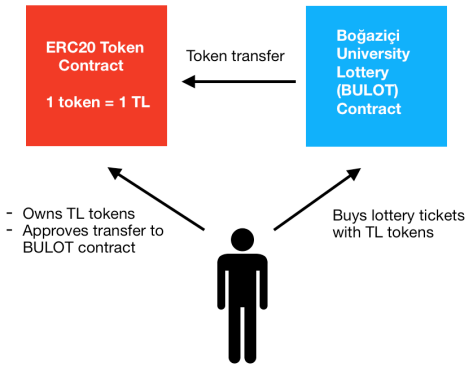
CMPE 483 Sp. Top. in CMPE Blockchain Programming
Fall 2020
Homework 1 (due Jan 9th)
(The project can be done in groups of at most three students)

Implement an autonomous decentralized lottery (called Bogazici Lottery (BULOT)) as a Solidity smart contract. One lottery round lasts two weeks and consists of two stages. A new lottery round starts right after the first stage of previous one is completed. A lottery ticket costs 10 TL.



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 (i) ticket purchase and random number submission (ii) reveal stages. The details of how a random number can be generated in order to determine winners 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 in an overlapping manner:

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/ Random No Submission (1 week)	Reveal (1 week)	
Lottery 2		Purchase/ Random No Submission (1 week)	Reveal (1 week)

....

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

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

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.

Your implementation should provide the following interface (and only the following interface) to the external world:

```
function buyTicket(bytes32 hash_rnd_number) public
function revealRndNumber(uint ticketno, uint rnd_number) public
function getLastBoughtTicketNo(uint lottery_no) public view returns(uint)
function getIthBoughtTicketNo(uint i,uint lottery_no) public view returns(uint)
function checkIfTicketWon(uint lottery_no, uint ticket_no) public view returns (uint amount)
function withdrawTicketPrize(uint lottery_no, uint ticket_no) public
function getIthWinningTicket(uint i, uint lottery_no) public view returns (uint ticket_no,uint amount)
function getCurrentLotteryNo() public view returns (uint lottery_no)
function getMoneyCollected(uint lottery_no) public view returns (uint amount)
```

You should also prepare a table of gas usages for the interface functions and discuss them.

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). You should also provide average gas usages for the interface functions.	30%
Comments in your code	10%
Correctly functioning Solidity code, test scripts and tests	60%

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.