University of Edinburgh Blockchains & Distributed Ledgers	Fall 2019-20
Due: Monday 11.11.2019	Instructor: Aggelos Kiayias Teaching Assistant: Dimitris Karakostas

Ethereum Smart Contract Development

The purpose of this project is to get familiar with the deployment of and interaction with smart contracts on the Ethereum blockchain. You can obtain ethers and connect to our private Ethereum blockchain in order to use them by following the instructions here.

The project is composed of two parts:

1. The Cookie Monster
2. The Morra game

The Cookie Monster

In the first part of the project you will have to compile and interact with a smart contract. You can find the contract's code here. In order to compile and interact with it you can use Remix. The goal of this part is to understand what the code of the smart contract does and use your ether to feed the Cookie Monster and post a message on the leaderboard at least once. *Your goal should be to try and collect the contract's rewards.*

You can post whatever messages you want to the leaderboard when feeding the monster (but remember that Ethereum is not anonymous). The leaderboard can be found here and the deployed contract's address is: *0x95f225e951f5204F553715C30CFa89AEeaEAD181*

Report

Your report should contain:

- A description of the smart contract's functionality.
- A short decsription of your strategy in trying to collect the rewards.
- The transaction id, address, and message you used to post a message on the leaderboard.

Morra ✌

The second part of the project will focus on writing your own smart contract to implement the Morra game. The contract will allow two players (A and B) to play a game of Morra at any point in time. Each player picks a number between 1-5 and also guesses which number their fellow player has picked. They both show their hands and, in case only player A guesses correctly, A wins and is rewarded x Ether, where x is the sum of the numbers both players guessed (similarly if B wins). After the game ends, a player can initiate a new game with the contract.

You will have to implement the smart contract and deploy it in our private Ethereum ledger. After deploying your contract, you should engage with other students' contracts in order to win more ether and feed the Cookie Monster. Before you engage with a fellow student smart contract you should evaluate their code and analyze its features in terms of fairness (refer to Lecture 04).

Report

Your report should contain:

- A detailed description of the high-level decisions you made for the design of your contract, including (but not limited to):
    - When and how is the deposit amount of each game decided and committed?
    - How are the winnings sent to the winner?
    - What happens in case of a draw?
- A detailed gas evaluation of your implementations, including:
    - The cost of deploying and interacting with your contracts
    - Whether your contracts are fair to both players or whether one has to pay more than the other
    - Techniques to make your contract more cost effective and/or fair
- A thorough listing of potential hazards and vulnerabilities that can occur in the smart contract. Provide a detailed analysis of the security of mechanisms that you have found to mitigate these hazards.
- A description of your analysis of your fellow students' contracts, including:
    - Any vulnerabilities discovered?
    - How could a player exploit any the vulnerabilities to win the game?
- The transaction history of an execution of a game of Morra.
- The code of your contract, properly annotated.

Submission

Your report for both parts should be submitted as a hard copy to ITO with a cover page including just your name, student number and course details. Late submissions will not be accepted.

Experimentation

You are free to experiment with our private blockchain and deploy smart contracts to see how they work. However, you will only be given a fixed amount of Ether, so you should use it wisely.