

Rock, Water, Air, Paper, Sponge, Scissors, and Fire with Commit-Reveal

This smart contract implements a version of Rock, Water, Air, Paper, Sponge, Scissors, and Fire (RWAPSSF) game on the Ethereum blockchain using the commit-reveal scheme to mitigate front-running and other security issues.

Problem 1 - Front-running problem

Solution:

- Implement commit-reveal scheme:
 - i. Players use the `commitChoice` function to commit their choice by providing a hashed value of their choice and a salt.
 - ii. The contract records the commitment.
 - iii. After both players have committed, they can reveal their choices using the `revealChoice` function.
 - iv. When both players have revealed their choices, the contract checks the winner and pays accordingly.

Problem 2 - Money Locking

Solution:

- Implement a timeout mechanism:
 - i. Record the timestamp when the first player joins to prevent indefinite locking of funds.
 - ii. After a specified time (e.g., 1 day), if both players have not revealed their choices, call a function to handle timeouts.
 - iii. Handle timeouts by returning funds and penalizing non-revealing players.
 - condition is:
 - a. return funds if only player is playing

- b. only 1 person committed, return both player
- c. only 1 person revealed, return pool prize to person that revealed

Problem 3 - Rock, Paper, Scissors => Rock, Water, Air, Paper, Sponge, Scissors, and Fire

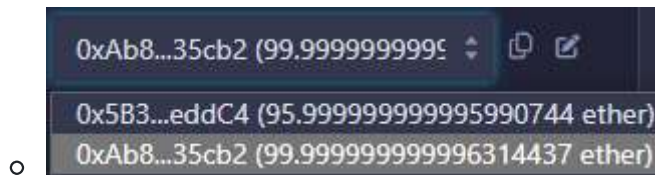
Solution:

1. Add additional choices (0-6) where 7 represents undefined.
2. Modify the `checkWinnerAndPay` function to handle the new choices by comparing them modulo 7.

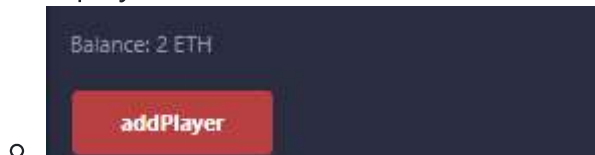
Example Scenarios

1.) Win/Loss

- Start

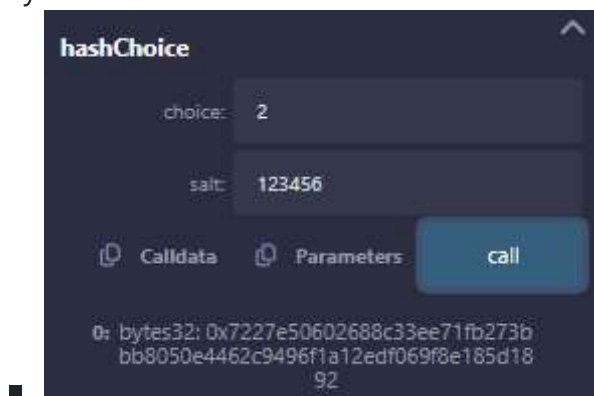


- Add 2 players



- Input

- Player 1



input

choice: 62c9496f1a12edf069f8e185d189d

Calldata Parameters **transact**

○ Player 2

hashChoice

choice: 1

salt: 654321

Calldata Parameters **call**

0: bytes32: 0x3f22648086b143cad07b74d92671461aacc8ae9b6d2891eff48c058da6eacfbcb

input

choice: 0x3f22648086b143cad07b74d926

Calldata Parameters **transact**

• Reveal

revealByUser

choice: 2

salt: 123456

Calldata Parameters **transact**

○

revealByUser

choice: 1

salt: 654321

Calldata Parameters **transact**

○

• After

0xAb8...35cb2 (98.999999999 ether)

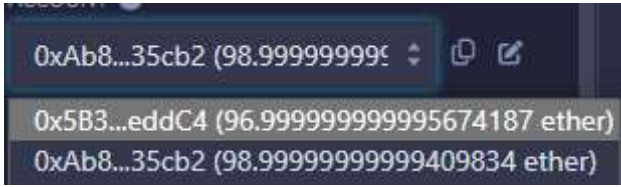
0x5B3...eddC4 (96.99999999995674187 ether)

0xAb8...35cb2 (98.9999999999409834 ether)

○

2.) Draw

- Start

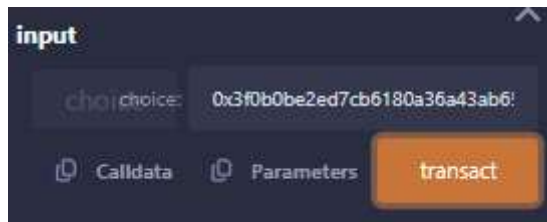
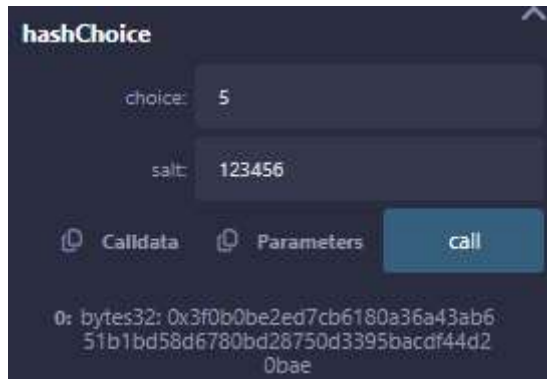


- Add 2 players

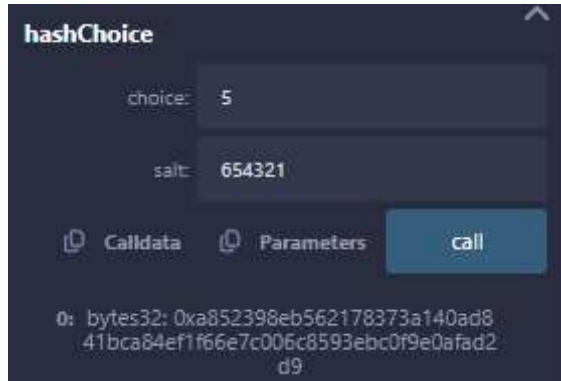


- Input

- Player 1



- Player 2



hashChoice

choice: 5

salt: 654321

Calldata Parameters call

0: bytes32: 0xa852398eb562178373a140ad841bca84ef1f66e7c006c8593ebc0f9e0afad2d9

- Reveal

revealByUser

choice: 5

salt: 123456

Calldata Parameters transact

revealByUser

choice: 5

salt: 654321

Calldata Parameters transact

- After

0xAb8...35cb2 (98.99999999 ether)

0x5B3...eddC4 (96.9999999999994057346 ether)

0xAb8...35cb2 (98.9999999999993847668 ether)