

# XCS251 Assignment 3: Important topics of blockchain

---

**Due Sunday, October 2 at 11:59pm PT.**

## Guidelines

1. If you have a question about this assignment, we encourage you to post your question on slack channel.
2. Familiarize yourself with the collaboration and honor code policy before starting work.

## Submission Instructions

You should submit a PDF with your solutions online in Gradescope. As long as the PDF is legible and organized, the course staff has no preference between a handwritten and a typeset  $\text{\LaTeX}$  submission. If you wish to typeset your submission and are new to  $\text{\LaTeX}$ , you can get started with the following:

- Download and install [Tex Live](#) or try [Overleaf](#).
- Submit the compiled PDF.

## Honor code

We strongly encourage students to form study groups. Students may discuss and work on assignment in groups. However, each student must write down the solutions independently, and without referring to written notes from the joint session. In other words, each student must understand the solution well enough in order to reconstruct it by him/herself. In addition, each student should write on the assignment the set of people with whom s/he collaborated. Further, because we occasionally reuse problem set questions from previous years, we expect students not to copy, refer to, or look at the solutions in preparing their answers. It is an honor code violation to intentionally refer to a previous year's solutions. More information regarding the Stanford honor code can be found at <https://communitystandards.stanford.edu/policies-and-guidance/honor-code>.

## Introduction

In this assignment, we will examine several important topics of blockchain. First, we will look into Nakamoto consensus and Streamlet, a simple and permissioned consensus protocol, to better understand the consensus design behind Bitcoin blockchain. Second, we will calculate the energy consumption of the Bitcoin blockchain and do two estimates to understand different considerations. Third, we consider mining pool sabotage and how two miners can synchronize the transactions in their mempool. Finally, a Ethereum smart contract is provided to demonstrate a potential attack. By the end of this assignment, you should have a good understanding of Nakamoto consensus and energy consumption behind the Bitcoin blockchain. You should also have a good understanding of the structure and security consideration of Ethereum smart contracts.

**Problem 1.** 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.** 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.** 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  $1\text{BTC} = \text{US\$}10000$  and that there are no transaction fees (only the block reward of  $6.25\text{BTC}$  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  $\text{US\$}0.05/\text{kWh}$  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 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  $D = 2^{75}$ . Recall that proof of work with difficulty  $D$  means given  $x$  find  $y$  such that  $H(x, y) < 2^{256}/D$ .

- 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. Mining pool sabotage.** In class we discussed the high variance of individual miners' earnings due to very high variance for time between block rewards and mentioned that individual miners can join mining pools to lower the variance of their earnings, while keeping the same expected returns. Here is how mining pool works. First, a mining pool authority provides block templates to each participant and assigns subproblems with lower difficulty to each participant of the pool. Second, each participant varies nonce to try to pass subproblem, and when a participant solves a subproblem, they submit the share (PoW solutions that are valid at a lower difficulty) to the pool authority. Then the pool authority will give another block template to the participant and assign another subproblem with lower difficulty to solve. As a result, participants repeatedly submit shares to prove how much work they are doing. Finally, when a participant of the pool solves a subproblem that also passes the bitcoin target difficulty, the coinbase from that block is split among the participants in proportion to the number of shares each submitted. Now, one risk of this is sabotage, in which a participant submits shares, but withholds full solutions if they are found (no coinbase is awarded for these withheld solutions).

- a. Consider a participant with mining power  $\beta \in [0, 1]$  (as a fraction of global mining power) in a pool with total mining power  $\alpha \in [0, 1]$  (as a fraction of global mining power), where  $\beta < \alpha$ . What is the expected fraction of the overall mining rewards (the rewards collectively earned by the entire network) that this individual will earn if he or she mine honestly? Assume rewards are distributed proportionally to the number of shares submitted by each participant.

**Hint:** There is no need for complicated expectation calculations throughout this entire question.

- b. What is the expected fraction of the overall mining rewards (the rewards collectively earned by the entire network) that this individual will earn if it devotes all of its power to sabotage?

**Hint:** Because  $\beta$  power is no longer used to find blocks, the total network mining power is now only  $(1 - \beta)$  times its full power. Therefore,  $P$ 's useful mining power, as a fraction of the entire network, is now  $(\alpha - \beta)/(1 - \beta)$ .

- c. Now consider two pools,  $P_1$  and  $P_2$  with mining power  $\alpha_1$  and  $\alpha_2$ , respectively. What will  $P_2$ 's expected share of the total earnings be if it dedicates  $\beta < \alpha_2$  power towards sabotaging  $P_1$ ? Note that when  $P_2$  finds a block, it gets the entire coinbase. When  $P_1$  finds a block,  $P_2$  receives a fraction of the coinbase proportional to the number of shares  $P_2$  generated while mining for  $P_1$ .

**Hint:**  $P_1$ 's total mining power is now  $\alpha_1 + \beta$ , but only  $\alpha_1$  is used for finding a new block.

- d. Provide concrete values for  $\alpha_1, \alpha_2, \beta \in [0, 1]$  in which this attack is profitable for  $P_2$  over honest behavior. You only need to provide one set of values for which this attack is profitable.

**Problem 6. Synchronizing the mempool across miners.** Miners  $A$  and  $B$  each have a set of transactions in their mempool. Suppose that miner  $A$ 's set is a superset of miner  $B$ 's. Miner  $A$  wants to send to  $B$  the transactions that  $B$  is missing. The problem is that  $A$  does not know which transactions  $B$  is missing. Now, suppose  $B$  is only missing one transaction. Show that  $A$  can send a single 32-byte message to  $B$  that quickly lets  $B$  identify the missing transaction hash.  $B$  will send the missing transaction hash to  $A$ , and  $A$  will send back the transaction data.

**Hint:** Think of computing the xor of all the transaction hashes in  $A$ 's mempool.

**Problem 7.** 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`.