COMP 4901W – Homeworks 4 and 5

A. K. Goharshady

Release Date: March 21, 2022
Deadline: April 12, 2022 (23:59 HKT)

Due to the unexpected pace of the smart contracts part of the course, we had to merge homeworks 4 and 5 together. As such, you will be given extra time (until April 12) for this joint homework. This homework accounts for 20% of your total grade. You should submit your main solution, i.e. a document explaining the logic behind every code, on Canvas as a single pdf file. Your codes should be submitted as `.sol` files. As usual, handwritten and scanned solutions will not be accepted since the TAs might be unable to read your handwriting. However, you can draw your figures, if any, by hand. You are also allowed to discuss the problems with your classmates but you have to write your solution and codes entirely on your own. All submissions will go through a plagiarism check. If you submit the same solutions as another student, you will both get a grade of F for the whole course. The deadline is firm and no extensions will be granted. You will receive feedback on your submission and normally be allowed to resubmit once. We reserve the right to disallow resubmissions if your original submission is of a very low quality, does not compile, or shows a lack of effort.

Important: In each of the exercises, you have to provide both the smart contract and an explanation of its flow, i.e. who calls which function in which order.

Exercise 1

This exercise accounts for 10% of your total grade.

Implement a Solidity smart contract that allows Alice and Bob to play a game of Rock–Paper–Scissors on the Ethereum Blockchain. Each party should first put a deposit of 1 ETH and then 2 ETH is paid to the winner of the game. If the game ties, each party receives 1 ETH back. You can hard-code the addresses of both Alice and Bob in your contract.

- Prove that neither party can cheat in your contract.
- Prove that no third-party can tamper with the game by changing or censoring the messages sent by either party.

Submit your code as a single file named `rps.sol`.

Exercise 2

This exercise accounts for 10% of your total grade.

Consider a simple auction in which people can bid for a specific item. Assume that the auction runs for 24 hours and anyone can enter a bid in this period. However, the bids must remain secret until the end of the bidding period. After the bidding ends, the winner should be announced and everyone must be able to independently verify that no cheating has taken place.

1. Implement a Solidity smart contract that performs the simple auction mentioned above.
2. What happens if the person with the highest bid refuses to pay? Provide a variant of your contract in which we can ensure payment by the highest bidder. Note that the bids should still remain hidden during the bidding period.
3. How much gas do your contracts use? Make sure the amount of gas used by each participant is no more than a fixed constant and find this constant.

Submit your codes as two files named `auction1.sol` and `auction2.sol`.