DARKWINDS

A trading card game on the Ethereum Blockchain

DRAFT

April 24, 2018

1 Introduction

> "I happily played World of Warcraft during 2007-2010, but one day Blizzard removed the damage component from my beloved warlock's Siphon Life spell. I cried myself to sleep, and on that day I realized what horrors centralized services can bring."
>
> —Vitalik Buterin, Creator of Ethereum

Collectible card games have existed in popular demand since decades. After the massification of the Internet, many of them were successfully digitized like *Magic: The Gathering* and *Pokemon* and new ones were created emulating the look and feel of the physical collectibles in form of a multiplayer videogame. However, being of electronic nature, it's physical existence is an entry on a database, and the amount of each card each player owns is a counter inside a central server. Using databases to create trading card games can produce a fun experience at the cost of conceptual problems:

- Only the owner of the software can allow/deny the use of the digital card within it's ecosystem.
- The digital card existence depends on the game systems to be online.
- The game owner can prohibit trading or markets for cards, which is usually enforced.
- The game owner can control the issuance of cards witout transparency to the user.

Thanks to Blockchain technology we can make a trading card game where all cards are stored in a Ethereum smart contract, where players obtain true ownership of the game object and are free to trade in an outside the game program.

By being a blockchain asset, each card will have the following qualities:

- It's securely stored in an Ethereum wallet.
- The owner has exclusive perpetual rights for transfer, trade or sale of the token
- It can be read by other applications, like a mobile wallet for ERC721 tokens.
- It's existence doesn't depend on the availability of the game owner systems.

The smart contract also controls immutable rules on the issuance of cards, including the total limit of cards to be issued and the rarity of card models.

2 About The Game

Darkwinds is an online trading card game where two players confront each other in a sea battle of ships.

Figure 1: Model #19 (Jordmundgander)

3 Anatomy of a Darkwinds card

The data model of every card is a tuple of a **serial number** and a **model id**.

The model determines it's properties in the game, which are:

3.1 Name

The name of the card

3.2 Energy Points

The energy points required to summon the card into played

3.3 Action

An action of rules in the game activated when the card is summoned, if any. Most of the time is an action the player can use against the enemy (Attack 5 points to the enemy of your choice) and in others against both (All cards into play lose 1 point of health).

3.4 Attack Points

The amount of damage the card inflicts on other creatures or the enemy player when attacking. Cards that have damage points are called **Bucaneers** and the others **Spells**

3.5 Defense Points

The amount of damage this card can receive before it's discarded out of the board. Spell cards don't have defense points and are discarded immediately after using.

4 Smart Contracts

Data-wise, each card is a tuple of a serial number and a model id that corresponds to it's attributes in the game. The serial-model tuples are stored on one contract, while there are 100 card models stored on a second contract.

The main contract conforms to all the functions according to the ERC721 [1] standard. Which means it's compatible with most exchanges and wallet software.

Players cannot buy a specific card, but with the payable function called **getBoosterPack** they can get a pack of random ones. The amount of cards returned to the owner is determined by the price of cards, which is set by the contract owner using the **setCardPrice** function.

5 Card Generation

Cards are generated with a KECCAK-256 operation on the last block timestamp with a modulo operation of 50. Every 5 cards we do another 50 modulo operation on a contract nonce in attempt to make a rare card. If the sum of both modulo operations is higher than 50, the card generated is considered rare as they are appear far less often as shown in Figure A.

While it's possible to determine exactly when cards are being released, efforts are probably not practical.

The smart contract stops generating cards when the hard cap of 1,000,000 is reached.

While the smart contract handles the ownership of tokens, game matches occur off-chain, in a webGL website running the Metamask web extension or compatible thin wallets. A game server is responsible for matchmaking between two adversaries, validating the signature of both players, thus verfying the ownership of both player decks. While the official game server will be the only endorsed way of playing Darkwinds, other developers are free to read the ABIs and access players cards to create different game modes, tournaments or applications that connect to the game.

Game servers only require a signed message from the user wallet to verify ownership. The user private keys are never read or stored.

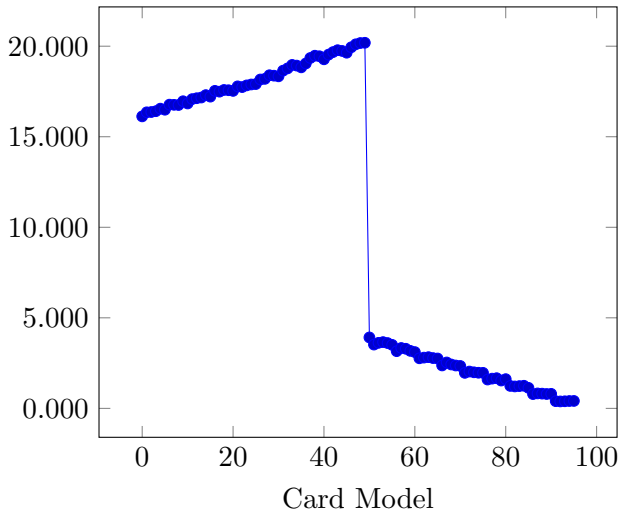

Figure 2: Distribution of 1 million cards estimated by a Monte Carlo simulation

6 Consolidation of game rules

After the ERC721 smart contract is deployed, drafting for a new contract will start. This contract will contain the rules and the extended metadata for each Darkwinds card. This will include the abilites, energy cost, power, resistance and final image.

The process where said contract is drafted will

be called “playtesting” and ends in a final deployment of the game rules on the Blockchain. Estimated date for this event is October 28, 2018. After this date, the game software will read the inventory of each player from contract A and the game rules for each card in contract B.

Players, if desired, can use a different rule contract on unnoficial servers.

References

[1] The ERC721 non-fungible token standard. https://github.com/ethereum/eips/issues/721, Dieter Shirley, 2017.