Dueslist King White Paper

Chiro Hiro - Nicole Ng

***Abstract*—The odds of winning a loot box have remained a mystery since the genesis of gaming and gambling. Distributors have been trying to offer anything but transparency to be able to keep the power to the sellers.**

We would like to present The Duelist King - the very first card game where cards are issued as Non-Fungible Tokens (NFTs) in a fair, transparent and traceable method using an oracle and verifiable Random Number Generator (RNG).

I. Introduction

DUESLIST KING, is the next generation of card game and collectible assets whereby:

- Each card is issued as a Non-Fungible Token *(NFT)*, allowing transferable and auditable ownership for the user
- Scarcity is guaranteed as each card is unique and time-stamped once issued. No other replica or edition of the issued cards will be produced or circulated.
- Card distribution is guaranteed fair, transparent and traceable via blockchain and smart contracts.
- In the future, the community will have voting rights with the specs, volume and type of news cards to be issued.

II. Related Work

SCRAPE: Scalable Randomness Attested by Public Entities [1] is a Decentralized Random Number Generator *(DRNG)* based on Coin Tossing Protocol and Guarantee Output Delivery. IOHK proposes a new way that allows people to generate random number securely. The issue is we would need significant resources to compute a random number and make sure that the result is immutable from adversaries.

A decentralized trustless pseudo-random number generation algorithm [2] is an algorithm proposed by Serguei Popov. This algorithm deals with secret withholding and colluding parties. It is a huge improvement from RANDAO's approach and RNG based on the commit scheme albeit very slow and inefficient for a real application.

III. Our Approach

The commit scheme is initiated by Duelist King Oracle that facilitates high throughput, allowing multiple participants to get involved in the distribution phase.

A. Draw random value

Random value will be generated from system's Cryptographic Random Number Generator (CRNG) by using OpenSSL. This value will be combined with time stamp to make sure that the value is unique and remains unchanged afterwards.

B. Secure Contract Execution

At the beginning of any phase of distribution, the Duelist King Oracle will commit all hashes of random values to a smart contract and these values are immutable and auditable with a cryptographic proof.

Even though Duelist King runs the Oracle, we are unable to manipulate or alter the results or intervene in the process. Our role is purely to make sure that the Oracle runs as per its design.

IV. Computation

Denote:

$\|\|$	String con cat
H	Secured hash function, keccak256
S_i	Secret i^{th} value
t_i	Unix timestamp of i^{th} secret
D_i	$D_i \in \{\forall t_i, \forall S_i \| D_i = H(S_i \| \| t_i)\}$

A. Commit digest of secret

In this step, Duelist King Oracle *(DKO)* will draw random number S_i from system's CRNG.

$$S_i \in \{0,1\}^{192} \tag{1}$$

Then combine S_i *(192 bits)* with current timestamp t_i *(64 bits)* to create an unique secret value. Digest of secret will be calculated and stored by the following algorithm:

1: $D \leftarrow$ blockchain state $[D_0, D_1, ...D_n]$
2: $i \leftarrow$ length of D
3: $S_i \leftarrow \{0,1\}^{192}$
4: $t_i \leftarrow$ *timestamp()*
5: $D_i \leftarrow H(S_i \| \| t_i)$
6: $D \leftarrow D$.*append*(D_i)
7: **return**

These digests will be stored by sequence in a smart contract which was deployed on a public blockchain, no one is able to modify the digest $D_i \in D$ or cheat the smart contract with fake secret.

B. Reveal secret

DKO will observe requests from participants and reveal secret $(S_i \| \| t_i)$ for corresponding to requested digest D_i. The verification could be done by this simple algorithm:

$i \leftarrow$ EVM assignment
$D_i \leftarrow$ blockchain state $\forall D_i \in [D_0, D_1, ...D_n]$
$S_i \leftarrow$ oracle state $\forall S_i \in [S_0, S_1...S_n]$
$t_i \leftarrow$ oracle state $\forall t_i \in [t_0, t_1...t_n]$
if $t_i \geq t_{i-1}$ **and** $H(S_i||t_i) == D_i$ **then**
    return (S_i, t_i)
else
    return *error*
end if

Algorithm is only satisfied if and only if S_i and t_i are the same with the values were used in committed digest D_i and $t_i \geq t_{i-1}$ since D_i is a time series data.

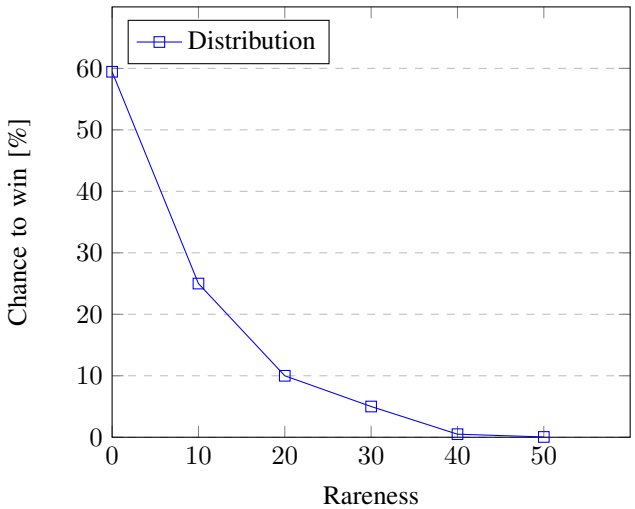
C. Card distribution

At each round of distribution we will issue 20 unique cards. There are 5,000,000 cards in circulation based on its rareness:

Total	Rareness	Symbol	Copies
1	Legendary	L	2,500
2	Special Super Rare	SSR	25,000
3	Super Rare	SR	250,000
4	Rare	R	500,000
5	Uncommon	U	1,250,000
5	Common	C	2,972,500

Subject to the total number of cards that will be distributed based on its rareness, we will be able to calculate the probability of acquiring new cards.

Distribution of card by rareness



Each loot box contains 5 cards that are available for purchase yet the rareness of the cards are randomly assigned. In theory you can get 5 legendary cards in the most ideal scenario since our algorithm won't leave out any possibility.

The probability of acquiring a new card will be adjusted by the algorithm that keeps the fairness in check. Also the probability will be updated and shared real-time to the community to ensure fair and well-informed distribution among the community.

Unsold cards will be transferred to a prize pool as rewards to winners at Duelist King tournaments.

Here is how our algorithm suppose to be:

$i \leftarrow$ EVM assignment
$(S_i, t_i) \leftarrow$ *reveal(i)*
$R \leftarrow$ rareness $\in [L, SSR, S, R, U, C]$
$T \leftarrow$ total of cards
$T_r \leftarrow$ total cards by rareness $\forall r \in R$
$C \leftarrow S_i$
for $c \leftarrow 1$ to 5 **do**
    if $C \mod T \in [T_{r-1}, T_r]$ **then**
        issue(r)
        $T_r \leftarrow T_r - 1$
    end if
    $T \leftarrow T - 1$
    $C \leftarrow H(C)$
end for

D. Verifiability

Ethereum Virtual Machine (EVM) is a Turing complete machine. Its processing is deterministic and audit-able plus its state will be stored on blockchain to make sure the result of Duelist King's Card Distribution remains immune to manipulation and verifiable. As Duelist King owner, we will provide a tool for everyone to verify their transactions and the distribution result.

As with physical card issuance, each card will contain a cryptographic proof that prevents other parties to produce a replica. The only way to transfer the card ownership is via a blockchain transaction.

All smart contracts will be open source and available soon on Github.

V. Conclusion

Duelist King aims to resolve pending challenges to NFT ecosystem such as real life utility of NFTs and transparency in token circulation and operational processes.

By facilitating a fair, transparent and verifiable platform to buy, earn, trade and play with Duelist King cards, we also empower the community to be able to vote, propose initiatives, host tournaments and earn a share in the performance of Duelist King business. We aspire to build Duelist King as one of the leading community-driven and most hollistic gaming platforms in the NFT and blockchain ecosystem.

References

[1] I. Cascudo and B. David, "Scrape: Scalable randomness attested by public entities," Cryptology ePrint Archive, Report 2017/216, 2017, https://eprint.iacr.org/2017/216.
[2] S. Popov, "On a decentralized trustless pseudo-random number generation algorithm," Cryptology ePrint Archive, Report 2016/228, 2016, https://eprint.iacr.org/2016/228.