University of Edinburgh Blockchains & Distributed Ledgers	Fall 2018-19
Due: Friday 16.11.2018	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 King of Ether game
2. The rock-paper-scissors game

The King of Ether

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 become the King and appear on the leaderboard at least once.

The contract will be constrained to 50 Ether contributions for 10 days, so that everybody can become King during that time period (given the amount of Ether you will get). You can post whatever messages you want to the leaderboard when becoming kings (but remember that Ethereum is not anonymous).

The leaderboard of Kings can be found here and the deployed contract's address is *0x65840e9c5dbbf36a7aed1cce4893b2f1218bcd6a*.

At the end of the semester, whoever is at the top of the leaderboard will be named King of the BDL project for 2018.

Report

Your report should contain:

- A short description of the smart contract's functionality;
- The transaction id, address and message you used the first time you became the King.

Rock-paper-scissors ✊✋✌

The second part of the project will focus on writing your own smart contract. You will have to code a contract that implements the rock-paper-scissors game (you can also extend it to lizard-Spock if you feel like it).

The contract will allow two players to play a game of rock-paper-scissors at any point in time. Each player will have to deposit the same amount of Ether to the contract at the beginning of a game. Then each player will commit to its hand. Finally, both players will reveal their hand and the winner is awarded both deposits. After the game has ended, a player can initiate a new game with the smart 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 become the King. 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-05).

Report

Your report should contain:

- A description of your analysis of your fellow students' contracts, including:
  - Any vulnerabilities discovered?
  - Is there a way for a player exploit any of the vulnerabilities to win the game?
- A description of mechanisms that you have found that can mitigate vulnerabilities.
  - Provide a detailed analysis of their security.
- A description of your high-level decision choices for the design of your contract, such as:
  - How is the deposit amount of each game decided?
  - How are the deposits sent to the winner?
- A gas evaluation of your implementations, such as:
  - Are your contracts fair to both players or does one have to pay more than the other?
  - How would you make your contract more fair?
- The transaction history of a game execution;
- 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, note that you will be given a fixed amount of Ether, so you should use it wisely - especially if you plan on being the King by the end of the course.