

IERG5590 / IEMS5709 (Spring 2020)

Advanced Topics in Blockchain -- Emerging Topics in IE Warm-up Programming Assignment

Introduction

In this programming assignment, you need to implement a smart contract on Solidity that allows two users to play Paper-Rock-Scissors. To ease you from setting up a complicated Ehtereum testing network, we use [Remix](#), an online integrated development environment (IDE) for Solidity.

Requirements

You need to write a small contract that provides the following functionalities:

1. Two players can register for a Paper-Rock-Scissors game.
2. After registration, they can input their choices.
3. Anyone can check who the winner is after the players provided their choice.

Security Issues

You can assume all players are honest. That said, think about what could go wrong otherwise. (*Bonus points*: wherever you thought there is a potential vulnerability/loophole, leave a comment and briefly explain what could possibly go wrong.)

Template

[Here](#) is a template for the smart contract. You need to fill in the code after the TODO comments.

Submission

Submit your code as a `[studentid].txt` file to Blackboard by 1430 on 31 January 2020.

****For students who are not yet enrolled in the Blackboard system by the deadline (*and only those*), please email your code using your institutional account (e.g. link.cuhk.edu.hk) to the TA nk1018[at]ie.cuhk.edu.hk with subject: [5590] Submission of Warm-up Programming Assignment with your name and student ID in the email.**

Questions

If you had any question, please feel free to raise it on the Blackboard system, or email to the TA.

How to Test Your Code

Upon finishing your implementation, you can deploy your code on a web browser and test your contract following these instructions.

3. Switch between different users

Account

Gas limit

Value

1. Select this

RockPaperScissorsSimpleGame - brc

2. Deploy your contract

At Address

Transactions recorded: 1

4. Test your functions

Deployed Contracts

RockPaperScissorsSimpleGame at 0x692...

```
1 pragma solidity >=0.4.22 <0.6.0;
2
3 contract RockPaperScissorsSimpleGame {
4     enum Choice {Rock, Paper, Scissor}
5
6     bool public isDraw;
7     address public winner;
8
9     // TODO: Other member data...
10
11 constructor() public {
12     isDraw = false;
13     // TODO: other initialization
14 }
15
16 function addPlayer() public payable {
17     // TODO: a player register here
18     // Note that a player cannot register twice
19 }
20
21 function input(Choice choice) public {
22     // TODO: a player makes a choice here
23 }
24
25 function winning() public {
26     // TODO:
27     // If the players make the same choice, set isDraw as true.
28     // Otherwise, set winner as the winner's address
29 }
30
31 // TODO: Other helper functions
32 }
33
34 }
```