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 ($2.6 * 10^{22}$ 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.

2. What does probabilistic consensus mean?

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

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?

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

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

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

8. How often is the mining reward halved?

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