Exercise 4

1. The nonce field is 32-bit long, resulting in 4.294.967.296 possible allocations. However, this is not sufficient for getting a high probability to find a valid block in current difficulty times ($6.4 * 10^{22}$ (May 2020) attempts to find a valid block). Explain possible changes that you can introduce in your block to change the hash without making the block invalid. Discuss which of these changes are more expensive than others.

   Solution:

   Many properties can be changed:

   - Change time
   - Change ScriptSig field of coinbase transaction
   - Change coinbase transaction address
   - Change ordering of transactions
   - Introduce new transactions / remove others / swap them

   Following order can be assumed:
   Nonce = Timestamp < ScriptSig (coinbase) < coinbase transaction address < ordering = new transactions
   Think of the operations you would have to make to ensure a valid block.

   - Nonce and timestamp can be changed without affecting other parts in the block.
   - The ScriptSig of the coinbase transaction only requires a calculation of a part of the Merkle root tree.
   - If we would change the coinbase transaction address, we would additionally have to generate a new public key.
   - Changing the ordering of transactions requires us (depending on the switches) to recalculate more paths of the Merkle tree.
   - If we introduce new transactions, we also have to recalculate parts of the Merkle tree.

2. What does probabilistic consensus mean?

   Solution:

   A probabilistic consensus means that, if a network agrees on a certain set of transactions to be executed, it is not 100% certain to be valid in the long term. Bitcoin and other blockchains which have a probabilistic consensus have no settlement finality directive. This means, it is possible that transactions can be reverted, however with a very low (and decreasing) probability. The reason for such reversal could be a 51%-attack.

3. Briefly describe two incentives for mining and full nodes to participate in the Bitcoin network.

Solution:

Miners invest a lot of money in the integrity of the network. In order to motivate the miners to keep the integrity up and protect the networks from attacks, they are incentivized by two rewards:

- Transaction Fees: For every transaction to be included in a block, the miner receives a fee.
- Block reward: For every block mined, the miner receives a reward of new Bitcoins.

Full nodes are incentivized not directly by any rewards. Reasons to set up a full node can be following:

- running their own full node to connect the light node / wallet software with it.
- supporting the integrity of the network by validating transactions and blocks.
- having a business which relies on the data (merchant, data analytics, ...).

4. Suppose a miner creates a double spending transaction and manages to mine the transaction in a block. What happens to the other transactions in the block?

Solution:

An honest node is going to ignore any invalid transaction sent to them. If they notice the double spending transaction created by the adverse node they will ignore it and will not include it in the block they are mining.
If the malicious node is able to mine the transaction in a block, this block will be ignored by other honest nodes and the blockchain will not include this block, as others will not build upon an invalid block.
In both cases other transactions are not affected by the double spending transaction. At any instant a transaction can be found in multiple blocks that are not mined yet. After being mined in a valid block nodes drop the transaction from their mempools.

5. Explain two reasons behind transaction fees. Why is the block reward not sufficient?

Solution:

The transaction fees protect the network from spam-transactions. Additionally, it enables a market around transactions, meaning that high priority transactions can pay a higher price than low priority transactions. Furthermore, when the block-reward gets less and less (because of the halving), then transaction fees should incentivize the miner to continue their work. Another reason is that there is no incentive to include transactions into the block if there is no transaction fee. Empty blocks could be mined.

6. Explain why the mining difficulty in the Bitcoin network is adjusted every 2016th block.

Solution:

The idea is to keep the block time at roughly 10 minutes to ensure a stable network. Why has the block time to be constant?
Too slow:

- Transactions take longer to be included
- Network capacity decreases

Too fast:

- Higher possibility of orphan blocks
- Network has to keep track of all blocks
- Empty blocks

7. How many bitcoins will there be at the end?

Solution:
21.000.000 Bitcoins.

8. How often is the mining reward halved?

Solution:
Every 210.000 blocks.

9. A company accepts cryptocurrencies as a payment. What factors should it consider regarding the confirmation time to receive transactions safely?

Solution:
The confirmation time has to be adjusted depending on

- the majurity of the network (The smaller or more novel the network, it is more prone to attacks)
- the amount of the payment (Higher payments should be considered with care)
- The identification of the counterparty (If a counter party can be identified, it could be sued)
- Other parameters (network activity, previous experiences, own business model)