Exercise 5

A. Blockchain Evolution

1. Explain the implications of changing consensus-relevant methods or data structures. Decide if following changes to the Bitcoin software would impact the consensus-layer.

   - Transactions in the mempool are deleted after a certain elapsed time.
   - The scheme for transactions is changed such that the transaction fee is explicitly stated.
   - After receiving and validating a block, the node encrypts the data before storing locally off-chain. (The data is decrypted before being sent to other nodes)
   - The node enables a new method / RPC-call, in which the user can search for stored texts on the Blockchain.
   - Bitcoin Script now supports an Op-Code which introduces loops and jumps.
   - The Blocksize is increased from 1 MB to 1.5 MB.

2. Assume, that the Bitcoin development team plans to increase the maximum block size limit from 1MB to 10MB. Explain if this change requires a hard fork or soft fork and explain the risks of changing this property only.

B. Blockchain Attacks

3. An adversary has more than 50% of the network hash power. Explain his options to attack the network.

4. Inform yourself about the 51-percent attack on Bitcoin Gold. Explain what happened and how high the damages were. Explain how exchanges can decrease the chance of such attack.

5. Consider slide 13 in the slidedeck "06 Bitcoin Assessment". Selfish mining is a process, in which an attacker with less than 50% of hashing power can attack the network. α defines the probability of the network choosing Block 3A from the attacker. Explain the minimum hashrate required to launch an successful attack, if α is 100%.