CMPE 483 Sp. Top. in CMPE Blockchain Programming Fall 2018

Baran Kılıç
2014400123

December 6, 2018

1 Implementation

When the contract is deployed, the lottery starts. The address of charity is needed when deploying because the money left over after allocating for the prizes will be donated to this charity.

The information about each lottery is stored in an array. When a person buys a ticket or tries to reveal the random number or gets refund, the lottery array is updated. If the last lottery is ended, new lotteries are created. A new lottery round starts right after the previous one is completed. In this way, the lottery array always remains up-to-date.

There are 100000 lottery tickets each having a ticket number in the range 00000...99999.

The lottery consists of two periods. The first period is for purchasing ticket and committing a random number. The second period is for revealing the random number. After this two periods, the ticket holder can withdraw his prize. The separation into two periods is necessary because if a purchaser reveals their random number immediately, others may choose their random number according to this random number.

The start and end dates of purchase and reveal periods for lottery are calculated from index of lottery and the start date of the first lottery.

In the purchase period, one can buy a ticket with 2 ethers with the buyTicket function. The submission of a ticket number and the hash (keccak256) of random number together with the address of purchaser is necessary. The buyer can use the calculateRandomNumHash function,which is a pure function, to calculate the hash. The function returns a week number. This number is necessary when withdrawing the prize.

In the reveal period, one can reveal their random number. If enough money for prizes is not collected, the ticket fee is refunded. If enough money is collected the correctness of commitment is checked. If previously submitted random number is not submitted correctly in the reveal stage, the chance of winning is lost.

There are 23 categories of prizes. Therefore, 23 random numbers must be calculated. The random numbers are calculated by summing the user submitted random numbers and taking the least significant digits using modulo operation. For 23 random numbers, there are 23 sums. Each submitted random number is added to the next sum in a circular manner. The random numbers are added to the sum during revealing operation.

The "transfer" function is used for sending money and the status of necessary variables are updated before using "transfer" to prevent reentrancy attacks.