RPS

Github

Github

How to play

1. Click on `addPlayer` to register and pay `PRICE` to contract
2. Think about choice and salt then call `getChoiceHash` push the choice and salt as arguments to function. It will return the bytes hash for next step.
3. Transact `input` with your hash and your idx that you got from first step.
4. Waiting another player commit the hash
5. Reveal your hash, transact `revealRequest` push your salt,choices and idx as arguments to function.
6. Waiting your income ^_^

Security

Front Runner

Fixed with the Commit-Reveal strategy by player must hash his/her choice with salt then commit his/her hash to contract another player can't know about choice that player selected. When two players have selected completely, Two players will reveal his choice and compare their choices.

Timeout

No another player join the contract

In `addPlayer` contract give 5 minutes to waiting another player join but if no player join to contract, player can refund his/her money from the contract to his/her pocket.

Player decision for long time

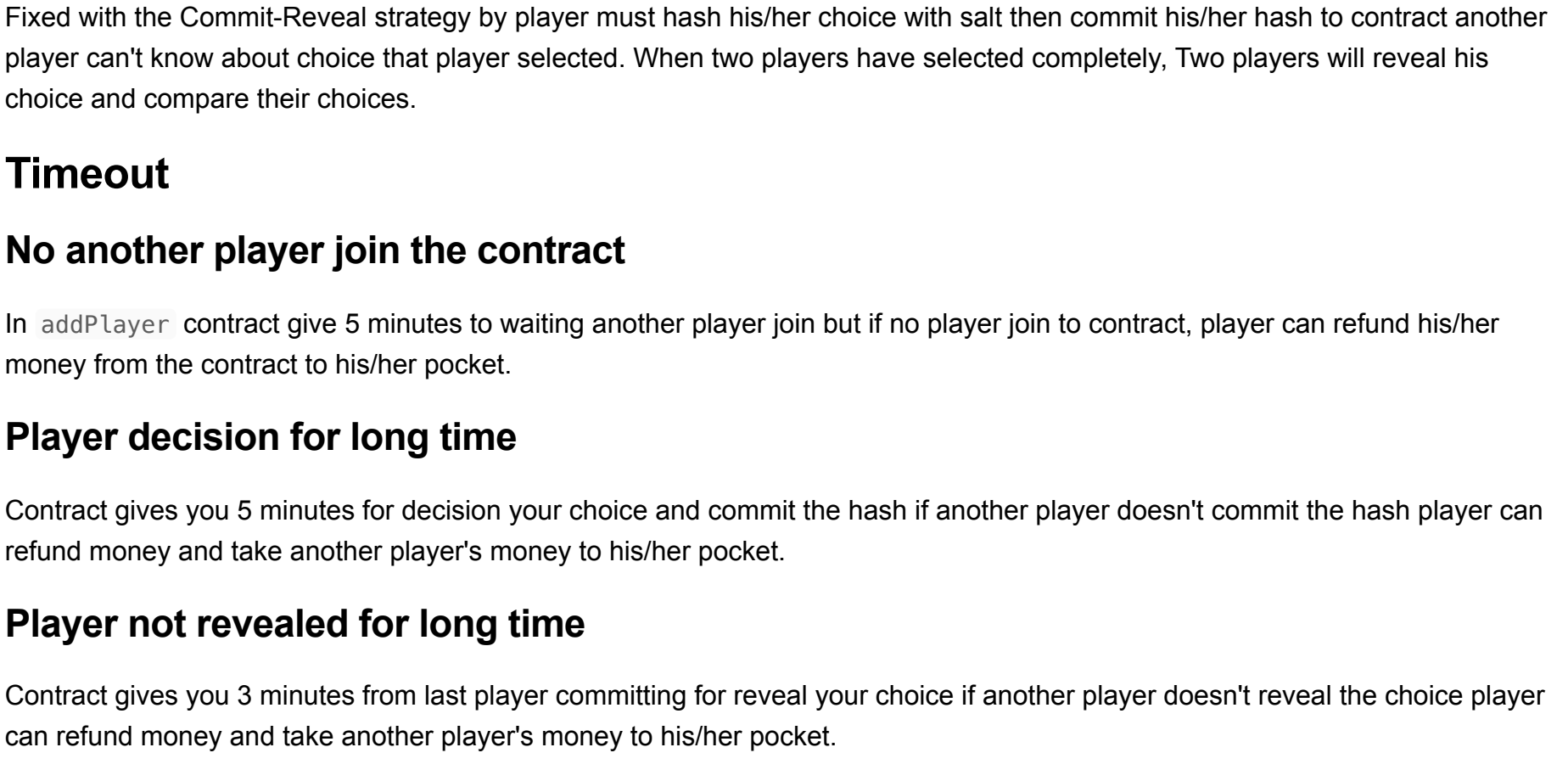
Contract gives you 5 minutes for decision your choice and commit the hash if another player doesn't commit the hash player can refund money and take another player's money to his/her pocket.

Player not revealed for long time

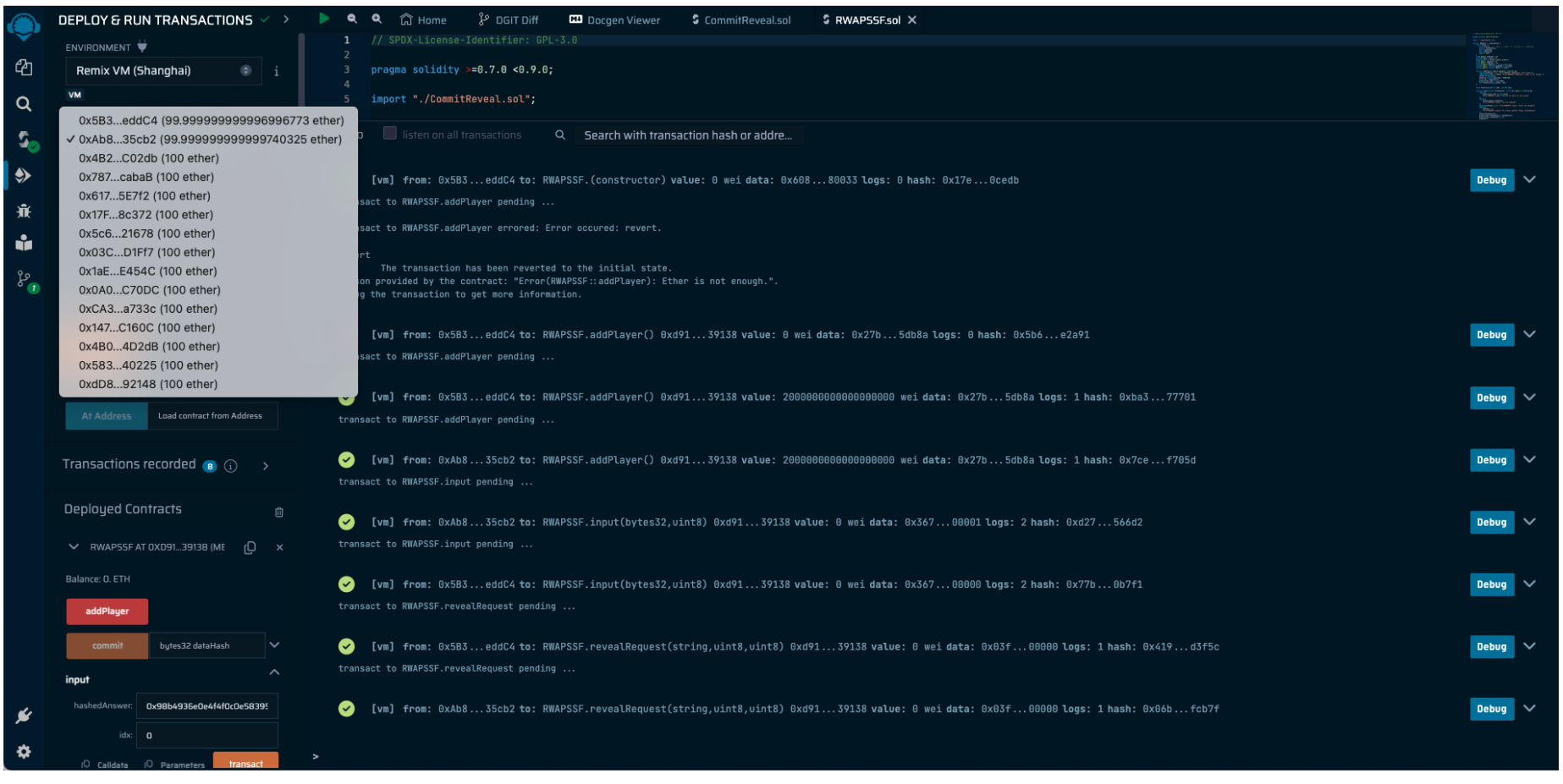
Contract gives you 3 minutes from last player committing for reveal your choice if another player doesn't reveal the choice player can refund money and take another player's money to his/her pocket.

Example

Win and Lose



Deal


DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
Remix VM (Shanghai)
VM
0x5B3...eddC4 (99.999999999996996773 ether)
0xAb8...35cb2 (99.999999999999740325 ether)
0x4B2...C02db (100 ether)
0x787...cabaB (100 ether)
0x617...5E7f2 (100 ether)
0x17F...8c372 (100 ether)
0x5c6...21678 (100 ether)
0x03C...D1Ff7 (100 ether)
0x1aE...E454C (100 ether)
0x0A0...C70DC (100 ether)
0xCA3...a733c (100 ether)
0x147...C160C (100 ether)
0x4B0...4D2dB (100 ether)
0x583...40225 (100 ether)
0xdD8...92148 (100 ether)
At Address
Load contract from Address
Transactions recorded 8
Deployed Contracts
RWAPSSF AT 0XD91...39138 (ME
Balance: 0. ETH
addPlayer
commit
bytes32 dataHash
input
hashedAnswer:
0x98b4936e0e4f4f0c0e5839
idx:
0
Calldata
Parameters
transact
Home
DGIT Diff
Docgen Viewer
CommitReveal.sol
RWAPSSF.sol
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.0 <0.9.0;
import "./CommitReveal.sol";
listen on all transactions
Search with transaction hash or addre...
[vm] from: 0x5B3...eddC4 to: RWAPSSF.(constructor) value: 0 wei data: 0x608...80033 logs: 0 hash: 0x17e...0cedb
Debug
transact to RWAPSSF.addPlayer pending ...
transact to RWAPSSF.addPlayer errored: Error occured: revert.
The transaction has been reverted to the initial state.
on provided by the contract: "Error(RWAPSSF::addPlayer): Ether is not enough.".
the transaction to get more information.
[vm] from: 0x5B3...eddC4 to: RWAPSSF.addPlayer() 0xd91...39138 value: 0 wei data: 0x27b...5db8a logs: 0 hash: 0x5b6...e2a91
Debug
transact to RWAPSSF.addPlayer pending ...
[vm] from: 0x5B3...eddC4 to: RWAPSSF.addPlayer() 0xd91...39138 value: 2000000000000000000 wei data: 0x27b...5db8a logs: 1 hash: 0xba3...77701
Debug
transact to RWAPSSF.addPlayer pending ...
[vm] from: 0xAb8...35cb2 to: RWAPSSF.addPlayer() 0xd91...39138 value: 2000000000000000000 wei data: 0x27b...5db8a logs: 1 hash: 0x7ce...f705d
Debug
transact to RWAPSSF.input pending ...
[vm] from: 0xAb8...35cb2 to: RWAPSSF.input(bytes32,uint8) 0xd91...39138 value: 0 wei data: 0x367...00001 logs: 2 hash: 0xd27...566d2
Debug
transact to RWAPSSF.input pending ...
[vm] from: 0x5B3...eddC4 to: RWAPSSF.input(bytes32,uint8) 0xd91...39138 value: 0 wei data: 0x367...00000 logs: 2 hash: 0x77b...0b7f1
Debug
transact to RWAPSSF.revealRequest pending ...
[vm] from: 0x5B3...eddC4 to: RWAPSSF.revealRequest(string,uint8,uint8) 0xd91...39138 value: 0 wei data: 0x03f...00000 logs: 1 hash: 0x419...d3f5c
Debug
transact to RWAPSSF.revealRequest pending ...
[vm] from: 0xAb8...35cb2 to: RWAPSSF.revealRequest(string,uint8,uint8) 0xd91...39138 value: 0 wei data: 0x03f...00000 logs: 1 hash: 0x06b...fcb7f
Debug