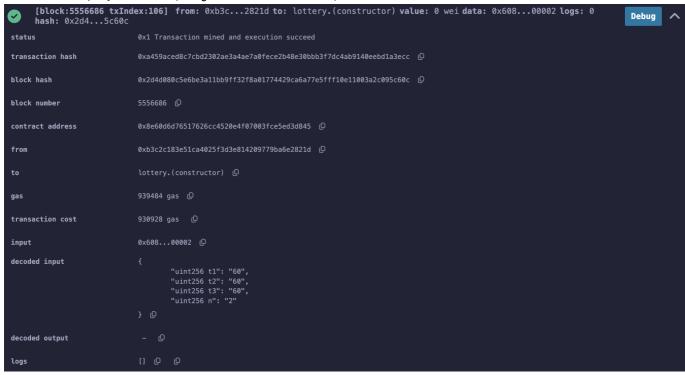
โปรแกรมนี้

- 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 หากผู้เล่นมี่ชนะ ทำผิดกฏเงินทั้งหมดจะตกมาให้ owner ในกรณีปกติจะโอนเงินให้ผู้เล่น 98% ของเงินทั้งหมดและอีก 2% ให้ owner
 - 5. withdraw ถอนเงินออกหาก owner ในกรณีที่เลยเวลาตรวจสอบผู้ชนะแล้ว

address ที่ deploy เกมลงไป (มีปัญหากับระบบ withdraw)



address ที่ deploy เกมลงไป (แก้ไข)

```
[block:5557238 txIndex:44] from: 0xb3c...2821d to: lottery.(constructor)
                                                                                             Debug
     value: 0 wei data: 0x608...00002 logs: 0 hash: 0x262...8fa5b
status
                          0x1 Transaction mined and execution succeed
transaction hash
                          block hash
                          0x262bf65b8cd5fab57bb6b8e175ea42244e424dc677264a48dc2cfcfb31a8fa5b
block number
                          5557238 🚇
contract address
                          0x47397312cbb0ced57034d86f4a22479638595a3e (D
from
                          0xb3c2c183e51ca4025f3d3e814209779ba6e2821d (D
                          lottery.(constructor) 🚨
to
                          938843 gas 🗘
gas
transaction cost
                          930292 gas 🗘
                          0x608...00002 (
input
decoded input
                                 "uint256 t1": "60",
                                 "uint256 t2": "60",
                                 "uint256 t3": "60",
                          } @
decoded output
                                Ō
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
②
                                                                                                                                                       Debug
status
                                   0x1 Transaction mined and execution succeed
 transaction hash
block hash
                                   0xb3c2c183e51ca4025f3d3e814209779ba6e2821d (D
from
                                   161177 gas 🗘
qas
transaction cost
decoded input
                                           "uint256 choice": "1", "uint256 salt": "1"
 decoded output
 logs
```

```
[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
                                    0x1 Transaction mined and execution succeed
status
transaction hash
block hash
block number
                                    5556691 @
from
                                    lottery.addUser(uint256,uint256) 0x8e60d6d76517626cc4520e4f07003fce5ed3d845 @
transaction cost
                                    127865 gas ()
decoded input
                                             "uint256 choice": "2", "uint256 salt": "1"
decoded output
logs
```

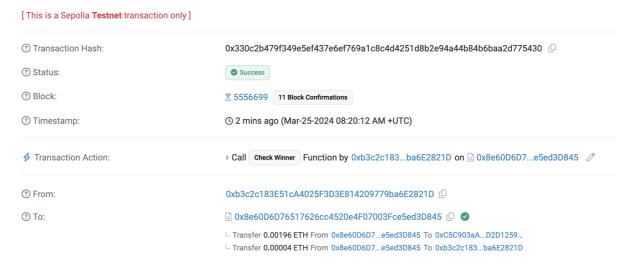
ผู้เล่น reveal choice ของตน

```
[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
0
                                                                                                                                Debug ^
status
                               0x1 Transaction mined and execution succeed
transaction hash
                               0x751fd963a02ea74b2d6f408ca23f34995a581df7467d2aa186eba6f48e3d5a13 (Q
block hash
                               block number
from
                               gas
                               72919 gas (D
                               72050 gas 🗘
input
                               0x41a...00001 @
decoded input
                                      "uint256 choice": "2",
"uint256 salt": "1"
decoded output
```

o Owner ทำการหาผู้ชนะ



โอนเงินให้ผู้ชนะ



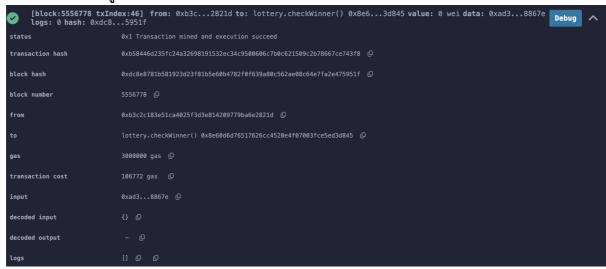
2. ผู้ชนะเล่นผิดกฎ

o ผู้เล่นเลือก choice และ salt

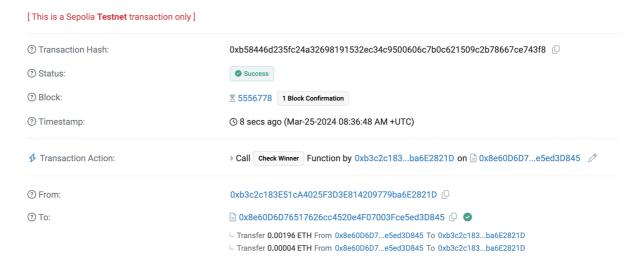


ผู้เล่น reveal choice ของตน

Owner ทำการหาผู้ชนะ



โอนเงินให้ owner



3. owner ไม่ทำการตรวจสอบผู้ชนะ (user ขอ withdraw)

o ผู้เล่นเลือก choice และ salt

```
[block:5557231 txIndex:29] from: 0xb3c...2821d
   to: lottery.addUser(uint256,uint256) 0x068...41a91 value: 10000000000000000 wei data: 0xe00...00001 logs: 0 hash: 0xd47...48946
                                                                 Debug
transaction hash
                     block hash
                     block number
from
                     gas
transaction cost
                     159959 gas 🗘
                     0xe00...00001 @
input
decoded input
                         "uint256 choice": "1",
decoded output
logs
                     1000000000000000 wei 🗜
value
```



ผู้เล่น reveal choice ของตน

```
[block:5557246 txIndex:70] from: 0xb3c...2821d
to: lottery.revealChoice(uint256,uint256) 0x473...95a3e value: 0 wei
                                                                                                       Debug
     data: 0x41a...00001 logs: 0 hash: 0x1da...70820
transaction hash
                                 0xc8076f5d883fcc1e5599708690b7a5b6ae75676ac4d79d2f098e2ff16c94a48d Q
                                 0x1daaaa9b202deab703946b740c72a0a759f81326ed8c1e8c27bef7f4ab570820 Q
block hash
block number
                                 5557246 t₽
                                 from
                                 lottery.revealChoice(uint256,uint256) 0x47397312cbb0ced57034d86f4a22479638595a3e
to
                                 3000000 gas @
gas
transaction cost
                                 86350 gas 🗘
input
                                 0x41a...00001 ©
decoded input
                                         "uint256 choice": "1",
                                         "uint256 salt": "1"
decoded output
logs
```



ผู้เล่นกดของเงินคืน



โอนเงินให้ผู้เล่นทั้งหมด

