**ReadMe RNG Lottery Ethereum**

**Participants**

1. Every buyer submits a commitment hash when they buy a ticket.
2. User’s is generating their number which they want to submit.
3. User’s secret number and address will be added to ticket list.

**Lottery System**

1. Ticketing period is over. Tickets cannot be purchased after this period.
2. User’s must reveal their own secret number. All reveals must occur after the ticket deadline and before the reveal deadline.
3. Verifying of commitment hash and must match the commitment submitted with the ticket.
4. If failed to submit their own number and address, dropped from the lottery.

**Draw winner** and **Withdraw** are nearly identical to SimpleLottery.

1. Draw winner

Generate random number, it will enable to select the user’s address to ticketlist.

Generate random seed for picking a winner, this is random seed to determine the winner. Each time a secret number is revealed, the seed is modified to incorporate the reveal.

1. Withdraw

Balance will be added to user’s address and will added to world state to verify the address of the user.