**CMPE 483 Sp. Top. in CMPE Blockchain Programming**
**Spring 2018**
**Homework 1** (due April 9th)
(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 40000 blocks. A new lottery round starts right after the previous one is completed. Lottery tickets are offered in three forms:

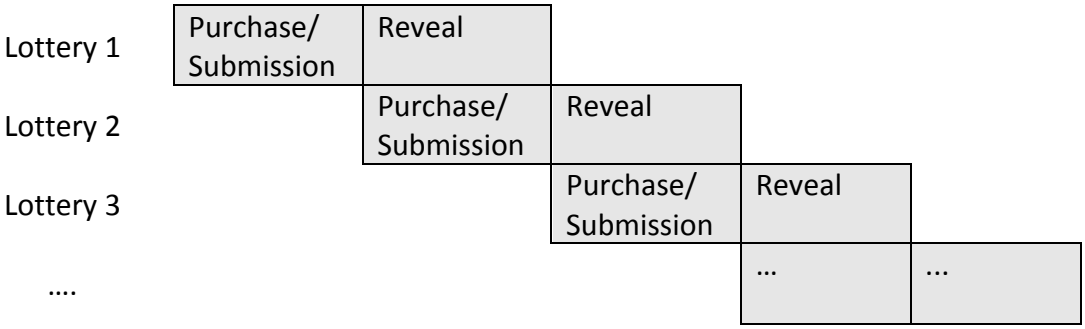
- A full ticket which costs 8 finneys,
- A half ticket which costs 4 finneys,
- A quarter ticket which costs 2 finneys.

Three unique winner tickets will be selected by computing random numbers that determine each winner ticket. Three random numbers are 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 : blocks 0..19999.
b) Random number reveal stage : blocks 20000…39999. 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.




Let M be the amount money collected from the sale of tickets at the current lottery round plus the amount that was carried over to the current round from the previous round. The following prizes will be awarded to the winners:

| Prize | Full ticket | Half Ticket | Quarter Ticket |
|---|---|---|---|
| 1st Prize | M / 2 | M / 4 | M / 8 |
| 2nd prize | M / 4 | M / 8 | M / 16 |
| 3rd Prize | M / 8 | M / 16 | M / 32 |

Note that a winning user should be able to withdraw his prize anytime after the lottery round ends.

**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%
- 48 < hours late <= 72 : 75%
- hours late > 72 : 100%