Decentralized Lottery

Abstract

Conventionally, dapp relies on the the future block hash for randomness, which has already been questioned since the bookkeepers can determine the random result without breaking any rules by filtering and/or reordering transactions when generating new blocks. This problem is especially serious in NEO, since we now only have four bookkeeper nodes.

This game provides a mechanism of generating genuine randomness. We make a lottery as the proof of concept of such system and hopefully it can provide other NEO developers some inspiration.

This system will take place in two rounds and ensure the winner is chosen completely at random. The steps are:

Set Up

To play the lottery, a user needs to have a wallet containing Neo GAS.

First Round

User will fill out a form with 3 pieces of data:

1. Chosen number of 4 bytes (0 - 4,294,967,296).
2. Amount of GAS required for the total number of entry tickets they wish to purchase
3. Their public key.

Once done, the user clicks “submit” and then needs to approve the transaction for the amount used to purchase the lottery ticket in their neo wallet client. The GAS will then be sent to a decentralized address through a smart contract.

(ex. 1 GAS = 1 entry)

Once transaction is approved the user’s computer will generate a random number through our client. This number will be generated by hashing (Chosen number, public key, system time) to produce a random number within the same range as the user’s picked number.

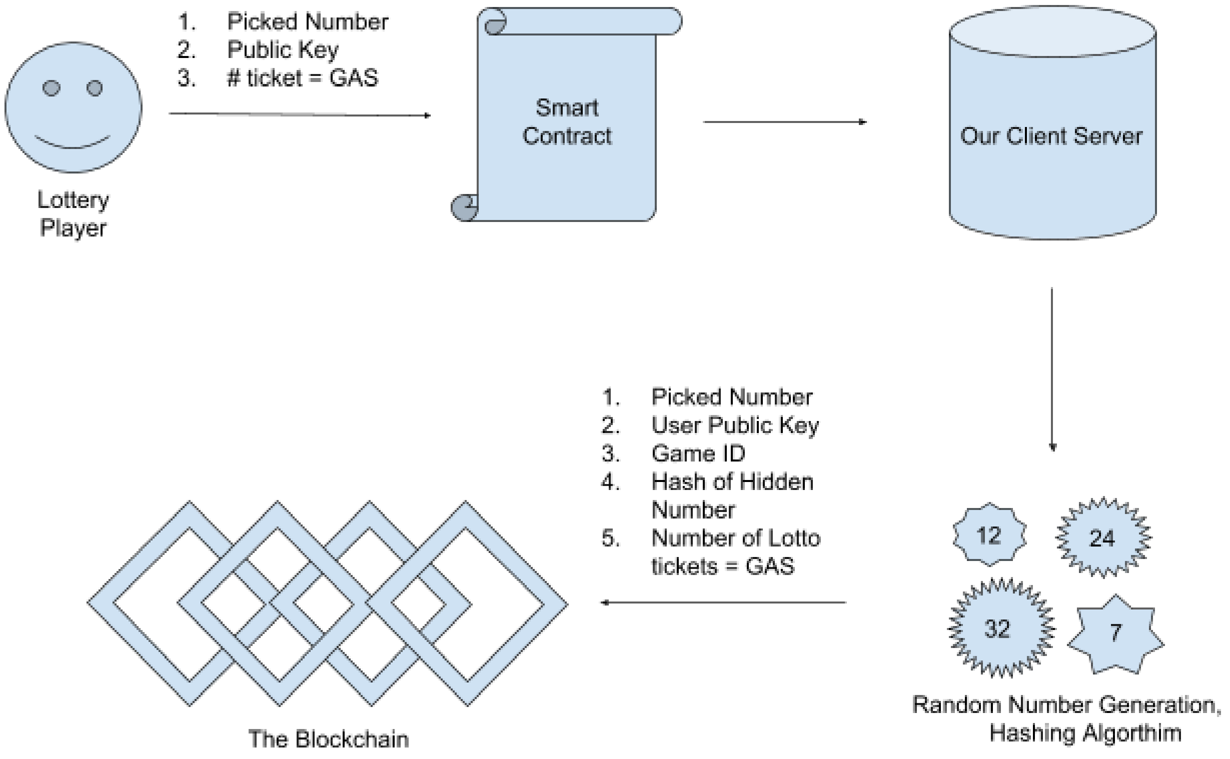
The random number generated is referred to as the “Hidden Number”. The system will now hash the hidden number with an open-source algorithm and produce a function referred to as the “Hash of Hidden Number”

The following 5 pieces of information are submitted onto the blockchain.

1. Game ID
2. Player's public key (PK)
3. Player's picked number
4. Amount of GAS paid = tickets purchased.
5. Hash of Hidden Number

Once the first round is completed, the system closes submission any new entries to the chain. No more lottery tickets will be sold.

Diagram illustrating processes of Decentralized Lottery, round 1

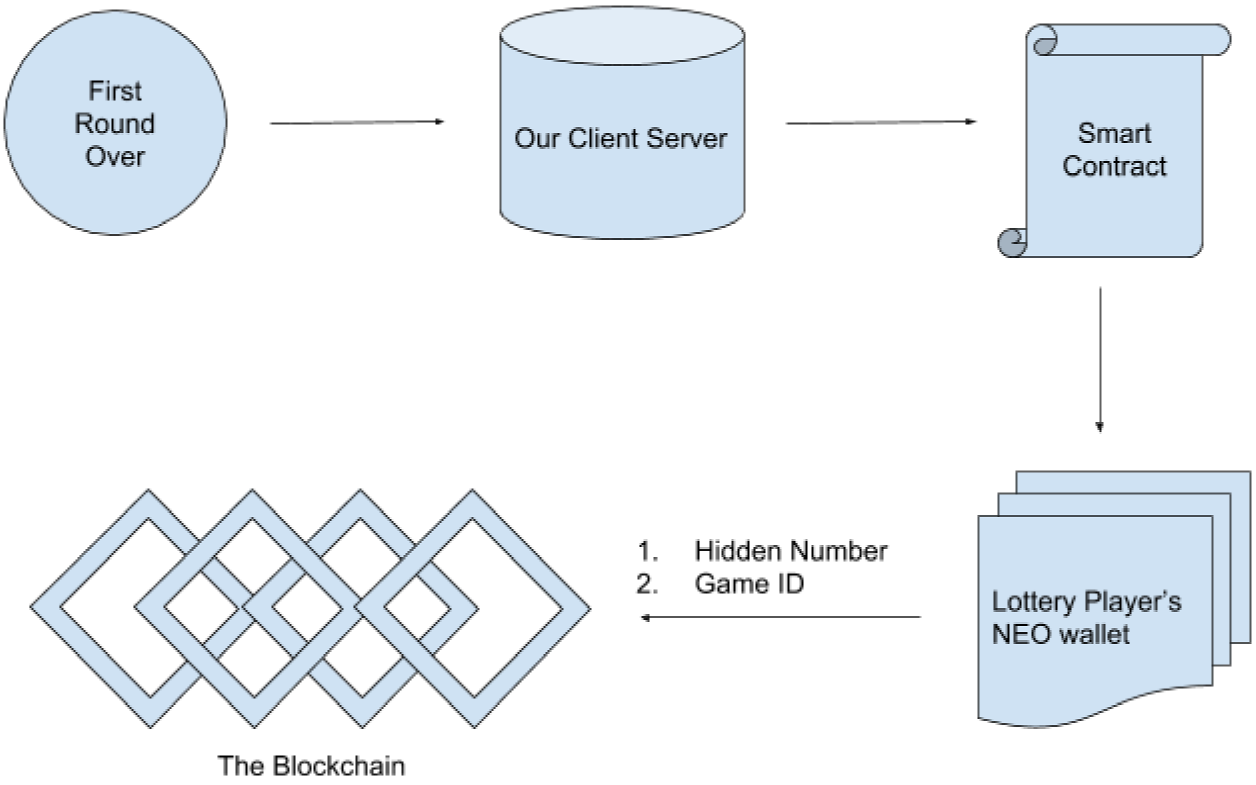


Second Round

All hidden numbers are posted to the chain from the user's wallet with the following data:

1. Game ID
2. Hidden number

Diagram illustrating processes of Decentralized Lottery, round 2

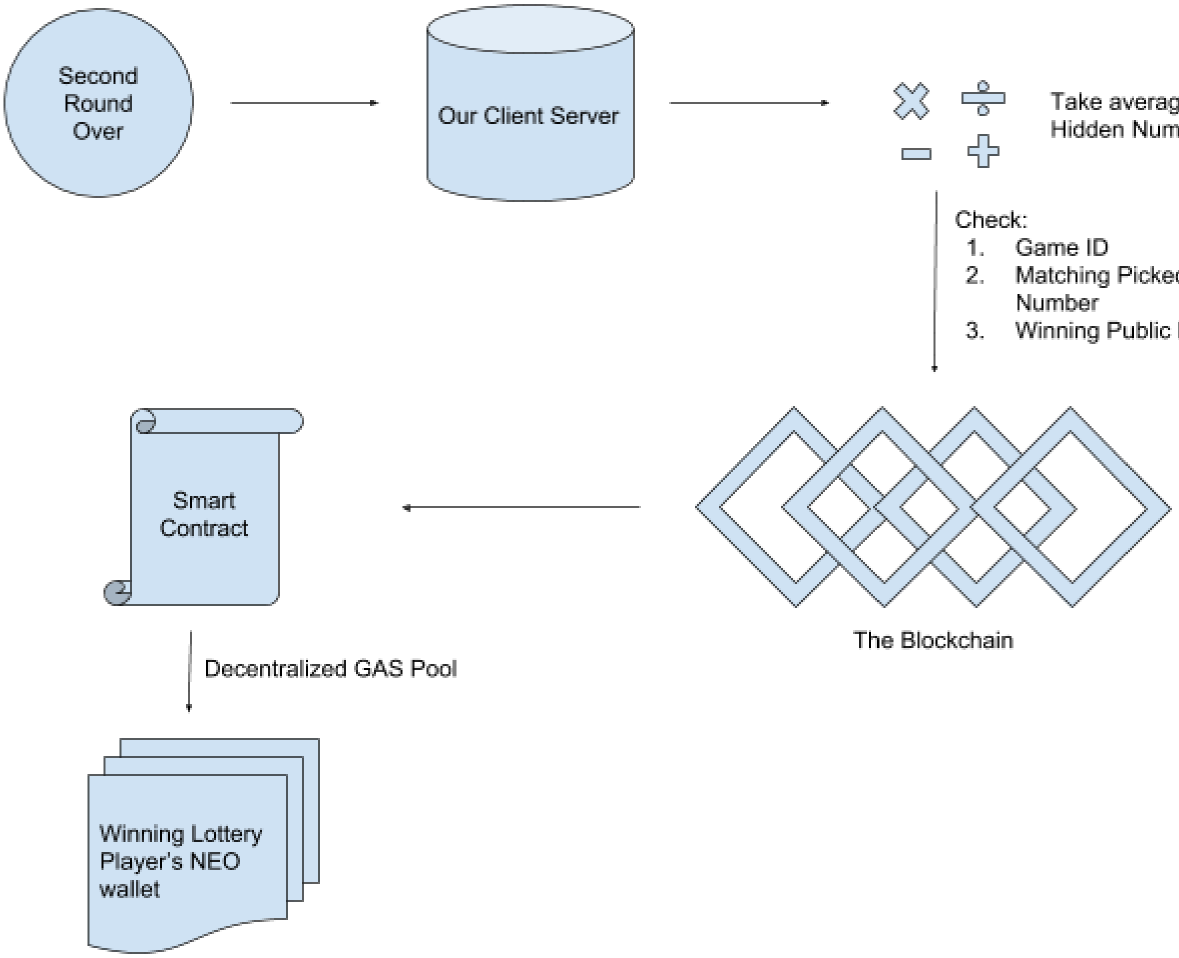


Determining the Winner

This ensures the user remains anonymous. Then the average of all the hidden numbers is used to determine the winner of the lottery by matching the hidden number average with the winning picked number by a user.

To match the number with the user, the winning number is hashed through the open algorithm, and if a user’s Hash of Hidden Number matched, the proceeds of the lottery are sent to their public key submitted with their original entry.

Check(gameID, playerAddress, Matching Picked Number)
Verifying the winner of the Decentralized Lotter in a decentralized fashion



Conclusion

The goal of this lottery is to run a completely decentralized system which creates randomness based on user submission. By leveraging the anonymity of the lottery numbers submitted, a system can perform a calculation on these numbers and determine the winner without any bias.