CMPE 483 Sp. Top. in CMPE Blockchain Programming
Fall 2018
Homework 1 (due Nov. 29th)
(The project can be done in groups of at most three students)

Implement an autonomous decentralized lottery as a Solidity smart contract. One lottery runs for a period of one week. A new lottery round starts right after the previous one is completed. There are 100000 lottery tickets each having a ticket number in the range 00000…99999. Each ticket costs 2 ethers. Prize distribution is as follows:

All 5 digits of the ticket										
Prize	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
Amount	50000	10000	400	400	200	200	200	200	200	200
Prize	11th	12th	13th	14th	15th	16th	17th	18th	19th	20th
Amount	200	200	200	200	200	100	100	100	100	100

Ending in 4 digits of the ticket: XXXX
Prize Amount: 40 ether each

Ending in 3 digits of the ticket: XXX
Prize Amount: 10 ether each

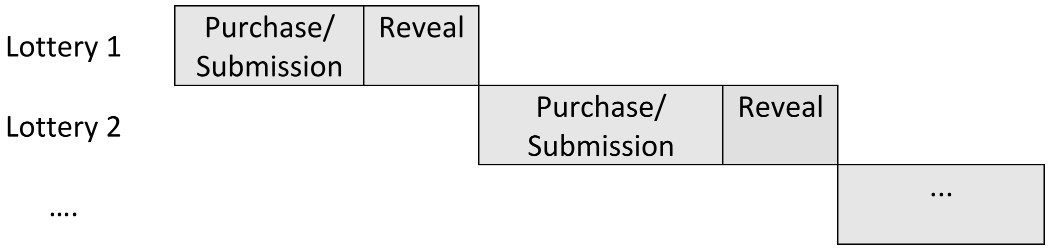
Ending in 2 digits of the ticket: XX
Prize Amount: 4 ether each

23 categories winner tickets (see above prizes) will be selected by computing random numbers that determine each winner ticket. One random number is to be supplied by the ticker 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 : 5 days.
b) Random number reveal stage : 2 days. Note that if previously submitted random number is not submitted correctly in the reveal stage, the chance of winning is lost.



Please note the following:

- If enough money is not collected to pay for all the prizes, then the cost of tickets will be refunded during the reveal stage. If enough money is collected to pay for all the prizes, then no refund will be made (even if the random number is not revealed during the reveal stage).

- A winner should be able to withdraw his prize anytime after the lottery round ends.
- The money left over after allocating for the prizes, will be donated to a charity. The address of the charity should be set in the constructor of the smart contract.

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%