University of Edinburgh	Fall 2017-18
Blockchains and Distributed Ledgers	Kiayias
Due: 19.11.2017	Project

Ethereum - Smart Contract Lottery

In this project you have to familiarize yourself with the way Ethereum smart contracts are designed and deployed. The general objective is to write a smart contract that performs the following actions.

- Accept ether and issue an amount of tokens at a certain fixed exchange rate between ether and your token. You are free to decide the exchange rate.
- The smart contract should maintain the token balances and the addresses that correspond to them.
- When the balance of ether is above a certain threshold, then you should find a way to access the hash value of the head of the chain and use that value to choose at random one of the token holders with probability proportional to the number of tokens they hold. Subsequently, issue a transaction that transfers all the ether held by the contract to the stakeholder selected.
- The contract should continue operating, issuing new tokens, and running lotteries as prescribed.

Instructions. To connect to our private Ethereum blockchain, follow the steps described here:
`https://github.com/solegga/blockchaincourse/blob/master/How_to_connect_to_university_of_edinburgh_private_blockchain.pdf`

After you deploy your contract, find three other students in the class and acquire tokens from their contracts. Monitor your own smart contract to ensure that at least once the lottery has taken place. If the lottery has not taken place, try to solicit the help of other students so that they buy tokens and the lottery takes place at least once.

You should prepare a report that contains (i) The high level description of your contract code as well as its address. (ii) The full analysis that explains how a winning stakeholder is selected by your contract with an explanation regarding any deviation from the ideal distribution, if your contract exhibits any. Your analysis should use tools such as statistical distance (covered in the Introduction to Modern Cryptography course). (iii) A complete narrative of all the steps that you have undertaken in the deployment of your contract and your engagement with other contracts written by other students. (iv) You should include a table that shows how much gas your contract requires for deployment and token acquisition. With respect to token acquisition find the gas that is required by each step of the contract execution and then explain all possible differences in gas consumption depending on the state of the contract and transaction input. (v) Provide a detailed answer to the question: is your smart contract fair to all its users? i.e., is everyone charged the same amount of gas to interact with it? (vi) Find ways to optimize your code (a) in terms of using as little gas as possible, (b) in terms of being fair, if you answered negatively in question v, above. Demonstrate your optimizations by deploying an improved smart contract and explaining the improvements with a table showing how a specific operation uses less gas or explaining why it is fair. (vii) Present your actual smart contracts code in the report properly annotated and documented. Also include the full transaction history of your wallet and your smart contracts (the ones that you submit for evaluation).

Submission. Your report should be submitted as a PDF 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 and you should use it wisely.