README_1.md

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

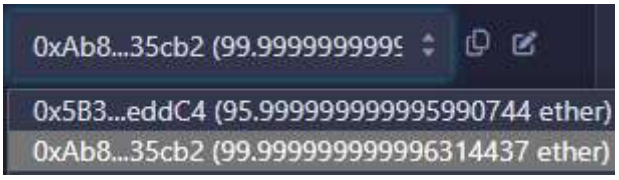
Problem 3 - Rock, Paper, Scissors => Rock, Water, Air, Paper, Sponge, Scissors, and Fire

Solution:

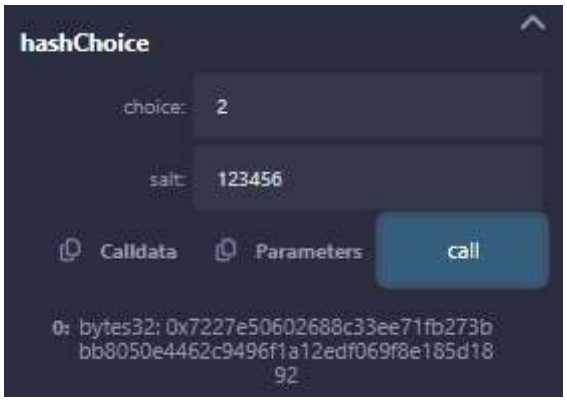
1. Add additional choices (0-6) where 7 represents undefined.
2. Modify the `checkWinnerAndPay` function to handle the new choices by comparing them modulo 7.

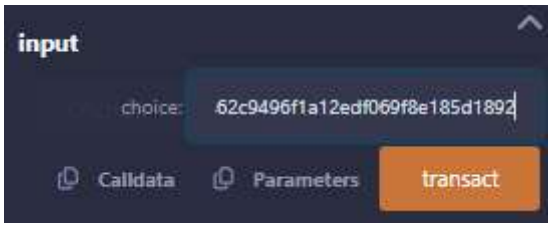
Example Scenarios

1.) Win/Loss

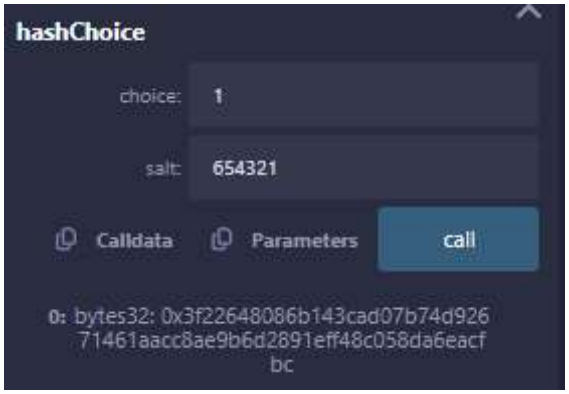
- Start
  - 

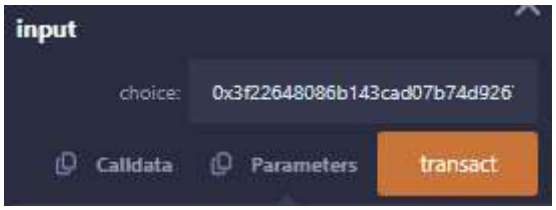
- Add 2 players
  - 

- Input
  - Player 1
    - 

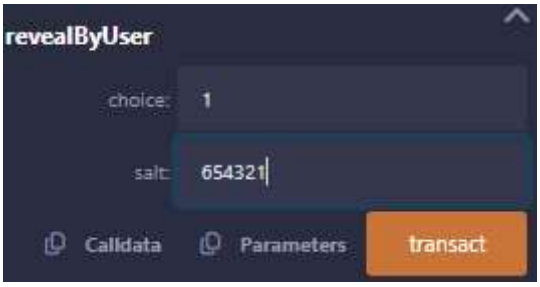


- Player 2

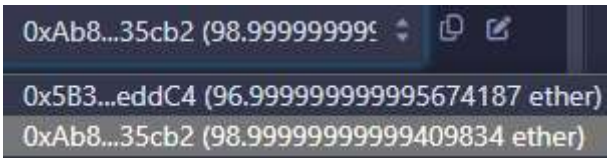




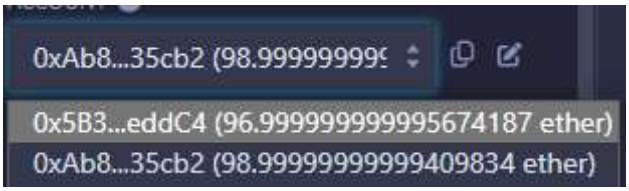
- Reveal



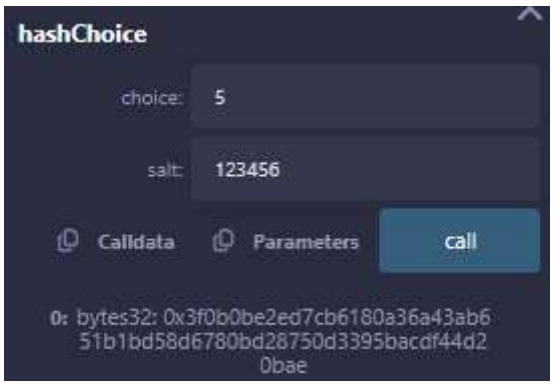
- After

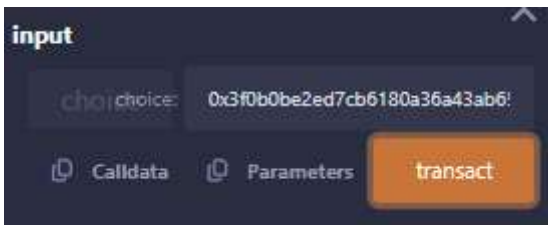


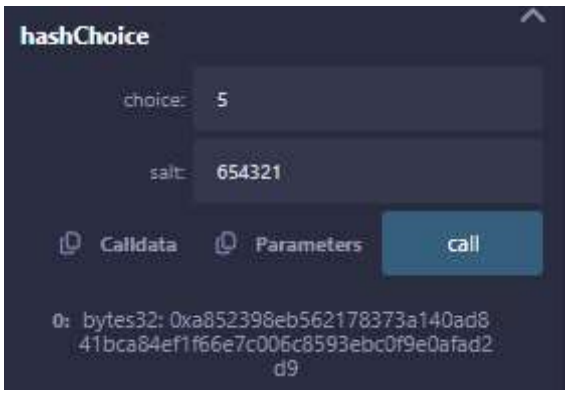
2.) Draw

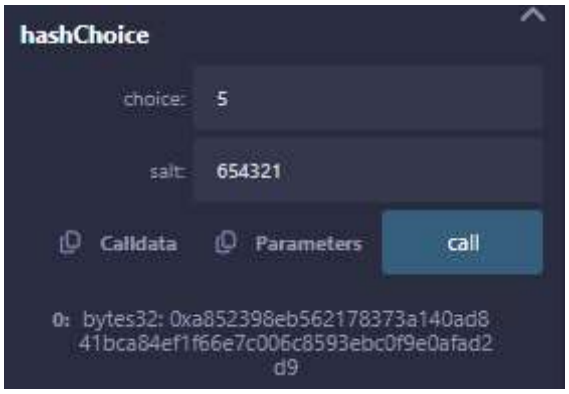
- Start
  - 

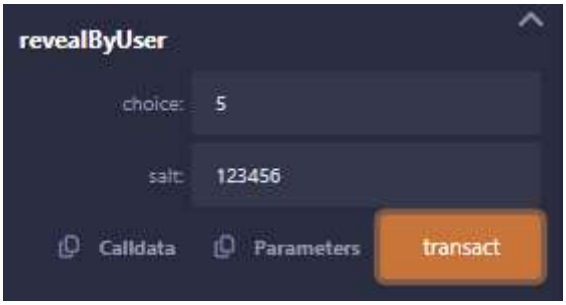
- Add 2 players
  - 

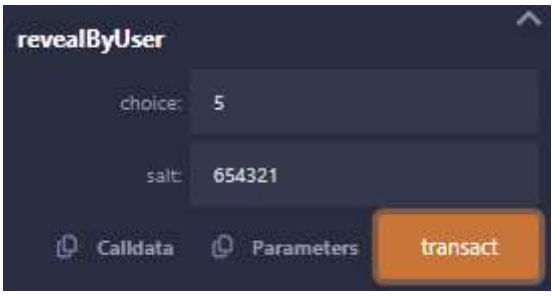
- Input
  - Player 1
    - 

    - 

  - Player 2
    - 



- Reveal
  - 

  - 

- After
  -