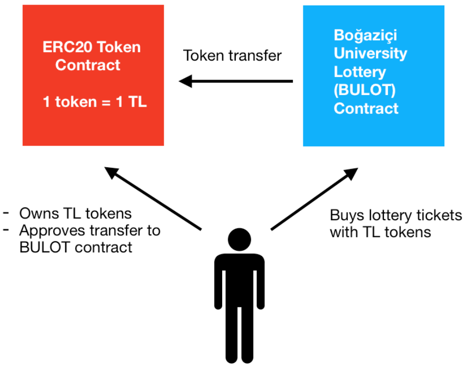
CMPE 483 Sp. Top. in CMPE Blockchain Programming
Fall 2019
Homework 1 (due Nov 25th)

(The project can be done in groups of at most three students)

Implement an autonomous decentralized lottery (called Bogazici Lottery(BULOT)) as a Solidity smart contract. One lottery round lasts two weeks. A new lottery round starts right after the previous one is completed. Each lottery ticket costs 10 TL paid with 1:1 TL tokens to the lottery contract.


ERC20 Token Contract
1 token = 1 TL
Token transfer
Boğaziçi University Lottery (BULOT) Contract
- Owns TL tokens
- Approves transfer to BULOT contract
Buys lottery tickets with TL tokens

Winner tickets will be selected by computing random numbers that determine each winner ticket. A random number is to be supplied by the ticket purchasers. The lottery should employ commitment (submission) and reveal stages. The details of how a random number can be generated is given here:

https://ethereum.stackexchange.com/questions/191/how-can-i-securely-generate-a- random-number-in-my-smart-contract

The stages of each lottery round are scheduled as follows:

a) Ticket purchase and random number submission stage : One week.

b) Random number reveal stage : One week. Note that if previously submitted random numbers are not submitted correctly in the reveal stage, the chance of winning is lost. Also, no ticket refund is made in this case.

Lottery 1	Purchase/ Submission (1 week)	Reveal (1 week)		
Lottery 2			Purchase/ Submission (1 week)	Reveal (1 week)
....				...

Let *M* be the amount money collected from the sale of tickets at the current lottery. The *i*th prize P_i will be awarded to the winners as follows:

$$P_i = \lfloor M/2^i \rfloor + (\lfloor M/2^{i-1} \rfloor \mod 2) \qquad i = 1,\ldots,\lceil log_2(M) \rceil$$

Note that a winning user should be able to withdraw his prize anytime after the lottery round ends. Also, it is possible that a ticket may win more than one ticket.

Grading

Your project will be graded according to the following criteria:

Documentation (written document describing how you implemented your project and also showing the correctness of your implementation)	30%
Comments in your code	10%
Correctly functioning Solidity code, test scripts and tests	60%

Late Submission

If the project is submitted late, the following penalties will be applied:

0 < hours late <= 24 :	25%
24 < hours late <= 48 :	50%
hours late > 48 :	100%

Timestamping

Project file should include your names in it. Please timestamp your project file using https://opentimestamps.org/ before you submit it. Keep the project file and its corresponding timestamp .ots file.