BULOT Smart Contract Documentation

Installation:

1. Install geth and parity
2. Create a directory called PARITYDATA
3. Use the command in the parity\_command.txt file. Change –base-dir path to the full path of PARITYDATA folder.
4. Use the command in the geth\_attach.txt file. You should see the geth console.
5. Run test files by importing

Definition:

This program written in solidity is a lottery smart contract . Users can buy a ticket with 10 tokens in order to participate. Each token is equal to 1tl. Tokens-tl exchange are done using ERC20 Contact. There are two periods of the lottery: submission and reveal. In submission period users buy tickets, and in the reveal stage they need to reveal their random numbers. According to the reveals a random number is generated. By hashing this number multiple times, a number which is proportional to logarithm of revealers of users win the lottery. Each winner takes half of the token prize of the previous winner. The first winner takes approximately half of the total tokens that is collected via ticket prices. The lottery lasts forever.

The submission reveal stage works