

โปรแกรมนี้

1. รับค่าตัวแปร T1, T2, T3, N จาก constructor
2. มี 5 functions ทำงานได้แค่เฉพาะ stage ของตัวเอง (ยกเว้น _reset) stage ขึ้นกับเวลา T1, T2, T3
 1. _reset - private ใช้ในการเริ่มต้นเกมใหม่หลังเกมจบหรือมีการถอนเงินเกิดขึ้น
 2. addUser - เพิ่มผู้เล่น โดยต้องมีการจ่ายเงิน 1 finney พร้อมทั้งใส่ choice และ salt ในการเก็บ hash ของ choice ที่ผู้เล่นเลือก
 3. revealChoice - เฉลยคำตอบที่ตนเองเลือก ต้องส่งมาทั้ง choice และ salt
 4. checkWinner - เลือกได้แค่ owner ของ contract นี้เท่านั้น ระบบจะจ่ายเงินคืนผู้เล่นที่ชนะ หากผู้เล่นมีชนะ ทำผิดกฎเงินทั้งหมดจะตกมาให้ owner ในกรณีปกติจะโอนเงินให้ผู้เล่น 98% ของเงินทั้งหมดและอีก 2% ให้ owner
 5. withdraw - ถอนเงินออกหาก owner ในกรณีที่เลยเวลาตรวจสอบผู้ชนะแล้ว

address ที่ deploy เกมลงไป (มีปัญหากับระบบ withdraw)

✓

[block:5556686 txIndex:106] from: 0xb3c...2821d to: lottery.(constructor) value: 0 wei data: 0x608...00002 logs: 0 hash: 0x2d4...5c60c

Debug

^

status	0x1 Transaction mined and execution succeed
transaction hash	0xa459aced8c7cbd2302ae3a4ae7a0fece2b48e30bbb3f7dc4ab9140eebd1a3ecc 🔗
block hash	0x2d4d080c5e6be3a11bb9ff32f8a01774429ca6a77e5fff10e11003a2c095c60c 🔗
block number	5556686 🔗
contract address	0x8e60d6d76517626cc4520e4f07003fce5ed3d845 🔗
from	0xb3c2c183e51ca4025f3d3e814209779ba6e2821d 🔗
to	lottery.(constructor) 🔗
gas	939484 gas 🔗
transaction cost	930928 gas 🔗
input	0x608...00002 🔗
decoded input	<pre>{ "uint256 t1": "60", "uint256 t2": "60", "uint256 t3": "60", "uint256 n": "2" }</pre> 🔗
decoded output	- 🔗
logs	[] 🔗 🔗

address ที่ deploy เกมลงไป (แก้ไข)

✓

[block:5557238 txIndex:44] from: 0xb3c...2821d to: lottery.(constructor)
value: 0 wei data: 0x608...00002 logs: 0 hash: 0x262...8fa5b

Debug

⌵

status 0x1 Transaction mined and execution succeed

transaction hash 0xb4196e75c6d4fd3b1e9efcd92314f1cb9fa8e66be66c422c83db75bd18c2c6b1 [🔗](#)

block hash 0x262bf65b8cd5fab57bb6b8e175ea42244e424dc677264a48dc2cfcfb31a8fa5b [🔗](#)

block number 5557238 [🔗](#)

contract address 0x47397312cbb0ced57034d86f4a22479638595a3e [🔗](#)

from 0xb3c2c183e51ca4025f3d3e814209779ba6e2821d [🔗](#)

to lottery.(constructor) [🔗](#)

gas 938843 gas [🔗](#)

transaction cost 930292 gas [🔗](#)

input 0x608...00002 [🔗](#)

decoded input [🔗](#)

```
{
  "uint256 t1": "60",
  "uint256 t2": "60",
  "uint256 t3": "60",
  "uint256 n": "2"
}
```

decoded output - [🔗](#)

logs [] [🔗](#) [🔗](#)

ตัวอย่าง

1. เล่นแบบปกติ

- ผู้เล่นเลือก choice และ salt

✓

[block:5556690 txIndex:35] from: 0xb3c...2821d to: lottery.addUser(uint256,uint256) 0x8e6...3d845
value: 1000000000000000 wei data: 0xe00...00001 logs: 0 hash: 0xf2c...14a7f

Debug

⌵

status 0x1 Transaction mined and execution succeed

transaction hash 0xd320aa6ff2d158835b884849b276a906a50704c4fbc4cd470b1a61b9965db0c8 [🔗](#)

block hash 0xf2c11408f0c39cf8e3cbd4a3d823962cd781ead1cb96102adeca7f5ee014a7f [🔗](#)

block number 5556690 [🔗](#)

from 0xb3c2c183e51ca4025f3d3e814209779ba6e2821d [🔗](#)

to lottery.addUser(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 [🔗](#)

gas 161177 gas [🔗](#)

transaction cost 159959 gas [🔗](#)

input 0xe00...00001 [🔗](#)

decoded input [🔗](#)

```
{
  "uint256 choice": "1",
  "uint256 salt": "1"
}
```

decoded output - [🔗](#)

logs [] [🔗](#) [🔗](#)

value 1000000000000000 wei [🔗](#)

✓ [block:5556691 txIndex:79] from: 0xc5c...2599d to: lottery.addUser(uint256,uint256) 0x8e6...3d845 value: 1000000000000000 wei data: 0xe00...00001 logs: 0 hash: 0x29a...0816e Debug

status 0x1 Transaction mined and execution succeed

transaction hash 0xac4eadf9f269c38aa854da48eaddcf8323b59716052f0a6cb8ead2776989c8ea [🔗](#)

block hash 0x29aebd4a4150549b92b53e9148c594cc3dc5d31e1bd2cbe34a8b70bd4400816e [🔗](#)

block number 5556691 [🔗](#)

from 0xc5c903aab965a6b55b17f45e7fc667fd2d12599d [🔗](#)

to lottery.addUser(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 [🔗](#)

gas 128955 gas [🔗](#)

transaction cost 127865 gas [🔗](#)

input 0xe00...00001 [🔗](#)

decoded input {
 "uint256 choice": "2",
 "uint256 salt": "1"
}

decoded output - [🔗](#)

logs [] [🔗](#) [🔗](#)

value 1000000000000000 wei [🔗](#)

○ ผู้เล่น reveal choice ของตน

✓ [block:5556696 txIndex:47] from: 0xb3c...2821d to: lottery.revealChoice(uint256,uint256) 0x8e6...3d845 value: 0 wei data: 0x41a...00001 logs: 0 hash: 0x586...9899a Debug

status 0x1 Transaction mined and execution succeed

transaction hash 0x4fa96135fb3ed9eb84a2130365f2bd5cf9e69bf9f0ff17e7eaf4c607818cf2bc [🔗](#)

block hash 0x586456a24e93d5949766aa64c6cd2f7367197e19a05f28abf26a67d8a429899a [🔗](#)

block number 5556696 [🔗](#)

from 0xb3c2c183e51ca4025f3d3e814209779ba6e2821d [🔗](#)

to lottery.revealChoice(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 [🔗](#)

gas 87276 gas [🔗](#)

transaction cost 86350 gas [🔗](#)

input 0x41a...00001 [🔗](#)

decoded input {
 "uint256 choice": "1",
 "uint256 salt": "1"
}

decoded output - [🔗](#)

logs [] [🔗](#) [🔗](#)

✓ [block:5556697 txIndex:54] from: 0xc5c...2599d to: lottery.revealChoice(uint256,uint256) 0x8e6...3d845 value: 0 wei data: 0x41a...00001 logs: 0 hash: 0xccd...844ec Debug

status 0x1 Transaction mined and execution succeed

transaction hash 0x751fd963a02ea74b2d6f408ca23f34995a581df7467d2aa186eba6f48e3d5a13 [🔗](#)

block hash 0xccd18a46dd1023a88b0e44f3d96d6bfaf329e27cf8fceed25babf952940844ec [🔗](#)

block number 5556697 [🔗](#)

from 0xc5c903aab965a6b55b17f45e7fc667fd2d12599d [🔗](#)

to lottery.revealChoice(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 [🔗](#)

gas 72919 gas [🔗](#)

transaction cost 72050 gas [🔗](#)

input 0x41a...00001 [🔗](#)

decoded input {
 "uint256 choice": "2",
 "uint256 salt": "1"
}

decoded output - [🔗](#)

logs [] [🔗](#) [🔗](#)

◦ Owner ทำการหาผู้ชนะ

✓

[block:5556699 txIndex:111] from: 0xb3c...2821d to: lottery.checkWinner() 0x8e6...3d845 value: 0 wei data: 0xad3...8867e logs: 0 hash: 0xf2d...8bf94

Debug

^

status

0x1 Transaction mined and execution succeed

transaction hash

0x330c2b479f349e5ef437e6ef769a1c8c4d4251d8b2e94a44b84b6baa2d775430

block hash

0xf2d72332dbdc80cba22c1e3312b1543751f512e4cf77912d7aa8977cd48bf94

block number

5556699

from

0xb3c2c183e51ca4025f3d3e814209779ba6e2821d

to

lottery.checkWinner() 0x8e60d6d76517626cc4520e4f07003fce5ed3d845

gas

300000 gas

transaction cost

113306 gas

input

0xad3...8867e

decoded input

{}

decoded output

-

logs

[]

◦ โอนเงินให้ผู้ชนะ

[This is a Sepolia **Testnet** transaction only]

Transaction Hash:

0x330c2b479f349e5ef437e6ef769a1c8c4d4251d8b2e94a44b84b6baa2d775430

Status:

Success

Block:

5556699

11 Block Confirmations

Timestamp:

2 mins ago (Mar-25-2024 08:20:12 AM +UTC)

Transaction Action:

Call

Check Winner

Function by 0xb3c2c183...ba6E2821D on 0x8e60D6D7...e5ed3D845

From:

0xb3c2c183E51cA4025F3D3E814209779ba6E2821D

To:

0x8e60D6D76517626cc4520e4F07003Fce5ed3D845

✓

Transfer 0.00196 ETH From 0x8e60D6D7...e5ed3D845 To 0xC5C903aA...D2D1259...

Transfer 0.00004 ETH From 0x8e60D6D7...e5ed3D845 To 0xb3c2c183...ba6E2821D

2. ผู้ชนะเล่นผิตกฏ

◦ ผู้เล่นเลือก choice และ salt

✓

[block:5556767 txIndex:121] from: 0xb3c...2821d to: lottery.addUser(uint256,uint256) 0x8e6...3d845 value: 1000000000000000 wei data: 0xe00...00001 logs: 0 hash: 0xa14...cf210

Debug

^

status

0x1 Transaction mined and execution succeed

transaction hash

0x881cdcb4aueb1157b2c70c59765d6e9a4047bde3def4d14d259f8f4d3bc3513d

block hash

0xa14351dcfe599b7677223efaf02eac8ba99d25037b53767ca40faf2a9b1cf210

block number

5556767

from

0xb3c2c183e51ca4025f3d3e814209779ba6e2821d

to

lottery.addUser(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845

gas

143935 gas

transaction cost

138059 gas

input

0xe00...00001

decoded input

{
 "uint256 choice": "1",
 "uint256 salt": "1"
}

decoded output

-

logs

[]

✓ [block:5556773 txIndex:70] from: 0xc5c...2599d to: lottery.revealChoice(uint256,uint256) 0x8e6...3d845 value: 0 wei data: 0x41a...00001 logs: 0 hash: 0xcd6...7a968 Debug ^

status	0x1 Transaction mined and execution succeed
transaction hash	0x7e7ee74f60e7186b74047b649c110ec6afab9a00f1937a8492b46243231c4d04 🔗
block hash	0xcd622598eacaab4f26f4fe5e2dcc9771a5f91b4faa97b269a3f925c0d057a968 🔗
block number	5556773 🔗
from	0xc5c903aab965a6b55b17f45e7fc667fd2d12599d 🔗
to	lottery.revealChoice(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 🔗
gas	3000000 gas 🔗
transaction cost	106262 gas 🔗
input	0x41a...00001 🔗
decoded input	{ "uint256 choice": "10000", "uint256 salt": "1" }
decoded output	- 🔗
logs	[] 🔗 🔗

○ ผู้เล่น reveal choice ของตน

✓ [block:5556773 txIndex:70] from: 0xc5c...2599d to: lottery.revealChoice(uint256,uint256) 0x8e6...3d845 value: 0 wei data: 0x41a...00001 logs: 0 hash: 0xcd6...7a968 Debug ^

status	0x1 Transaction mined and execution succeed
transaction hash	0x7e7ee74f60e7186b74047b649c110ec6afab9a00f1937a8492b46243231c4d04 🔗
block hash	0xcd622598eacaab4f26f4fe5e2dcc9771a5f91b4faa97b269a3f925c0d057a968 🔗
block number	5556773 🔗
from	0xc5c903aab965a6b55b17f45e7fc667fd2d12599d 🔗
to	lottery.revealChoice(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 🔗
gas	3000000 gas 🔗
transaction cost	106262 gas 🔗
input	0x41a...00001 🔗
decoded input	{ "uint256 choice": "10000", "uint256 salt": "1" }
decoded output	- 🔗
logs	[] 🔗 🔗

○ Owner ทำการหาผู้ชนะ

✓ [block:5556778 txIndex:46] from: 0xb3c...2821d to: lottery.checkWinner() 0x8e6...3d845 value: 0 wei data: 0xad3...8867e logs: 0 hash: 0xdc8...5951f Debug ^

status	0x1 Transaction mined and execution succeed
transaction hash	0xb58446d235fc24a32698191532ec34c9500606c7b0c621509c2b78667ce743f8 🔗
block hash	0xdc8e8781b581923d23f81b5e60b4782f0f639a80c562ae08c64e7fa2e475951f 🔗
block number	5556778 🔗
from	0xb3c2c183e51ca4025f3d3e814209779ba6e2821d 🔗
to	lottery.checkWinner() 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 🔗
gas	3000000 gas 🔗
transaction cost	106772 gas 🔗
input	0xad3...8867e 🔗
decoded input	{}
decoded output	- 🔗
logs	[] 🔗 🔗

○ โอนเงินให้ owner

[This is a Sepolia **Testnet** transaction only]

Transaction Hash:

0xb58446d235fc24a32698191532ec34c9500606c7b0c621509c2b78667ce743f8

Status:

Success

Block:

55567781 Block Confirmation

Timestamp:

8 secs ago (Mar-25-2024 08:36:48 AM +UTC)

Transaction Action:

Call Check Winner Function by 0xb3c2c183...ba6E2821D on 0x8e60D6D7...e5ed3D845

From:

0xb3c2c183E51cA4025F3D3E814209779ba6E2821D

To:

0x8e60D6D76517626cc4520e4F07003Fce5ed3D845

Transfer 0.00196 ETH From 0x8e60D6D7...e5ed3D845 To 0xb3c2c183...ba6E2821D

Transfer 0.00004 ETH From 0x8e60D6D7...e5ed3D845 To 0xb3c2c183...ba6E2821D

3. owner ไม่ทำการตรวจสอบผู้ชนะ (user ขอ withdraw)

○ ผู้เล่นเลือก choice และ salt

✓

[block:5557231 txIndex:29] from: 0xb3c...2821d
to: lottery.addUser(uint256,uint256) 0x068...41a91 value: 100000000000000 wei
data: 0xe00...00001 logs: 0 hash: 0xd47...48946

Debug

status

0x1 Transaction mined and execution succeed

transaction hash

0xe1a386a2e058273d3ad7e1ecb9aa89eafe41d7dd6830f4ba32d69da48341d6b2

block hash

0xd47e696aa21ec6b7b8c7bccbd1720de31ee25dfd74b64901362bf19583148946

block number

5557231

from

0xb3c2c183e51ca4025f3d3e814209779ba6e2821d

to

lottery.addUser(uint256,uint256) 0x068f0dc216233a188320b6e3a996850be9f41a91

gas

161177 gas

transaction cost

159959 gas

input

0xe00...00001

decoded input

{
 "uint256 choice": "1",
 "uint256 salt": "1"
}

decoded output

-

logs

[]

value

1000000000000000 wei

6 / 9

[block:5557231 txIndex:29] from: 0xb3c...2821d
 to: lottery.addUser(uint256,uint256) 0x068...41a91 value: 1000000000000000 wei
 data: 0xe00...00001 logs: 0 hash: 0xd47...48946

Debug

^

status	0x1 Transaction mined and execution succeed
transaction hash	0xe1a386a2e058273d3ad7e1ecb9aa89eafe41d7dd6830f4ba32d69da48341d6b2 🔗
block hash	0xd47e696aa21ec6b7b8c7bccbd1720de31ee25dfd74b64901362bf19583148946 🔗
block number	5557231 🔗
from	0xb3c2c183e51ca4025f3d3e814209779ba6e2821d 🔗
to	lottery.addUser(uint256,uint256) 0x068f0dc216233a188320b6e3a996850be9f41a91 🔗
gas	161177 gas 🔗
transaction cost	159959 gas 🔗
input	0xe00...00001 🔗
decoded input	<pre>{ "uint256 choice": "1", "uint256 salt": "1" }</pre> 🔗
decoded output	- 🔗
logs	[] 🔗 🔗
value	1000000000000000 wei 🔗

○ ผู้เล่น reveal choice ของตน

[block:5557246 txIndex:70] from: 0xb3c...2821d
 to: lottery.revealChoice(uint256,uint256) 0x473...95a3e value: 0 wei
 data: 0x41a...00001 logs: 0 hash: 0x1da...70820

Debug

^

status	0x1 Transaction mined and execution succeed
transaction hash	0xc8076f5d883fcc1e5599708690b7a5b6ae75676ac4d79d2f098e2ff16c94a48d 🔗
block hash	0x1daaaa9b202deab703946b740c72a0a759f81326ed8c1e8c27bef7f4ab570820 🔗
block number	5557246 🔗
from	0xb3c2c183e51ca4025f3d3e814209779ba6e2821d 🔗
to	lottery.revealChoice(uint256,uint256) 0x47397312cbb0ced57034d86f4a22479638595a3e 🔗
gas	3000000 gas 🔗
transaction cost	86350 gas 🔗
input	0x41a...00001 🔗
decoded input	<pre>{ "uint256 choice": "1", "uint256 salt": "1" }</pre> 🔗
decoded output	- 🔗
logs	[] 🔗 🔗

✓

[block:5557248 txIndex:31] from: 0xc5c...2599d
to: lottery.revealChoice(uint256,uint256) 0x473...95a3e **value:** 0 wei
data: 0x41a...00001 **logs:** 0 **hash:** 0xeec...a401c

Debug

^

status	0x1 Transaction mined and execution succeed
transaction hash	0x76aab863dea9a5c6278ff1dc343e354e1e61879c3634ab1c83353016b6b3bcfd 🔗
block hash	0xeeca18f3046c9c3ce65758120516b82616657d0a51aaf0b6c44d2ce6258a401c 🔗
block number	5557248 🔗
from	0xc5c903aab965a6b55b17f45e7fc667fd2d12599d 🔗
to	lottery.revealChoice(uint256,uint256) 0x47397312cbb0ced57034d86f4a22479638595a3e 🔗
gas	72919 gas 🔗
transaction cost	72050 gas 🔗
input	0x41a...00001 🔗
decoded input	<pre>{ "uint256 choice": "1", "uint256 salt": "1" }</pre> 🔗
decoded output	- 🔗
logs	[] 🔗 🔗

○ ผู้เล่นเกมของเงินคืน

✓

[block:5557268 txIndex:65] from: 0xc5c...2599d **to:** lottery.withdraw() 0x473...95a3e
value: 0 wei **data:** 0x3cc...fd60b **logs:** 0 **hash:** 0x645...15adf

Debug

^

status	0x1 Transaction mined and execution succeed
transaction hash	0x7442c6acdda50419a9dda205249e4cbc7718b03df19c407eb3b685ba5e2b7db2 🔗
block hash	0x64565dd104442d8bacbb6fecc999d0942e550e60b5fa09dd18e3b5f461015adf 🔗
block number	5557268 🔗
from	0xc5c903aab965a6b55b17f45e7fc667fd2d12599d 🔗
to	lottery.withdraw() 0x47397312cbb0ced57034d86f4a22479638595a3e 🔗
gas	138779 gas 🔗
transaction cost	110618 gas 🔗
input	0x3cc...fd60b 🔗
decoded input	{ } 🔗
decoded output	- 🔗
logs	[] 🔗 🔗

○ โอนเงินให้ผู้เล่นทั้งหมด

[This is a Sepolia **Testnet** transaction only]

Transaction Hash:

0x7442c6acdda50419a9dda205249e4cbc7718b03df19c407eb3b685ba5e2b7db2

Status:

Success

Block:

55572681 Block Confirmation

Timestamp:

15 secs ago (Mar-25-2024 10:19:36 AM +UTC)

Transaction Action:

Call Withdraw Function by 0xC5C903aA...D2D12599D on 0x47397312...638595A3E

From:

0xC5C903aAB965a6b55b17F45E7fC667FD2D12599D

To:

0x47397312cBB0Ced57034D86F4a22479638595A3E

Transfer 0.001 ETH From 0x47397312...638595A3E To 0xb3c2c183...ba6E2821D

Transfer 0.001 ETH From 0x47397312...638595A3E To 0xC5C903aA...D2D1259...