

สิ่งที่แก้ไขจากของเก่า

struct Player มีการเพิ่ม

1. timestamp - ใช้อ้างอิงตอนเรียกขอเงินคืนโดยถ้ารอมานานเกินกว่า timeLimit

สร้าง map (address => uint) เพื่อให้ user ไม่ต้องนั่งหา id ของตัวเอง

function

1. _reset

- เพื่อทำการรีเซ็ตค่าต่างๆเมื่อเกมจบรอบหรือมีคนถอนเงินออก โดยมีการกำหนดว่าค่า default ไว้ว่า

- player id = 0 - หมายความว่า address นี้ยังไม่ได้ลงทะเบียนในรอบนั้นๆ
- player choice = 7 - หมายความว่า player ยั่วไม่ได้เลือกคำตอบ

2. viewPlayer

- เพื่อดูค่าต่างๆของ player address นั้นๆ
- ดูได้เฉพาะของคนที่เราเรียก

3. viewGameStatus

- ดูค่าต่างๆในเกม เช่น จำนวนผู้เล่น
- ใครเข้ามาดูก็ได้

4. addPlayer

- ดักกรณี player เพิ่มตัวเองสองครั้งและแก้ไข player id เริ่มที่ 1

5. input

- ปรับให้ใช้ในแบบไม่ต้องให้ player ใส่ idx เอง
- เวลา input ตอนแรกจะไม่ได้เก็บค่า choice แต่เป็น hash ของ choice และ

salt

- ต้องเป็นคนที่ลงทะเบียนไว้แล้วเท่านั้น

6. revealChoice

- เป็นการเฉลยคำตอบของตัวเองด้วยการใส่ choice และ salt ที่ใส่ใน input ไปตอนต้นโดยค่านี้อาจจะต้องเท่ากันถึงจะยอมรับคำตอบ

- สามารถเฉลยได้ครั้งเดียว
- ต้องเป็นคนที่ลงทะเบียนไว้แล้วเท่านั้น

7. withdraw

- เพื่อขอตึงเงินคืนตอนที่ไม่มีคนเข้ามาเล่นด้วยหรือเข้ามาแล้วแต่ไม่เล่น
 - ตอนที่ไม่มีคนเข้ามาเล่นด้วย: คืนให้คนขอคืนนั้น
 - เข้ามาแล้วแต่ไม่เล่น: คืนเงินเท่าๆกันให้ทั้งสองฝ่าย
 - เข้าเล่นทั้งคู่แต่มีคนเฉลยคำตอบตัวเองแค่คนเดียว: คืนเงินเท่าๆกันให้ทั้งสองฝ่าย
- ต้องเป็นคนที่ลงทะเบียนไว้แล้วเท่านั้น
- เวลาต้องผ่านไป 10 นาทีแล้วจากที่คนนั้นเข้าร่วมเล่น
- กดคนเดียว

8. _checkWinnerAndPay

- แก้ไขเงื่อนไขในการชนะ ปรับเพื่อให้รองรับการเล่น RWAPSSF

ตัวอย่างการเล่น มีผู้ชนะ

1. ผู้เล่นเข้าร่วมครบ 2 คน

0x787...cabaB (98.9999999999999844785 ether)
0x617...5E7f2 (98.9999999999999878985 ether)

▼

RWAPSSF AT 0X929...5447E (M

×

Balance: 2 ETH

addPlayer

input

uint256 choice, uint256

▼

revealChoice

uint256 choice, uint256

▼

withdraw

viewGameSt...

0: uint256: numberOfPlayer 2

1: uint256: gameReward 2000000000000000000000000

2: uint256: numberOfInput 0

3: uint256: numberOfReveal 0

4: uint256: canWithdrawAfter 600

viewPlayer

2. ผู้เล่นทั้ง 2 คนใส่ input ทั้งสองคน

▼

RWAPSSF AT 0X929...5447E (M

×

Balance: 2 ETH

addPlayer

input

^

choice:

1

salt:

10

Calldata

Parameters

transact

revealChoice

uint256 choice, uint256

▼

withdraw

viewGameSt...

0: uint256: numberOfPlayer 2


1: uint256: gameReward 2000000000000000000000000

2: uint256: numberOfInput 1

3: uint256: numberOfReveal 0
4: uint256: canWithdrawAfter 600

viewPlayer

0: uint256: choice 7
1: bytes32: commit 0xbbc70db1b6c7afd11e79c0fb0051300458f1a3acb8ee9789d9b6b26c61ad9bc7
2: bool: isRevealed false
3: uint256: timestamp 1707768076
4: uint256: playerNumber 1
5: address: addr 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB

✓ RWAPSSF AT 0X929...5447E (M)  



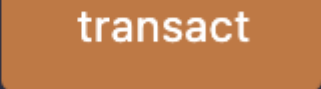
Balance: 2 ETH

addPlayer

input 

choice:

salt:

 Calldata  Parameters 

revealChoice

uint256 choice, uint256

**withdraw****viewGameSt...**

0: uint256: numberOfPlayer 2

1: uint256: gameReward 2000000000000
0000000

2: uint256: numberOfInput 2

3: uint256: numberOfReveal 0

4: uint256: canWithdrawAfter 600

viewPlayer

0: uint256: choice 7

1: bytes32: commit 0xa50eece07c7db163
1545c0069bd8f5f54d5935e215d5909
7edf258a44ba91634

2: bool: isRevealed false

3: uint256: timestamp 1707768083

4: uint256: playerNumber 2

5: address: addr 0x617F2E2fD72FD9D55
03197092aC168c91465E7f2

3. ผู้เล่นทั้ง 2 คน reveal คำตอบของตน

6 / 16

viewPlayer

- 0: uint256: choice 1
- 1: bytes32: commit 0xbbc70db1b6c7afd11e79c0fb0051300458f1a3acb8ee9789d9b6b26c61ad9bc7
- 2: bool: isRevealed true
- 3: uint256: timestamp 1707768076
- 4: uint256: playerNumber 1
- 5: address: addr 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB

▼ RWAPSSF AT 0X929...5447E (M)  

Balance: 0. ETH

addPlayer

input

uint256 choice, uint256 ▼

revealChoice ^

choice: 2

salt: 11



Calldata



Parameters

transact

withdraw**viewGameSt...**

- 0: uint256: numberOfPlayer 0
- 1: uint256: gameReward 0
- 2: uint256: numberOfInput 0
- 3: uint256: numberOfReveal 0
- 4: uint256: canWithdrawAfter 600

viewPlayer

- 0: uint256: choice 1
- 1: bytes32: commit 0xbbc70db1b6c7afd11e79c0fb0051300458f1a3acb8ee9789d9b6b26c61ad9bc7
- 2: bool: isRevealed true
- 3: uint256: timestamp 1707768076
- 4: uint256: playerNumber 1
- 5: address: addr 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB

(player คนหลังดู

ข้อมูลไม่ได้แล้ว)

```
CALL [call] from: 0x617F2E2fD72FD9D5503197092aC168c91465E7f2 to: RWAPSSF.viewPlayer() data: 0x44c...e4375
call to RWAPSSF.viewPlayer errored: Error occured: revert.

revert
The transaction has been reverted to the initial state.
Reason provided by the contract: "Registered player only".
Debug the transaction to get more information.
```

Debug ▼

4. ผู้เล่นที่ชนะจะได้เงินไป 2 ether

ตัวอย่างการเล่น เสมอ

9 / 16

```
2: uint256: numberOfInput 0
3: uint256: numberOfReveal 0
4: uint256: canWithdrawAfter 600
```

viewPlayer

```
0: uint256: choice 7
1: bytes32: commit 0x0000000000000000
  00000000000000000000000000000000
  0000000000000000000000000000
2: bool: isRevealed false
3: uint256: timestamp 1707768463
4: uint256: playerNumber 2
5: address: addr 0x617F2E2fD72FD9D55
  03197092aC168c91465E7f2
```

2. ผู้เล่นทั้ง 2 คนใส่ input ทั้งสองคน



RWAPSSF AT 0X929...5447E (N



Balance: 2 ETH

addPlayer

input



choice:

1

10

Calldata

Parameters

transact

uint256 choice, uint256

withdraw

viewGameSt...

```
1: uint256: gameReward 200000000000  
      0000000
```

3: uint256: numberOfReveal 0

4: uint256: canWithdrawAfter 600

viewPlayer

```
1: bytes32: commit 0xbbc70db1b6c7afd1
    1e79c0fb0051300458f1a3acb8ee9789
    d9b6b26c61ad9bc7
```

2: bool: isRevealed false

4: uint256: playerNumber 1

```
5: address: addr 0x78731D3Ca6b7E34aC
      0F824c42a7cC18A495cabaB
```

▼

RWAPSSF AT 0X929...5447E (M

×

Balance: 2 ETH

addPlayer

input

^

choice:

1

salt:

10

Calldata

Parameters

transact

revealChoice

uint256 choice, uint256

▼

withdraw

viewGameSt...

0: uint256: numberOfPlayer 2

1: uint256: gameReward 2000000000000000000000000

2: uint256: numberOfInput 2

3: uint256: numberOfReveal 0

4: uint256: canWithdrawAfter 600

viewPlayer

0: uint256: choice 7

1: bytes32: commit 0xbbc70db1b6c7afd11e79c0fb0051300458f1a3acb8ee9789d9b6b26c61ad9bc7

2: bool: isRevealed false

3: uint256: timestamp 1707768463

4: uint256: playerNumber 2

5: address: addr 0x617F2E2fD72FD9D5503197092aC168c91465E7f2

3. ผู้เล่นทั้ง 2 คน reveal คำตอบของตน

▼ RWAPSSF AT 0X929...5447E (M)

Balance: 2 ETH

addPlayer

input

uint256 choice, uint256

revealChoice

choice: 1

10

CalldataParameterstransact

withdraw

viewGameSt...

0: uint256: numberOfPlayer 2
1: uint256: gameReward 2000000000000000000000000
2: uint256: numberOfInput 2
3: uint256: numberOfReveal 1
4: uint256: canWithdrawAfter 600

viewPlayer

0: uint256: choice 1
1: bytes32: commit 0xbbc70db1b6c7afd11e79c0fb0051300458f1a3acb8ee9789d9b6b26c61ad9bc7
2: bool: isRevealed true
3: uint256: timestamp 1707768457
4: uint256: playerNumber 1
5: address: addr 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB

✓ RWAPSSF AT 0X929...5447E (M)

Balance: 0. ETH

addPlayer

input uint256 choice, uint256

revealChoice

choice:

1

salt:

10



Calldata



Parameters

transact

withdraw

viewGameSt...

0: uint256: numberOfPlayer 0

1: uint256: gameReward 0

2: uint256: numberOfInput 0

3: uint256: numberOfReveal 0

4: uint256: canWithdrawAfter 600

viewPlayer

0: uint256: choice 1

```
1: bytes32: commit 0xbbc70db1b6c7afd1
1e79c0fb0051300458f1a3acb8ee9789
d9b6b26c61ad9bc7

2: bool: isRevealed true

3: uint256: timestamp 1707768457

4: uint256: playerNumber 1

5: address: addr 0x78731D3Ca6b7E34aC
0F824c42a7cC18A495cabaB
```

(player คนหลังดู

ข้อมูลไม่ได้แล้ว)

```
CALL [call] from: 0x617F2E2fD72FD9D5503197092aC168c91465E7f2 to: RWAPSSF.viewPlayer() data: 0x44c...e4375
call to RWAPSSF.viewPlayer errored: Error occurred: revert.

revert
The transaction has been reverted to the initial state.
Reason provided by the contract: "Registered player only".
Debug the transaction to get more information.
```

Debug

4. ผู้เล่นได้เงินคืนคนละ 1 ether

```
0x787...cabaB (100.9999999999999408844 ether)
0x617...5E7f2 (98.9999999999999448177 ether)
```