Dominion in Perun app channel

Blockchain Technology Lab
Group 6: Tim Fischer, Christian Franck, Till Müßig
21. April 2022

Topic Selection

Our group was formed with the idea to implement a game on the perun app channel for the 6CP Blockchain Technology Lab. Instead of the suggested chess game we propose to implement the 2-4 player turn-based deck building card game ***Dominion***.

Dominion

In Dominion, each player draws and activates cards in order to generate money, which can be used to buy better cards and victory points. Basically, there are three resources: Money, actions and buys, as well as three types of cards: action-cards, treasure-cards and victory cards. You start with a bad deck and 5 cards in your hand. In your turn, you can activate one action-card and buy one card from a shared supply. The action-cards can allow you to activate further cards, draw from your deck or purchase more cards.

Technology

We will use the go-perun framework to build an app channel on which the game will run. As a blockchain solution, we will use perun's ethereum backend.

Security

In order to keep the game fair we include the security perspective into the architecture and the implementation of our project. We will try to fix security issues or at least point them out in our report. From a security perspective randomly drawing cards onto a hidden hand will be very interesting.

Challenges

We gathered a set of challenges of this project. During the lab we will elaborate which of them can be realized. We came up with the following list ordered in descending priority.

Basic mechanism The first challenge will be to implement the basic rules for a game of two players. Players should be able to draw, activate and buy cards. Also the game should prevent cheating attempts like double spending or drawing without permission. As an optional goal, we could extend the game for up to 4 players.

Cards Dominion is designed in a modular way. There are over 500 different cards, but a match typically includes only 16 of them. This allows us to begin our implementation with simple cards and extend it with more challenging cards later on.

Randomness The drawing mechanism involves randomness. In order to prevent cheating or draw prediction the randomness seed has to be changed each time a player draws cards. We thought about using some kind of secure a coin-flipping algorithm. Players exchange hashes of a random value as a commitment, then they reveal the hashs' pre-images, Xor those and use the result as seed.

Hidden cards In the original game the player's hand is hidden. This could be realized by not revealing the drawing player's pre-image in the random seed generation process. However, in order to prevent cheating, the player keeps the pre-image until-the end of a round and reveals them afterwards for the opponent to verify he did not manipulate his hand.

UX User experience is not in the focus of this project, so we probably keep it simple as a command-line game. If we got time left, we might represent the game state in some table format or fancy web 3.0 site.

Cards as NFTs The original game sells its cards in expansion packs. The blockchain version could be free to play but sell further cards as NFTs.

We appreciate feedback on our proposal and hope that our topic will be accepted as we all three enjoy playing the card game.

You can contact us via:

till.muessig@stud.tu-darmstadt.de