

# 【project 阶段三】合约部署报告

15331197 林杰群

## 1. 项目简介

利用智能合约完成彩票的投注、开奖和发奖。

## 2. 智能合约内容

### (1) 定义玩家下注的功能

```
function enter() public payable {
    require(msg.value > .0001 ether); // 要求投注金额大于 0.001 ether

    players.push(msg.sender);
}
```

宣告下注函数 enter() 为公开，因为需要支付以太币，函数设为 payable。将这次交易的发起人加入 players 阵列，以便知道有多少名玩家。

### (2) 随机挑选赢家

```
function random() private view returns(uint) {
    return uint(keccak256(block.difficulty, now, players));
}

modifier ownerOnly() {
    require(msg.sender == owner); // pickWinner 只能由 owner 发起
    _;
}

function pickWinner() public ownerOnly {
    uint index = random() % players.length;
    players[index].transfer(this.balance);

    players = new address[](0);
}
```

利用 keccak256 这个特殊的 SHA 函数求值，带入 block.difficulty、目前时间和玩家阵列得到一个 hash 值，再转化为整数，以此随机挑选赢家。然后用 transfer 将奖金转给赢家。

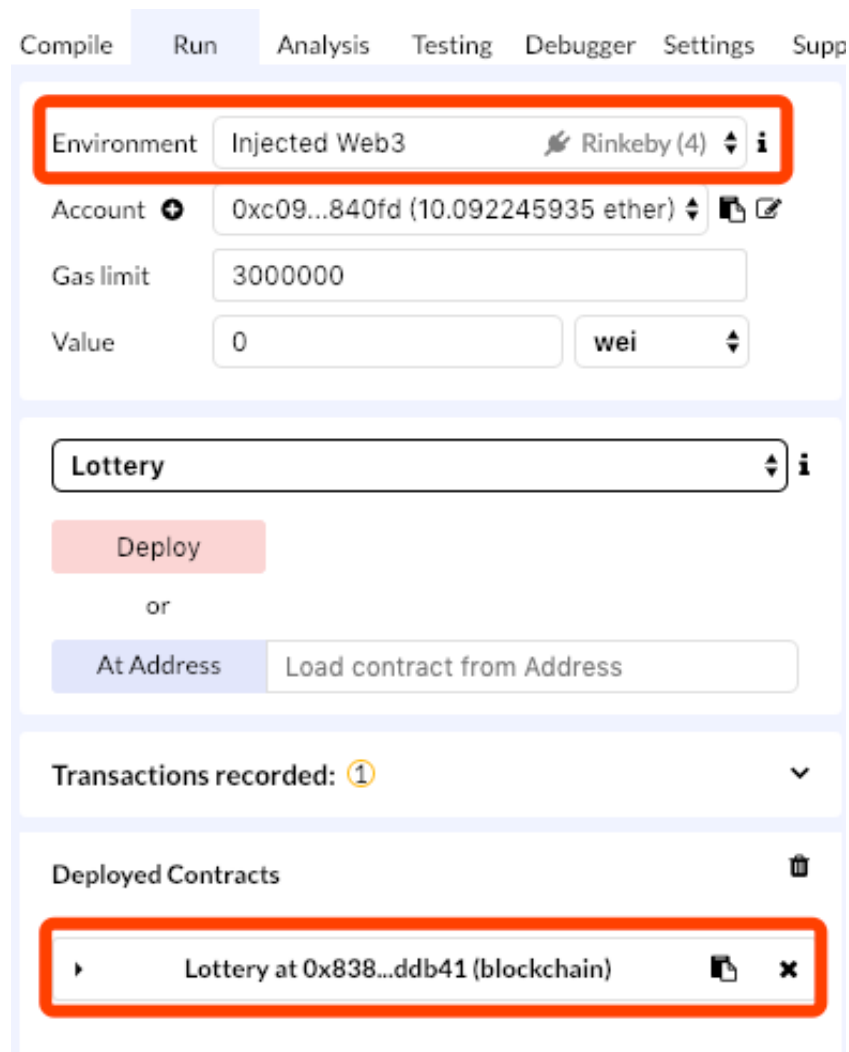
modifier ownerOnly 的作用是规定只能由 owner 调用挑选赢家的函数。

详细代码见 contracts/Lottery.sol。

## 3. 合约部署

这里利用 RemixIDE 和 Rinkeby 来部署和测试合约。

在 RemixIDE 上部署合约 Lottery.sol，得到合约的地址：



由于要用到 Rinkeby 测试，所以 Environment 要选择 Injected Web3。本次部署得到的合约地址为：0x838b71d0f0dfb26c4fbce84d0f4ad0e0025ddb41。由此可以得到在 Rinkeby 测试网络上的链接：

Transaction 0x990afd9f466e75e10068afd19df1126a2a0d69e30a0fdb0c05950386757f3f315

Home / Transactions / Tx Info

## Overview

## Transaction Information

Tools &amp; Utilities

[ This is a Rinkeby Testnet Transaction Only ]

TxHash: 0x990afd9f466e75e10068afd19df1126a2a0d69e30a0fdb0c05950386757f3f315

TxReceipt Status: Success

Block Height: 3647909 (1709 Block Confirmations)

TimeStamp: 7 hrs 7 mins ago (Jan-07-2019 07:52:17 AM +UTC)

From: 0xc092cb451eeb25cbd881505fd72547ec6b7840fd

To: [Contract 0x838b71d0f0dfb26c4fbc84d0f4ad0e0025ddb41 Created]

Value: 0 Ether (\$0.00)

Gas Limit: 505503

Gas Used By Transaction: 505503 (100%)

Gas Price: 0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee: 0.000505503 Ether (\$0.000000)

Nonce &amp; (Position): 17 | (5)

Input Data:

```
0x6060604052341561000f57600080fd5b3360008060101000a81548173fffffffffffffffffffffffffffffffffffffffff021916908373ff
ffffffffffffffffffffffffffffffffffffffff16021790555061064c8061005e6000396000f30060606040526000357c0100000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
5b146100e8578063e97dcb621461013d578063f71d96cb1461014757600080fd5b341561007457600080fd5b61007c610aa565b005b3415
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

View Input As

可以看到合约的发起人是我的账户 0xc092cb451eEb25cBd881505FD72547ec6b7840fd，合约部署成功。通过查询也可以得到合约的交易情况：

## Transactions

## Internal Txns

## Code

## Events

Latest 8 txns

TxHash	Block	Age	From	To	Value	[TxFee]
0x99a1c074928666...	3648096	6 hrs 26 mins ago	0xc092cb451eeb25...	IN 0x838b71d0f0dfb26...	0 Ether	0.000023758
0x4ce32a405481eb...	3648093	6 hrs 27 mins ago	0xc092cb451eeb25...	IN 0x838b71d0f0dfb26...	1 Ether	0.000047432
0x145d8f89bfe9d39...	3648093	6 hrs 27 mins ago	0x47cac6a7e2ad3b...	IN 0x838b71d0f0dfb26...	1 Ether	0.000062432
0x188de785cec3cd...	3648035	6 hrs 41 mins ago	0xc092cb451eeb25...	IN 0x838b71d0f0dfb26...	0 Ether	0.000026553
0xe3426a41a51990...	3648000	6 hrs 50 mins ago	0x1e8b4a8661930a...	IN 0x838b71d0f0dfb26...	2 Ether	0.000047432
0xaffce1736ec2c98...	3647996	6 hrs 51 mins ago	0x47cac6a7e2ad3b...	IN 0x838b71d0f0dfb26...	3 Ether	0.000047432
0xb219664a2b326d...	3647964	6 hrs 59 mins ago	0xc092cb451eeb25...	IN 0x838b71d0f0dfb26...	2 Ether	0.000062432
0x990afd9f466e75e...	3647909	7 hrs 13 mins ago	0xc092cb451eeb25...	IN Contract Creation	0 Ether	0.000505503

[ Download CSV Export ]