Engineering Blockchain and Web3 Apps
Problem Set #2

Problem 1. Bitcoin proof-of-work. Why is the difficulty of the proof of work in Bitcoin set to ten minutes? What would go wrong if it were changed to ten seconds?

Problem 2. Bitcoin consensus. Suppose two groups independently implement the Bitcoin protocol. Some miners run implementation A and other miners run implementation B. At some point an attacker finds a vulnerability in implementation A that causes miners running that implementation to accept transactions that double spend a UTXO. Implementation B treats such transactions as invalid.

a. Suppose 80% of the mining power runs the buggy implementation and 20% runs the non-buggy one. What will happen to the blockchain once a block containing a double-spending transaction is submitted to the network?

b. What will happen to the blockchain in the reverse situation where 20% of the mining power runs the buggy implementation and 80% runs the non-buggy one?

Problem 3. Energy consumption of Bitcoin mining. In this exercise we look at two estimates for the amount of energy consumed by the Bitcoin network. Assume in your answer that the current exchange rate is 1BTC = US$10000 and that there are no transaction fees (only the block reward of 6.25BTC per block). Recall that energy is measured in killoWatt-hours (kWH). You may assume that one bitcoin block is generated every 10 minutes exactly.

a. Estimate the network's hourly energy consumption assuming the entire block reward is spent on electricity for mining. Use US$0.05/kWH as the price of energy and express your answer in kWH.

b. Next, estimate the network's hourly energy consumption assuming all mining is done using Antminer S9 Hydro devices. Each device has a hash rate of 18 terra-hash /sec (one terra-hash is one trillion hashes) and consumes 1.7 kW of power (running the device for an hour consumes 1.7 kWH of energy). Assume the current difficulty of generating a bitcoin block is $D = 2^{75}$.

c. Can the difficulty ever become so great that your answer for part (b) becomes larger than your answer for part (a)? For your answer, you may assume that Antminer S9 Hydro is the best mining device available.

Problem 4. Streamlet. In class we discussed the StreamLet protocol where nodes notarize a block if it has 2/3rd of the vote, and finalize a chain up to the second to last block if the chain ends with three notarized blocks from consecutive epochs, e.g. 7-8-9. Suppose we relax the Streamlet finalization rule so that nodes consider a chain finalized up to the second to last block if the chain ends with three notarized blocks from four consecutive epochs, e.g. 7-8-10. Come up with an adversary that can break consistency. Here you may assume that the network is not synchronized so honest nodes can receive blocks out of order

Problem 5. Ethereum.Bob posts the following wallet contract to Ethereum to manage his personal finances:

```
contract BobWallet {
    function pay(address dest, uint amount) {
        if (tx.origin == HardcodedBobAddress)
```

```
            dest.send(amount);
        }
    }
```

The function pay lets Bob send funds to anyone he wants. Suppose Mallory can trick Bob into calling a method on a contract she controls. Explain how Mallory can transfer all the funds out of Bob's wallet into her own account.

Hint: Make sure you understand the semantics of `tx.origin`.