Tutorial
Distributed Systems (IN2259)

EXERCISES ON BLOCKCHAIN

EXERCISE 1 - Byzantine Generals

Consider the following Byzantine generals example, with 5 generals. The 2 colored generals are faulty, while the rest are non-faulty. The correct generals wish to unanimously decide on the same action (attack or retreat), while the traitors work together to prevent them from doing so. Each general can communicate to any other general with a fixed delay (i.e., synchronous network).

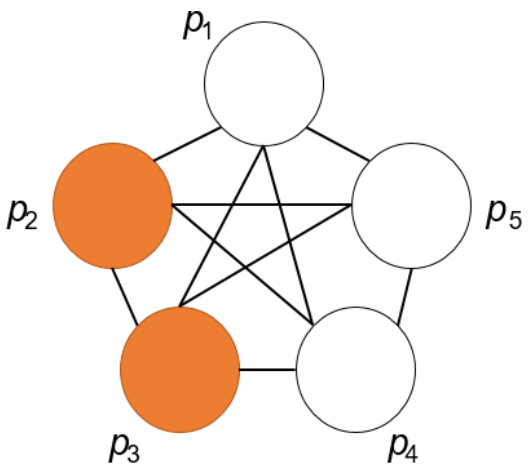

Figure 1.1: Byzantine generals example

(a) Assume $p1$ is the commander, while the others are lieutenants. Can Lamport's original solution to the problem work in this situation? If yes, explain why. If not, show a counter-example.

(b) Assume there are no commander. Describe an algorithm which achieves consensus in the above example with high probability. What happens if the number of traitors is increased to 3? Assume each general has equal computational power.

EXERCISE 2 - Merkle Tree

Consider the function $f(x) = (2 \times x) mod 100$. A Merkle Tree can be built using $f(x)$ as the hashing function, and the pairing of results is done by summation of the results (e.g., $f(f(x) + f(y))$).

(a) Draw the Merkle Tree for transactions 66, 20, 45, 59, 38, 2, 6, 100. The input of $f(x)$ is only the id of each transaction. The tree is sorted in ascending order.

(b) Provide the Merkle proof for transaction 45. Then, show how transaction 45 is verified using the Merkle proof as in the Simple Payment Verification (SPV).

(c) Suppose that all the unspent transaction outputs (UTXOs) of transactions 20, 38, 6, and 2 are consumed in that order. Show how the Merkle tree can be safely pruned if it only tracks the transactions with UTXOs.

EXERCISE 3 - Attacking Bitcoin

Consider "feather-forking", where a Bitcoin mining pool with a proportion $\alpha \in [0,1]$ of the global hash-rate blacklists a specific transaction by refusing to mine a new block on top of any block containing this transaction, and instead branches off with a different block that does not contain it. In a two-block feather-fork attack, the attacker abandons the attack once two confirmations are made. The following figure illustrates the attack:

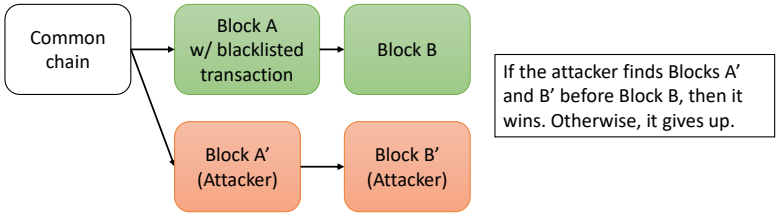

Figure 3.2: Feather-forking attack.

(a) Given $\alpha = 0.25$, what is the probability for a given feather forking attack to succeed? Assume that the probability of mining the next block is proportional to the hash-rate of the miner.

(b) If honest miners are aware of a feather-forking attack, how should their mining decision be affected?

(c) Given a block reward of 12.5 BTCs and an average transaction fee of 0.1 BTCs, what should the blacklisted transaction fee be to subvert the attack? Assume each block contains 100 transactions and that $\alpha = 0.25$.