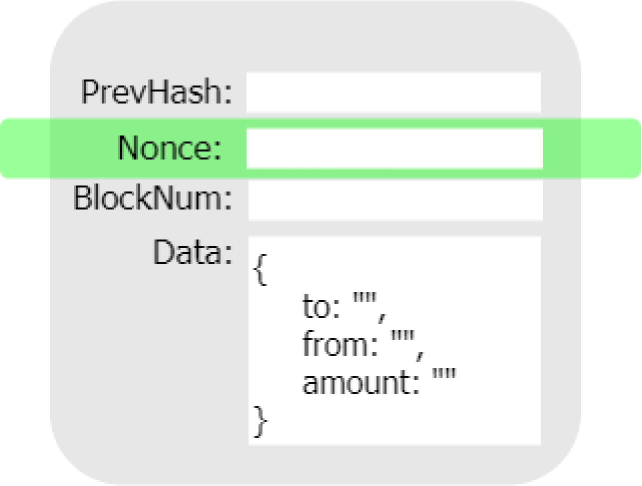
Bitcoin Mining

WE'LL COVER THE FOLLOWING

Mining

In Bitcoin implementation there is an extra field added in each block, called `nonce`.



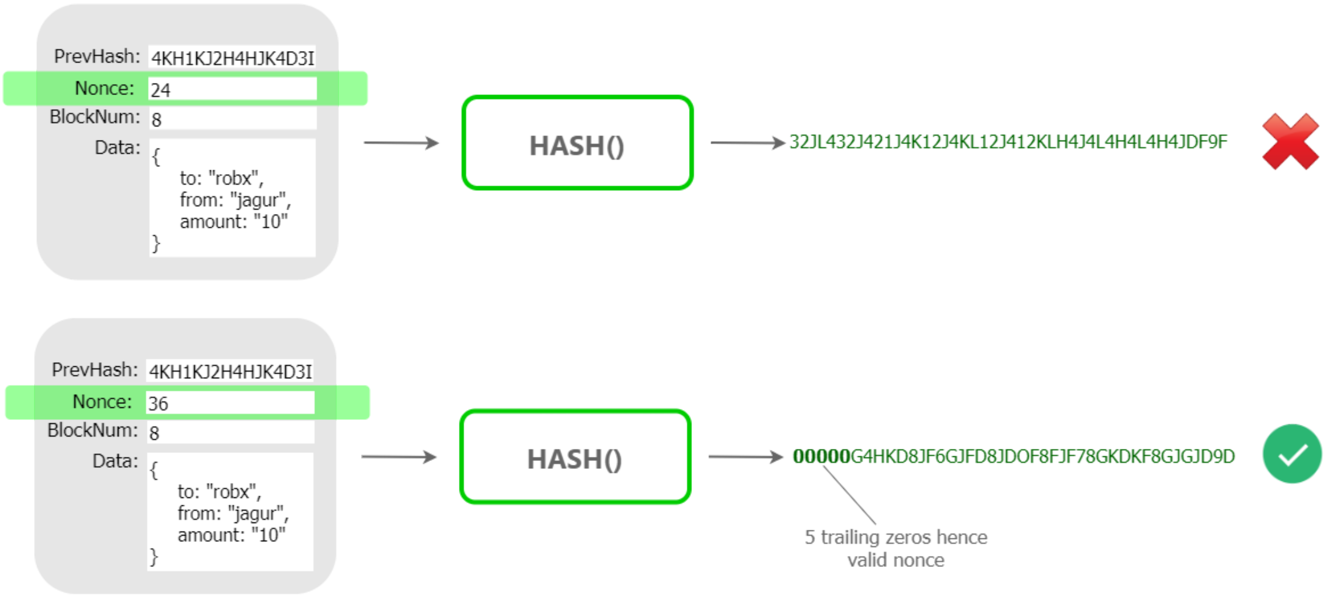
Mining peers continuously receive new transactions submitted on the chain. In order for a transaction to be confirmed, it should be put in a block, that needs to be created.

Simply adding transactions to a block is simple - you get the hash or prev block, increment the block number, add the list of transactions, and take its hash. Pretty fast! But in order to incentivize to run a node, Bitcoin awards miners for creating new blocks by giving them newly generated Bitcoins.

Since it would be very simple to mine a block and devalue the generated coin, Bitcoin has made the block creation process challenging. This difficulty self-adjusts to ensure the global pool of miners are able to mine around one block every 10 seconds. This ensures that the supply of new coins is not too fast, making bitcoin a valuable asset.

Nonce Mining

So Bitcoin adds this extra requirement for a block to have a `nonce` value, such that the block hash of the new block with the nonce has X number of trailing zeros. This X is adjusted by the protocol to control the speed of coin generation. The higher the value of X, the harder it is to calculate a nonce.


PrevHash: 4KH1KJ2H4HJK4D3I
Nonce: 24
BlockNum: 8
Data: {
to: "robx",
from: "jagur",
amount: "10"
}
HASH()
32JL432J421J4K12J4KL12J412KLH4J4L4H4L4H4JDF9F
PrevHash: 4KH1KJ2H4HJK4D3I
Nonce: 36
BlockNum: 8
Data: {
to: "robx",
from: "jagur",
amount: "10"
}
HASH()
00000G4HKD8JF6GJFD8JDOF8FJF78GKDKF8GJGJD9D
5 trailing zeros hence valid nonce

Now since hash functions are one-way functions the nonce cannot really be 'calculated'. Miners do a hit and trial kind of algorithm to see if they can find a nonce that satisfies the requirement(X trailing zeros) for the next block.

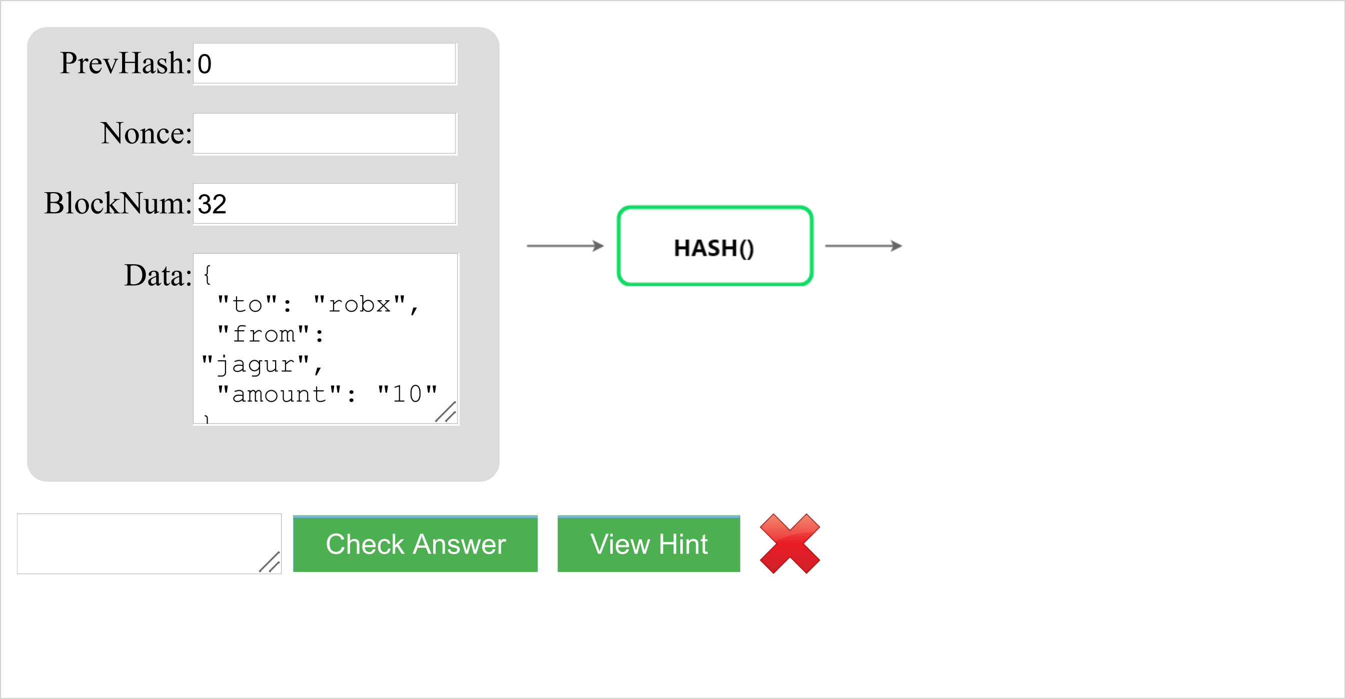
If we go back to our block # 40000 that we looked at earlier, you will find that its hash is `000000000000000004ec466ce4732fe6f1ed1cddc2ed4b328fff5224276e3f6f` which has 17 trailing zeros.This means that when this block was mined in 2016, the value for X was 17.

Exercise - Mining

The purpose of this exercise is to understand how block mining is 'hard'.

Let's say you have a list of transactions that you are mining a block for. And you are required to find a value for nonce that creates blockhash with 3 trailing zeros. Input a value of nonce and the hash will adjust. See if you can find a good nonce in a minute.

find a good nonce in a minute.



PrevHash: 0

Nonce:

BlockNum: 32

Data:
```
{
  "to": "robx",
  "from":
"jagur",
  "amount": "10"
}
```

Test Yourself

Q

Mining a bitcoin essentialy is:

COMPLETED 0%

1 of 1

In the next lesson, we will discuss the value of bitcoin…