About cryptocurrencies and blockchains – part 2

Jyväskylä 18th of April 2018

Henri Heinonen (henri.t.heinonen@jyu.fi)

Mining

- What is the motivation for ”mining”?
- It is the solution for the Byzantine Generals’ Problem assuming that at least more than half of the network’s computing power is ”benevolent”.
- It is rather simple but not the only possible way to reach consensus in a distributed system.

Mining

- The Bitcoin blocks are secured by Proof-of-Work consesus algorithm (PoW), which is using cryptographic hashes.
- What is the possibility in finding a hash with five leading zeros (0x00000ABCDEF…)?
- There are sixteen different hexas.
- The first character is 0 with a probability of 1/16.
- The second character is 0 with a probability of 1/16. etc.
- Answer: $(1/16)^5 = 1 / 1\ 048\ 576$.

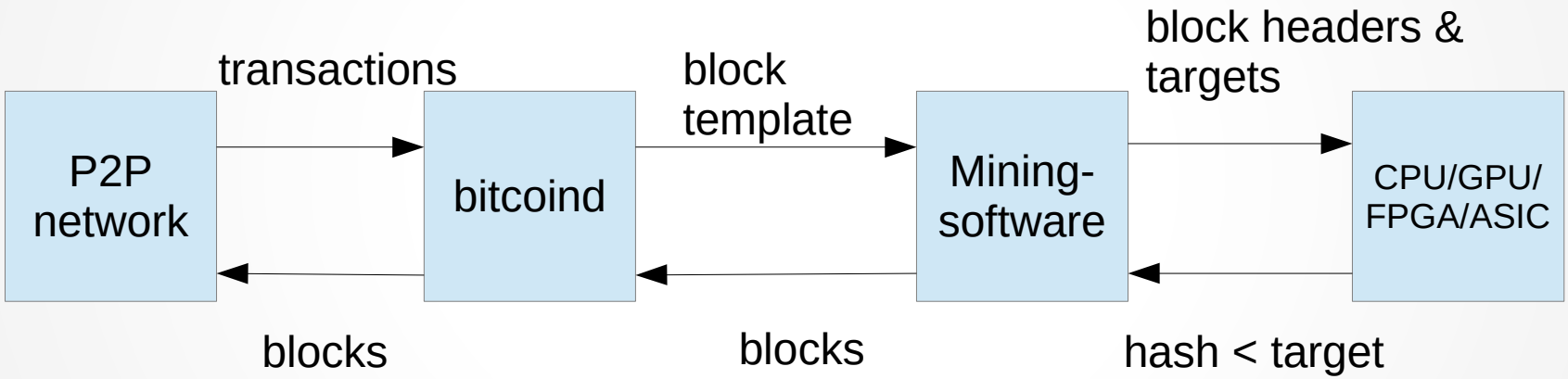
Mining

```
while(nonce < MAX):
    if sha256(sha256(block+nonce)) < target:
        return nonce
    nonce += 1
```

Solo mining

- When Bitcoin started, mining was solo mining. This was possible, because there were a little of miners, and back then computer CPUs were used to mine, so mining was quite even. For example: If there were only about 1000 CPUs in the world doing mining, it was a good chance to win in this lotter game.
- Nowadays it is difficult to mine solo, because it is unlikely that one will earn any bitcoin without considerable hardware investments.
- The mining software gets block templates from bitcoind program.
- If after long streak of trying (one needs to try billions of nonces usually) one is able to find a block, the mining software will send the block to bitcoind program, which in turn sends it to the peer-to-peer network.

Solo mining


P2P network
transactions
bitcoind
block template
Mining-software
block headers & targets
CPU/GPU/ FPGA/ASIC
blocks
blocks
hash < target

Pool mining

- Nowadays mining is done in pools, which are servers where many users can connect. Usually ASIC miners are being used that will cost a few hundred or thousand euros.
- A new Bitcoin block can be found by a pool, which has a computing power of all its users' miners computing power combined.
- Users will get a prototype block from the pool instead of a block template for bitcoin mining.
- The pool is getting shares instead of blocks from the users.
- The pool will get a block reward and transactions fees as a reward for the found block.
- The rewards will be shared among the users; there are lots of different reward sharing methods. The pool itself will usually take a small share to pay for the maintenance costs.
- It could be dangerous for the consensus, if a malicious pool gets a half or more of the total network computing power: ”51% attack”

”51% attack”

An attacker could:

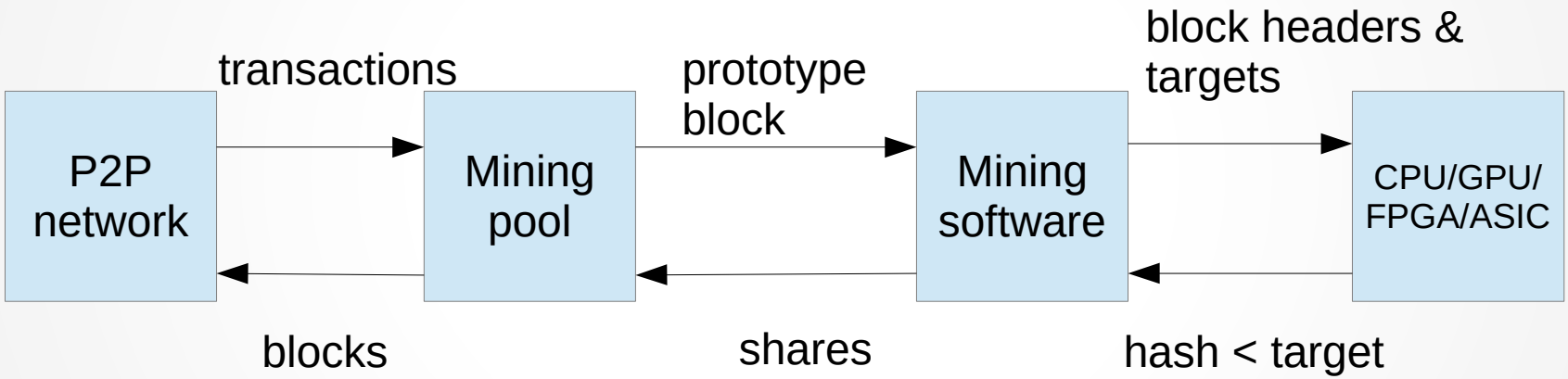
- Cancel transactions so that he/she sends money to someone and then take it back.
- Block some or even all of the transactions to get confirmations.
- Block some or even all of the miners of mining valid blocks.

An attacker **could not**:

- Block other people’s transactions without their consent.
- Forbid broadcasting transactions (one would see 0 confirmations).
- Change the block reward.
- Create coins from thin air.
- Send coins that have never belonged to him/her.

Source: https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

Pool mining


P2P network
transactions
blocks
Mining pool
prototype block
shares
Mining software
block headers & targets
hash < target
CPU/GPU/ FPGA/ASIC

Why is not mining used to calculate something ”useful”?

- It is common to say that hashing is useless: there are no scientific use cases for hashes (beside making the blockchain to work).
- It would be difficult to make a decentralized solution that calculates e.g. medicine simulations: a) where would the data come from?, b) who will check up that the results are valid?, c) how to change the difficulty of calculations?, d) how about the advantage of being the organization that manages the calculations? One could choose to do calculations where one is better than anyone else.
- There are some interesting projects: a) PrimeCoin is using mining to find new prime numbers, b) GridCoin runs BOINC projects and gives gridcoins as a reward.