Bitcoin Evolution and Challenges

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.

Solution:

Generally, changes to the consensus layer implicate the necessity for a hard- or soft-fork. The complete network needs to upgrade to the new version, otherwise changes could lead to two seperate chains.

- Transactions in the mempool are deleted after a certain elapsed time. No, this change does not impact the consensus layer. If a single node removes transactions after a certain period of time, it does not affect other nodes in their behavior. It is up to the node how it manages the mempool.
- The scheme for transactions is changed such that the transaction fee is explicitly stated. Yes. The transaction scheme is new and therefore other nodes have to recognize to format to validate transactions correctly.
- After receiving and validating a block, the node encrypts the data before storing. (The data is decrypted again before sent to other nodes). No. It is irrelevant for the network how a single node stores its data.
- The node enables a new method / RPC-call, in which the user can search for stored texts on the Blockchain. No. Advanced functionalities, which only read from one node are not impacting the consensus layer.
- Bitcoin Script now supports an Op-Code which introduces loops and jumps. Yes, new Op-Codes can only be used if the complete network agrees to the proposal. A node has to recognize and understand what an Op-Code does in order to execute it.
- The block size is increased from 1 MB to 1.5 MB. Yes. A new max-size for blocks requires an update for all nodes.

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.

Solution:

This change can be considered a hard fork, as old versions become incompatible with the new version. This means, blocks produced by the new version nodes are not considered as valid by the old version nodes. There are some risks:

- A hard fork can lead to two chains, if the hash power of the new software is bigger than the hash power of the old version. However, this can be very dangerous: If the hash power changes (old chain has more hash power), it could be possible that the new chain (with 10MB blocks) gets destroyed as the miners of the new chain also accept blocks of the old chain, as they would follow the rule of "highest accumulated weight". This would result in the 10MB blockchain to be orphaned.
- There is risk of a replay attack. If there are two chains, then a user would control two different types of coins, let's say BTC_A and BTC_B. If the user creates a transaction spending his BTC_A, then the transaction is also valid in BTC_B. Therefore, malicious nodes can propagate these transactions between the two networks, spending the coins from transactions on both chains.

Appropriate actions depend on the intentions of the development team: If they want to keep one Blockchain and do not want to fork, then a compatible Blockchain is the best shot. However, if they are intentionally forking (like with Bitcoin Cash), then you would have to install a replay-protection. The basic idea is that the compatibility between both chains is broken, such that BTC_A does not accept a block or transaction from BTC_B and the other way around.

B. Blockchain Attacks

3. 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.

Solution:

- The attacker can block transactions from a single address. Yes. If an honest node publishes a block which contains such transaction, the adversary can orphan this block.
- The attacker can halt payments between some users. Yes. The attacker can prevent new transactions from gaining confirmations by modifying the ordering of transactions.
- The attacker can DoS the network. Yes. The attacker can propose empty blocks and thus render the network unusable.
- The attacker can change the mining reward. No. The attacker can't change the mining reward since this is a protocol level change.
- The attacker can create coins out of thin air. No. The only way to mine/create tokens is by finding the next block.

4. 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.

Solution:

- May 18, the communications director of Bitcoin Gold alerts the crypto-community: Someone is trying to use 51% of hash power to perform double spends, advises to increaste confirmations.
- Suspected hacker has sent Bitcoin Gold to exchanges and trades them for other coins, withdraws the other coins. Double spends his transaction to the exchange and gains about 18 million USD.
- To decrease the chances of a successful attack, exchanges have to, after receiving funds from unknown addresses, wait for a high number of confirmations, such it gets harder and harder for the attacker to double spend. The longer the transaction is in the Blockchain, the harder it is to double spend it.

5. 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 the block found by the attacker. Explain the minimum hashrate required to launch a successful attack, if α is 100%.

Solution:

If α is 100%, then every time someone finds a block with the same height as the attacker, the attacker publishes his found block and always wins the race (hence the 100%). If this is the case, then any amount of hashing power can try to use selfish mining, because there is no downside to it. As α is 100%, there is no chance of losing the race and therefore no risk.
To read more about selfish-mining, check this article written by Vitalik in 2013: https://bitcoinmagazine.com/technical/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440