

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.

3.	B. Block chain Attacks 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.

attacker with less	3 in the slidedeck "0 s than 50% of hashing Block 3A from the , if α is 100%.	ng power can attacl	k the network. α	lefines the probab	ility of the