THE UNIVERSITY OF SYDNEY

COMP3221 Lab 8

Consensus & Mining

The goal of this lab is to understand how to reach consensus despite the presence of failures and understand Bitcoin mining procedure and consensus protocol.

Exercise 1: Failure-free consensus

How many round(s) minimum could a consensus protocol take in a failure-free environment?

Duration: 5 min

Exercise 2: Crash-tolerant consensus

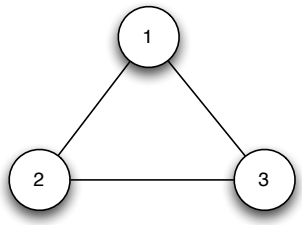

Figure 1: A distributed system comprising three participants trying to solve the consensus problem

Consider the synchronous network depicted in Figure 1, where up to $f = 1$ participant may fail. Assume that during the execution of the crash tolerant consensus, participant 1 fails in round 1, right before sending its value, and does not recover. Is the consensus still reached after 2 rounds? Why?

Duration: 10 min

Exercise 3: The Byzantine-tolerant consensus game

Form groups of $n = 4$ or $n = 5$ students to run the Byzantine synchronous consensus seen during the lecture with $f = 1$. Assign an identifier from 1 to n to each of your group member.

Stack n other papers with "Byzantine" written on one paper and "correct" on the $n-1$ others, place them upside down and mix them. Each group member picks one paper to know how to behave:

- If you pick "Byzantine" your goal is to try to make the algorithm fail by proposing the values of your choice to others and without revealing that you are misbehaving.
- If you pick "correct" your goal is to run the Byzantine synchronous consensus algorithm correctly.

Each pair of members exchange values without letting others know and writes down the values they receive. Do the same secret exchanges with the vectors of values. If the game is successful, all correct should have the same values. If not, try to identify what you did wrong during the protocol.

Duration: 25 min

Exercise 4: Consensus in Blockchains

4.1 When the difficulty target field of a block header contains **`0x1903130c`**, what is the difficulty target in hexa decimal for this particular block?
Note: This notation expresses the difficulty target as a coefficient/exponent format, with the first two hexadecimal digits for the exponent and the next six hex digits as the coefficient. The formula to calculate the difficulty target from this representation is:

```
target = coefficient * 2^(8 * (exponent - 3))
```

4.2 What is the difficulty target in terms of bits.

4.3 Explain the task of a miner in mining the next valid block with this difficulty target.

4.4 If two miners roughly at the same time produced two blocks with following two hashes. Are they valid hashes and why ? What is the consensus algorithm used by Bitcoin in such scenarios ? Which block will be appended to the main blockchain and why ?
Block 1: 0000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569
Block 2: 00000000000000005a64bd65a438c0374c55529305185aaaa44542b01284f056

4.5 Why the difficulty target is adjusted at every 2016 blocks?

4.6 Consider a scenario where a malicious attacker Mallory goes to Carol's gallery and purchases a beautiful triptych painting depicting Satoshi Nakamoto as Prometheus. Carol sells "The Great Fire" paintings for $250,000 in bitcoin, to Mallory. Once the transaction is verified

and included in a block after approximately 10 minutes, Carol wraps and hands the paintings to Mallory. If Mallory works with an accomplice, Paul, who operates a large mining pool, explain how Mallory may do a double spending attack.

4.7 Under what circumstance Mallory and Paul can guaranteed to be successful in their attack?

4.8 What cloud have been done differently by Carol to avoid such attacks against his bussiness?

4.9 In addition to a double-spend attack, describe another potential consensus attack that can be carried out by an attacker with majority of mining power.

Duration: 20 min