BLOCKCHAIN - FINAL PROJECT

https://github.com/Pop-Vlad/Blockchain-Project

TEAM MEMBERS:

Galatanu Tiberiu-Adrian
Purcel Maria-Loredana
Pop Vlad
Hosu Dan-Marian

IDEA:

Our idea is to create a lottery on the Ethereum blockchain. The contract allows the users to exchange ETH for game tokens implementing the ERC-20 standard, called tickets. The users can use these tickets to take part in the lottery. A user can use 1 ticket for a chance to win and has a fixed probability of winning. The winner is decided based on generated random numbers. When a user loses they receive nothing and their token is added to the prize pool. When a user wins they receive a fixed percentage of the prize pool. The rest is kept in the prize pool to avoid the value of the prize pool being too small. When a user wins the amount of ETH corresponding to the accumulated prize pool is transferred to their account. The owner can extract the accumulated earnings from the contract fees. When the game starts, or if the prize pool is too small, the owner can add tokens to the prize pool to incentivize users to play the game and he can modify the percentage of tickets that are left in the prize pool when a user wins. The user can also view the prize pool, check it's own amount of tickets, view the owner fee and transfer tickets to another user.

DESCRIPTION:

To buy tickets, a user calls "buyTickets(uint256 nrTickets)", specifying the number of tickets they want to purchase. When calling the function they send a value greater or equal to the price of the tickets. The rest is returned to the user's account.

A user can try one ticket at a time by calling "tryTicket(uint8[] calldata numbers)". This consumes 1 of their tickets. The user supplies an array of 5 numbers to the function representing the numbers guessed. If the numbers are correct, they win and a certain amount of ETH is transferred to their account. This is provided by the

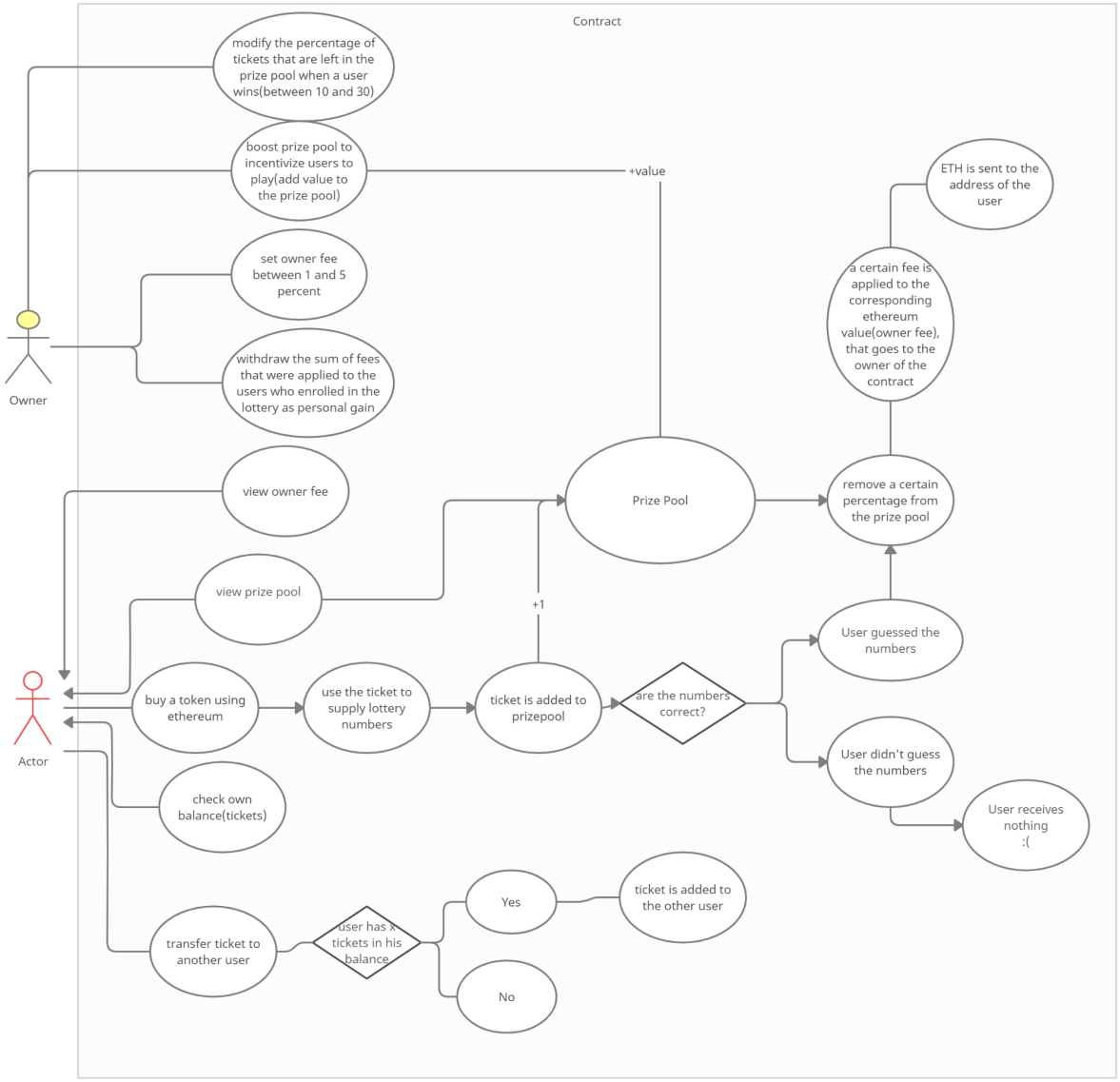
internal “win()” function and the amount won is: prizePool* (100-retainPrize)/100 * (100-exchangeFee)/100 * ticketPrice. Some of the prize is kept for the next winner (20%) and some is kept as fees for the owner (2%). The amount a user wins if they guess the numbers correctly is also given by the view function getPrize().

A user can also see the ticket price getTicketPrice(), the fee: getExchangeFee() and the retained prize percentage for the next user: getRetainedPrize().

The owner can withdraw the earnings of the contract’s fees with the withdrawEarnings() function. It returns the amount transferred to the owner. The amount the owner can withdraw is limited so it does not deplete the contract below the amount reserved for the winners:
uint256 reservedBalance = _totalSupply * (100 - exchangeFee) / 100 * ticketPrice;

The prize pool can be increased by boostPrize() function. It can be done from any account, but is normally done by the owner if the prize pool becomes too low, to incentivize users to use the lottery. The owner can also modify the fees (“updateFee(uint8 newFee)”) and retained prize pool (“updateRetainedPrize(uint8 newRetainedPrize)”), but only between some limits.

The winning conditions: The numbers given by the user calling “tryTicket(uint8[] calldata numbers)” are compared to some random generated numbers, using the “equal(uint8[] memory a, uint8[] memory b, uint8 n)” internal function. This compares 2 arrays of length n to check if they contain the same numbers (in any order). The random numbers are generated using “generateRandomDistinctNumbers(uint8 _sampleSize, uint8 _domainSize)”. This generates _sampleSize distinct numbers in {1, 2, 3, ... , _domainSize}. This function uses “randMod(uint _modulus)” to generate 1 number at a time in the set {0, 1, …, _modulus}. To ensure the numbers are distinct and their distribution is uniform, each number is chosen as: “uint8 r = uint8(randMod(_domainSize-i)) + 1”, where i is the number of numbers already generated. Then r is increased by 1 for each generated number smaller than itself. Then r is added to the sorted list of generated numbers.


Contract
modify the percentage of tickets that are left in the prize pool when a user wins(between 10 and 30)
boost prize pool to incentivize users to play(add value to the prize pool)
+value
ETH is sent to the address of the user
set owner fee between 1 and 5 percent
a certain fee is applied to the corresponding ethereum value(owner fee), that goes to the owner of the contract
Owner
withdraw the sum of fees that were applied to the users who enrolled in the lottery as personal gain
view owner fee
Prize Pool
remove a certain percentage from the prize pool
view prize pool
+1
User guessed the numbers
buy a token using ethereum
use the ticket to supply lottery numbers
ticket is added to prizepool
are the numbers correct?
Actor
User didn't guess the numbers
check own balance(tickets)
User receives nothing :(
Yes
ticket is added to the other user
transfer ticket to another user
user has x tickets in his balance
No