Group Project: Rock, paper and scissors

Patrick McCorry

Cryptocurrency Class 2022
stonecoldpat@gmail.com

Abstract. Rock, paper and scissors is easy to play in real life, but can it be played via the internet when players cannot watch each other in real time? This coursework explores how to use the *commit and reveal* paradigm to build the game as a smart contract. Remember this is the group project, so your team will be expected to build the game as a smart contract and then present why it is secure during the final class!

1 Rock, paper and scissors.

While the game rock, paper and scissors was first introduced to England around the 1920s, it first originated in China 206-220 AD and it was very popular in Japan[1] as seen in Figure 1.

Fig. 1: Kitsune-ken was a popular Japanese rock–paper–scissors variant. From left to right: The hunter (ryōshi), village head (shōya) and fox (kitsune).

It is a two-round game. Both players must *commit* to their choice (by making a fist), and then both players must *reveal* their choice (by opening their fist). In person, it is an easy game to play. Each player can verify their counterparty isn't cheating by watching them *in real time* during the game. If someone doesn't open their fist in time, we can verify that. If someone changes their choice when

[1] According to wikipedia.

opening their hand, we can verify that. But what if we try to play the game online without a middleman? Can it be built in a way that guarantees the fair exchange of the answers and allows the winner to collect their winnings? In this group project, it is up to you and your team to solve the problem with a smart contract.

2 Group Project

Your team must write a secure smart contract for rock, paper and scissors. You will present it to the class alongside why the smart contract is secure and the lessons learnt.

Forming teams You (alongside your coursemates) will need to form groups of four. Please register your team by Friday with Patrick McCorry.

Building the rock, paper and scissors smart contract We recommend reading this paper[2] to understand how to write secure smart contracts. All smart contract code must be written using Solidity.

Group presentation All teams have 10 minutes for their presentations. We recommend that you focus on the following four topics:

- Why smart contracts and provably fair gaming are worthy of further investigation.
- Why your rock, paper and scissors game is secure.
- The difficulities your team encountered when building the game and future improvements.

Patrick McCorry will have a copy of your smart contract at hand to ensure the presentation matches the submission.

How to distribute tasks? There are several ways to distribute the team's task and this is ultimately left up to you. One recommendation is to let two members of the team build the smart contract, and then the two other members audit the smart contract for correctness. All team members can then contribute to the group pitch.

[2] https://eprint.iacr.org/2015/460.pdf