Randpool Protocol for powering Win-Win blockchain lotteries based on decentralized true randomness

Email: play@coinlotto.win

Randomized asymmetric entropy can be used to run a decentralized lottery on a public permissionless blockchain like Ethereum. A truly randomized entropic lottery is different than other lottery systems as it is impossible to manipulate. This is because no one knows the numbers entered into the lottery, preventing one from rigging the outcome to select a winning number. This is possible by breaking the lottery into 2 parts. The first part users select a number and submit a hash of this number along with other data to the block chain using asymmetric encryption. Second, their selected numbers are submitted to the chain unencrypted and used to generate a winning number using an open source algorithm and randomness derived from user input. This process will be known as "Randpool based on Asymmetric encryption" and the "Entropy" of user input to generate random numbers and decentralized the winning number selection process. The process is outlined in detail below.

Abstract: Conventionally, Decentralized Applications (Dapps) rely on the future block hash for randomness. This method has already been questioned since the bookkeepers/miners of the blockchain can determine the random result without breaking any rules by filtering and/or reordering transactions when generating new blocks. This game provides a mechanism of generating genuine randomness. 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 an ERC20-compatible wallet e.g. Metamask containing Ether 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 lottery entry tickets they wish to purchase
3. 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 ERC-20-compatible wallet or Metamask wallet client. The GAS will then be sent to a decentralized address through a smart contract.

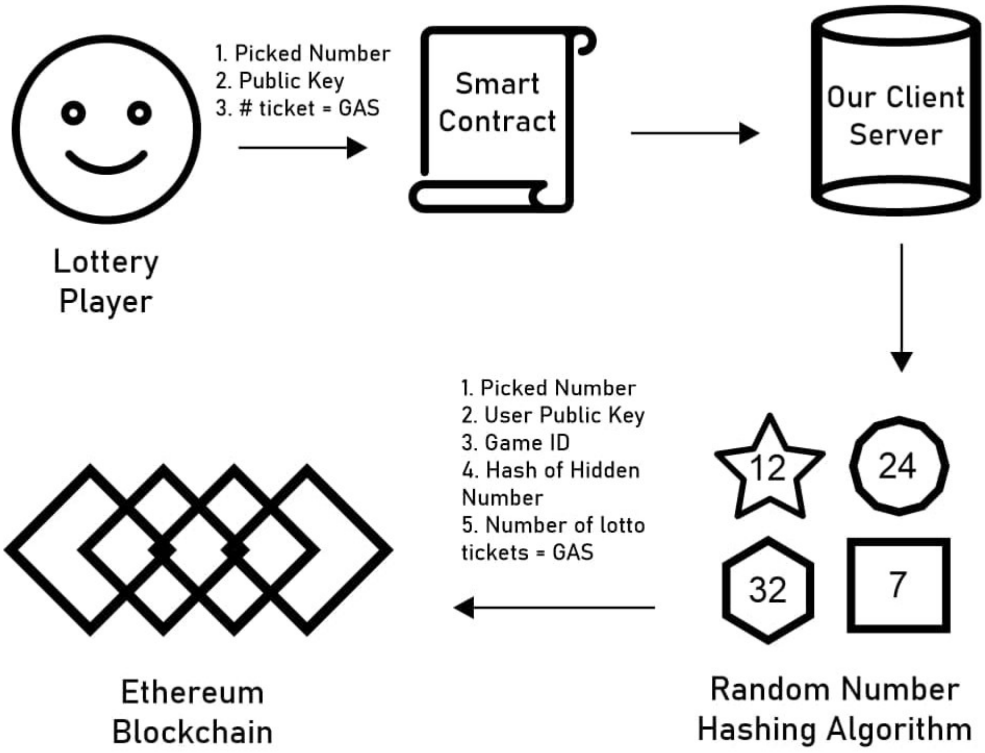
(ex. 1 GAS = 1 entry)

Once a 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:

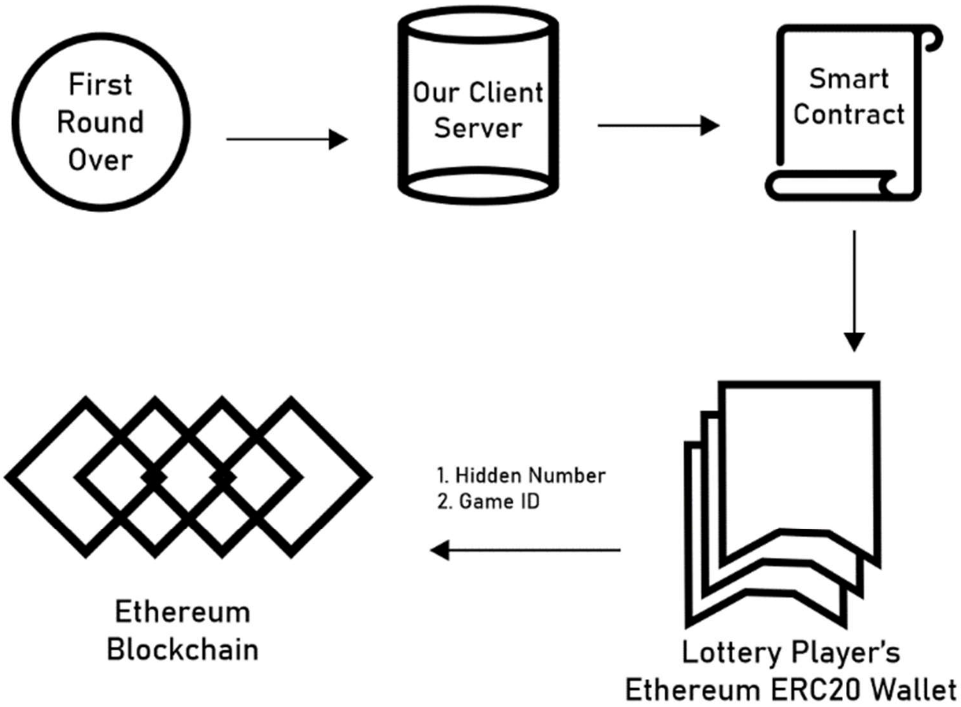
1. Game ID
2. Player’s public key (PK)
3. Player’s picked number
4. Amount of GAS paid = tickets purchased.
5. Hash of Hidden Number

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



Second Round

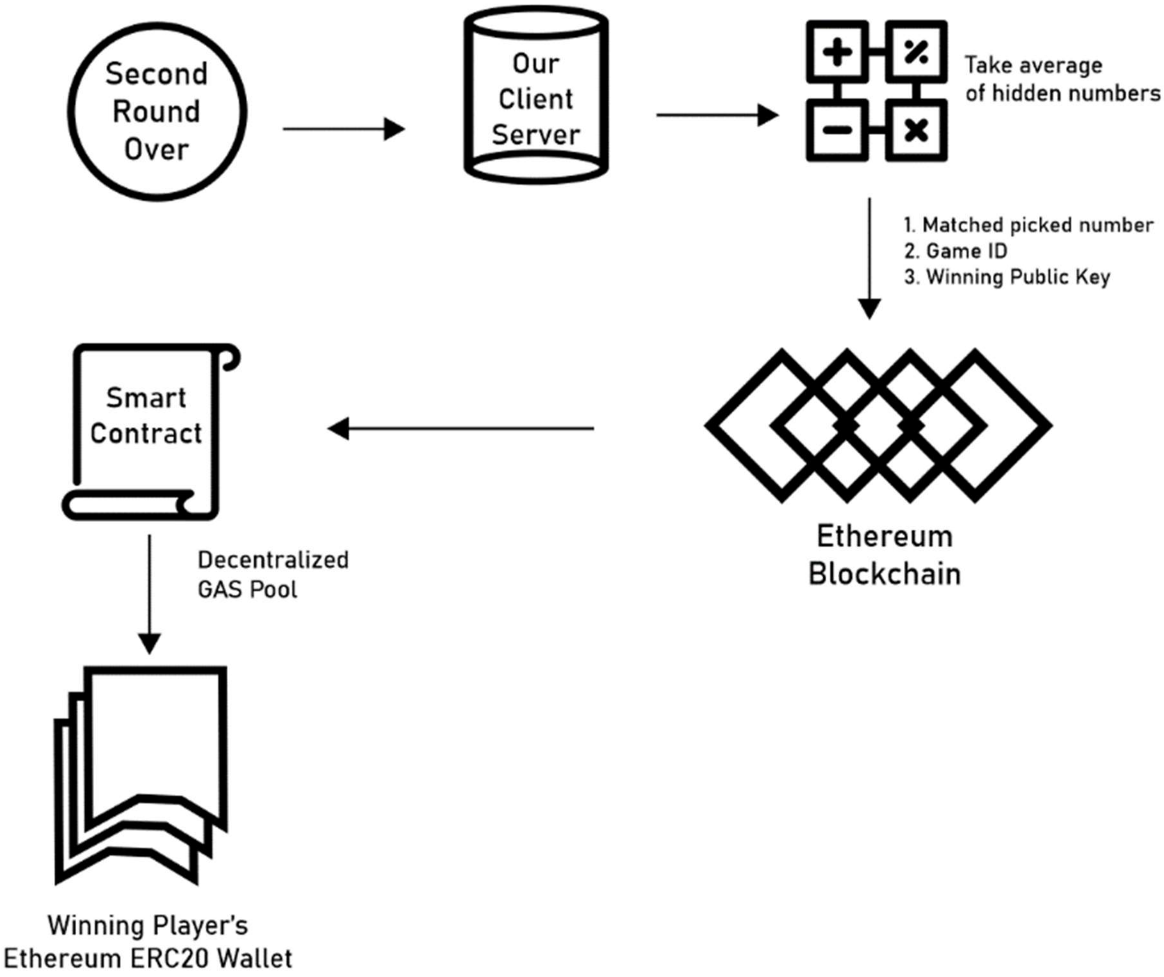
All hidden numbers are posted to the chain from the user's wallet with the
following data:
1. Game ID
2. Hidden number



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, 70% out of the 50% of the total proceeds of the lottery are sent to their public key submitted with their original entry.

Check(gameID, playerAddress, Matching Picked Number)



The second winner (whose hashed number is closest to the winner's number) gets the balance 30% out of the 50% of the total proceeds. Balance 50% of the total proceeds shall be invested in YLD DeFi and Balancer liquidity pools for liquidity mining and yield farming. And it will remain invested for 6 months or until it produces 200% cumulative returns on total capital invested. In the present DeFi scenario where everyone growing craxy and DeFi protocol tokens like Yearn and Uniswap gaining 10,000 returns 3 to 4 months' timeframes, it won't take more than 2 to 4 months to generate this nominal returns. Once this goal is achieved, consolation prizes will be awarded automatically by our Randpool smart contract to all ticket holders (except the winner and second winner) to their respective ERC20-comptaible wallets e.g. Metamask wallets.

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. And moreover all lottery players turn out to be winners in this decentralized lottery games, there are no losers.