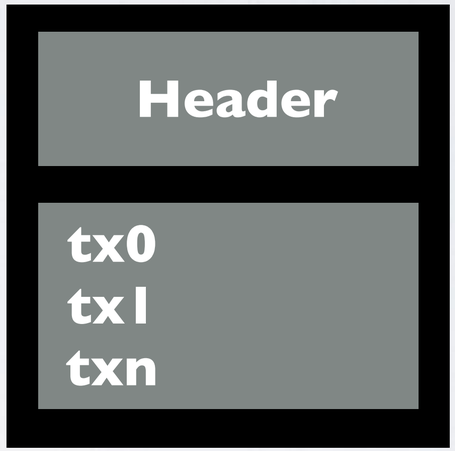




BLOCKCHAIN

- Other miners on the network will receive this block and they validate this block before they append it to their chain of blocks.

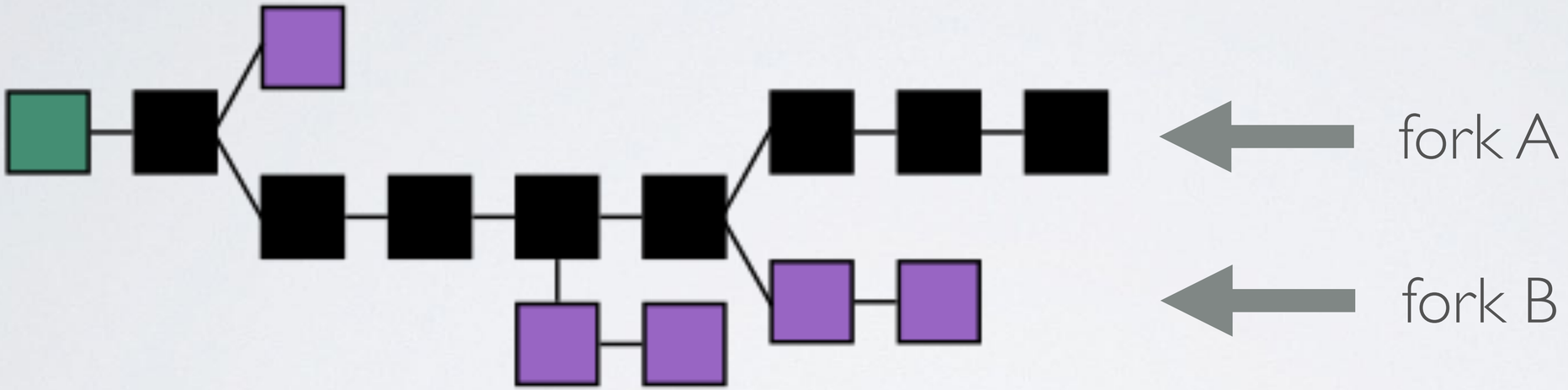




- It happens regularly that another "valid" block is broadcasted on the network because another miner has solved the puzzle at nearly the same time.

BLOCKCHAIN

- When this happens, temporarily forks are created, for example fork A and fork B.



- Lets assume 2/3 of the miners on the network are working on fork A and the rest on fork B. In this example fork A becomes the main chain because it consists of the longest series of blocks from the genesis block. Miners should always work on the longest chain. Blocks on fork B will be orphaned.

BLOCKCHAIN

- The miner who has solved the hash puzzle and his block is on the main chain means that this miner received the block reward and also all the transactions fees (tx1, tx2 etc) in his block.

- The miner who has solved the hash puzzle and his block is on an orphaned fork can not spend the block reward and transactions fees because his block in not on the main chain.