Bitcoin Evolution and Challenges

Blockchain Evolution

1. Explain the implications of changing consensus-relevant methods or data structures. Decide if the 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 block size is increased from 1 MB to 1.5 MB.

2. Imagine there are only 100 miners and 100 full nodes in the Bitcoin network. $F_{fullnodes}$ and F_{miners} represent the number of full nodes and miners that adopted the fork. $L_{fullnodes}$ and L_{miners} represent the number of legacy full nodes and miners (i.e., nodes following the old rules). For each of the given fork adoption scenarios, determine whether a chain split will occur or not and briefly explain why.

   (a) **Soft Fork**: $F_{fullnodes} = 1$, $F_{miners} = 1$, $L_{fullnodes} = 99$, $L_{miners} = 99$

   (b) **Hard Fork**: $F_{fullnodes} = 99$, $F_{miners} = 1$, $L_{fullnodes} = 1$, $L_{miners} = 99$

3. 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.

4. In 2017, Bitcoin underwent the SegWit upgrade soft fork which enabled placing more transactions into a Bitcoin block without directly increasing the block size limit.

   (a) Briefly explain how SegWit manages to increase the transaction throughput without increasing the maximum block size.

   (b) What indicates that SegWit was a soft fork and not a hard fork?

Blockchain Attacks

1. Justify whether the following scenarios can be achieved by an attacker holding 51% of the network's hash power.

   - The attacker can block transactions from a single address.
   - The attacker can halt payments between some users.
   - The attacker can DoS the network.
   - The attacker can change the mining reward.
   - The attacker can create coins out of thin air.

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

3. 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/following the block found by the attacker. Explain the minimum hash rate required to launch a successful attack if α is 100%.