Kakegurui BRPS

Ballot Rock Paper Scissors Game

V1.0

support@kakegurui.io

Jan 2022

Abstract

This document describes the rules and definitions of the Kakegurui BRPS game and explains the implementation on multiple aspects.

Contents

1. The Origin

Kakegurui - Compulsive Gambler is a Japanese manga series written by Homura Kawamoto and illustrated by Tōru Naomura. The story takes place at Hyakkaou Private Academy, one of Japan's most prestigious schools where, unlike normal schools, the hierarchy is determined by gambling. Yumeko Jabami is a transfer student whose beautiful, innocent façade hides a psychotic addiction to gambling and high-stakes situations. With a keen intellect able to pierce through the elaborate cheating methods used by the most powerful students to rig games in their favor, Yumeko threatens to destroy the twisted hierarchy of the school simply for the thrill of it.

An anime television adaptation by MAPPA aired in Japan from July to September 2017. A second season, titled Kakegurui ××, aired from January to March 2019. The anime series has been licensed and streamed by Netflix outside of Japan.

It is noted that a video game adaptation was released in November 2018, but it became inaccessible after its servers were shut down in March 2020. The game is now reconstructed on blockchains, starting on the scene in the first episode of the anime series: the Ballot Rock Paper Scissors challenge between Mary Saotome and Yumeko Jabami.

For those who have not seen the story before, the two video clips on Netflix's YouTube channel provides a quick presentation of the game:

1) https://youtu.be/iiSXg3zowM4

2) https://youtu.be/8TMibLdjzDQ

2. Introduction of Rules

In general, Kakegurui BRPS is a mutant Rock Paper Scissors game where players can use cards from a ballot pool to win bets and voters can earn by staking over the right card types without risks.

Since all participants are playing remotely on the dApp, the game will look slightly different from the one in the story: the ballots are represented by non-fungible tokens (NFTs), and the ballot box is replaced by a smart contract with three staking slots.

2.1. Basics

Rock Paper Scissors' basic rule is simple: Rock > Scissor > Paper > Rock. The one plays the greater card wins.

According to Kakegurui, two roles are involved with the game – voters and players. The game does not need any sign-up procedure. Instead, a wallet address is the only thing to identify a participant.

2.2. Voters

A voter picks one of the card types (Rock, Paper or Scissor) and stake the ballot NFTs into the card pool which is a slot on the smart contract. Thus, the ballots determine the basic pr obability of the card set.

The number of the ballots is limited by the issuance of the NFTs, but NFT holders are never forced to vote. Therefore, to encourage voting, the economic stimulus is needed: the voters who keep their NFTs in the pool will earn commission from matches.

To strengthen the game theory nature, voters do not evenly earn. As in each match ending with a winner, there must be a 'winning card', the commission of this match will only be rewarded to the voters who sit on this 'winning card' type. The ballots contribute to each voter's weight in revenue distribution.

2.3. Players

There are always two players in one match.

2.3.1. Fetching Cards

Each player must randomly fetch three cards from the ballot pool to form a card set at the beginning. The card sets cannot be changed in the current match.

2.3.2. Bets

The two players must stake the equal bet for the match's bet pool before showing their cards.

2.3.3. Matchmaking

The initiative player (the first player who opens a match) should have the card set and the bet ready so that the follower (the second player who accepts a match) can find the table to play.

If there is not any rival matching within a certain period, the initiative player must retrieve the bet and close the game. No commission will be charged.

2.4. Gameplay

The players select and compare cards, one from one side for one round. If there is a winner, the match ends immediately. If the cards are the same, the match continues to the next round. As each player has three cards, there are three rounds in one match at most. If the third round does not end with a winner, the match turns to be a tie.

2.4.1. Winning

The winner collects all fund from the bet pool of this match, paying commission.

2.4.2. Losing

The loser has nothing to retrieve but is compensated with a chance to mint new ballot NFTs.

2.4.3. Tie

The two players retrieve their funds respectively, paying commission.

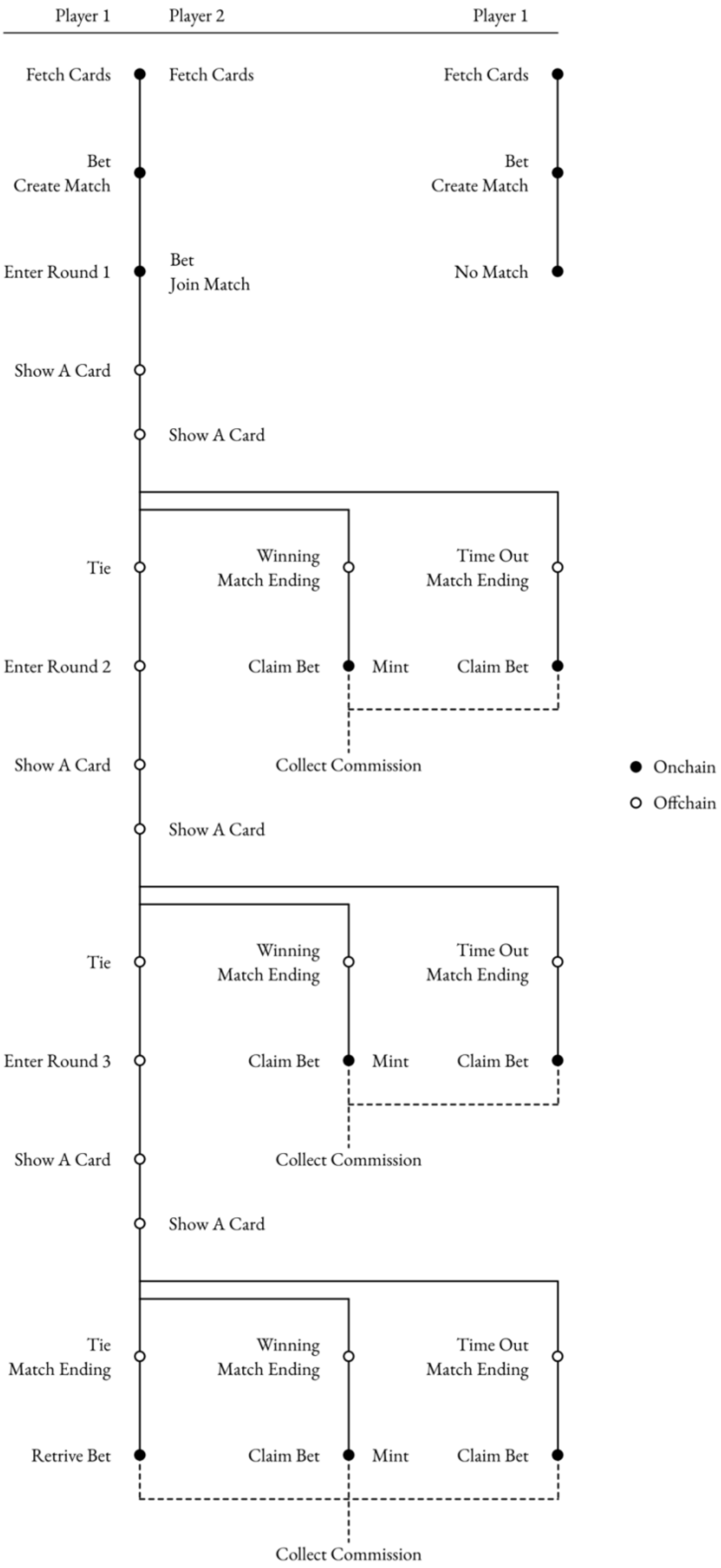
2.4.4. Time-out

During any round, the follower must check the card within a limited period. Otherwise, the match will eventually end turning the follower as a loser compulsively. Such a player will not be compensated with a new minting chance.

Leaving the match is equivalent to pending until time is out, since all the operations are asynchronous.

3. The Implementation

The core gaming progress is made of onchain and offchain parts, illustrated in the diagram.



3.1. Based on ERC1155

In consideration of Gas saving and batch operation demands, the ERC1155 standard is imported to develop the ballot NFTs. Any integral amount of BRPS NFTs can be deposited or withdrawn over the voting contract in a single transaction.

There are two types of BRPS NFTs distinguished by their sources and the weight in the card pool:

1) BRPS Genesis (BG)

   BG is from the initial issuance of ballot NFTs with a limited amount. It has a certain weight in voting and commission collection.

2) BRPS Doge (BD)

   BD is issued only by losers at the end of matches. Its number is unlimited. Its weight is much smaller than BD.

   Players can aggregate their BD minting quota for a batch mint to reduce Gas spending.

By staking BG and BD, the voters determine the fundamental probability of cards for fetching.

3.2. Card Sets

Fetching a card set is the first step to open a match. The generator is the combination of three factors: the fundamental probability, a random number, and the card set generation algorithm.

Fee payment is possibly required depending on the cost of randomness tasks.

3.2.1. The Fundamental Probability

The fundamental probability data is always public and dynamic, shown by the voting contract in three percentage figures. The generator reads such ballot distribution in three slots when fetching is requested.

3.2.2. The Random Number

A random number is used to stimulate a player's fetching interaction over the ballot box. It must hide in the offchain service throughout the match, because if the three factors are all exposed, the card set is known by everyone.

The random number will be uploaded onchain after the match for verification purpose. Regarding the legitimacy issue of the entropy sources, please refer to Section 4.1.

3.2.3. The Generation Algorithm

The generation algorithm is always public and stable. A card set is stored in an ordered array with three elements, e.g. [2, 1, 3] defining a card set: Paper (2), Rock (1), Scissor (3). There are 27 possible arrays to generate:

111	112	113	121	122	123	131	132	133
211	212	213	221	222	223	231	232	233
311	312	313	321	322	323	331	332	333

Below is the function to generate the array taking a random number and the ballot distribution as variables.

```
(1)    Defining three cards:
       $Y_0$, $Y_1$, $Y_2$ in integers ( $1 <= Y_i <= 3$ )
(2)    Acquiring ballot distribution of three card types:
       $X_0$, $X_1$, $X_2$ in integers ( $X_0 + X_1 + X_2 = 100000000$ )
(3)    The entropy source provides a 256-bit number [N] in the big-endian order
(4)    Taking the least significant 64 bits of [N] as [$N_0$] ( $0 <= N_0 <= 2^{64} - 1$ )
(5)    Given $M = 2^{64}$, $M_0 = M * X_0 / 100000000$, $M_1 = M * X_1 / 100000000 + M_0$
       If $0 <= N_0 < M_0$, $Y_0 = 1$
       If $M_0 <= N_0 < M_1$, $Y_0 = 2$
       Else $Y_0 = 3$
       Similarly, right shifting [N] with 64 bits thus taking the new seeds leads
       to $Y_1$ and $Y_2$
```

After generation,

1) any new fetching attempt of this account is suspended by the [account address – card set] locker, unless
   a) a match is finished using this card set.
   b) time exceeds the limit without a bet.
2) an encrypted proof is sent in the transaction onchain for the verification purpose after the match. Please refer to Section 4 to learn more.

3.3. Bet & Matchmaking

After the generation of a card set, bet placement is the key operation to lead the player into a new/existing match.

3.3.1. Bet Placement

Both players must stake the same bet into the pool prior to a match. There are five kinds of position to choose: 1/10/100/1000/10000 (the unit shall be the native token of the network).

For instance, the players choose 10 Ether, so the pool of the match will be 20 Ether in total.

The bet position also determines the loser's BD minting quota at the end of a match.

3.3.2. Matchmaking

When the initiative player stakes the bet, the match is created, assigned with a unique GameID onchain, pending for a rival. The neighbor-matching rule is applied here to assure the most efficient and fair matchmaking, which is: a follower always matches to the latest initiative player who placed the same bet.

For instance, Alice set a bet size at 10 Ether while initiating a new matchmaking space; after a moment, Bob came to set another bet size at 10 Ether, so the smart contact would automatically assign Bob into Alice's match, avoiding creating another 10-Ether-bet match.

A matchmaking space remains open for a certain length.

3.4. Game Session

The card comparing procedure is asynchronous. In other words, the result of a round will not be revealed until the follower shows the card. Series of methods are planted onchain and offchain to prevent Gas wasting, cheating and endless pending during the match.

1) Sit & Check

   The initiative player can call for the first round before the matchmaking is done.

2) No Regret

   Players cannot revert their choices after checking. The backend signs the transaction with the users simultaneously.

3) Countdown

   The follower must check the card. If not, after the time is up, the round will close compulsively with the rival winning.

4) Leave Them Alone

   If both players do not call in a round, the system will not interfere until the contract time exceeds its maximum limit.

5) Gas Payment

   Round 1&2 Ending with A Tie: no onchain transaction.

   Game Ending without Time-out: both players confirm the result onchain.

   Game Ending with Time-out: the existing player (winner) confirms the result onchain.

3.5. Commission Collection

Commission is collected from a match's bet pool at a certain ratio. The commission consists of two equal parts: one half for the voters, one half into the project vault.

For instance, if the commission ratio is 10%, and the bet pool is 20 Ether, the winner can claim 18 Ether while the voters and the vault will collect 1 Ether respectively.

1) Game Ending with A Winner

   The winner claims the funds, leaving the entire commission to the voters and the vault. The voters who stake on the 'winning card' share the gain.

2) Game Ending with A Tie

   The players both claim their funds accordingly, leaving the half commission to the vault. The voters cannot earn from this match due to missing 'winning card'.

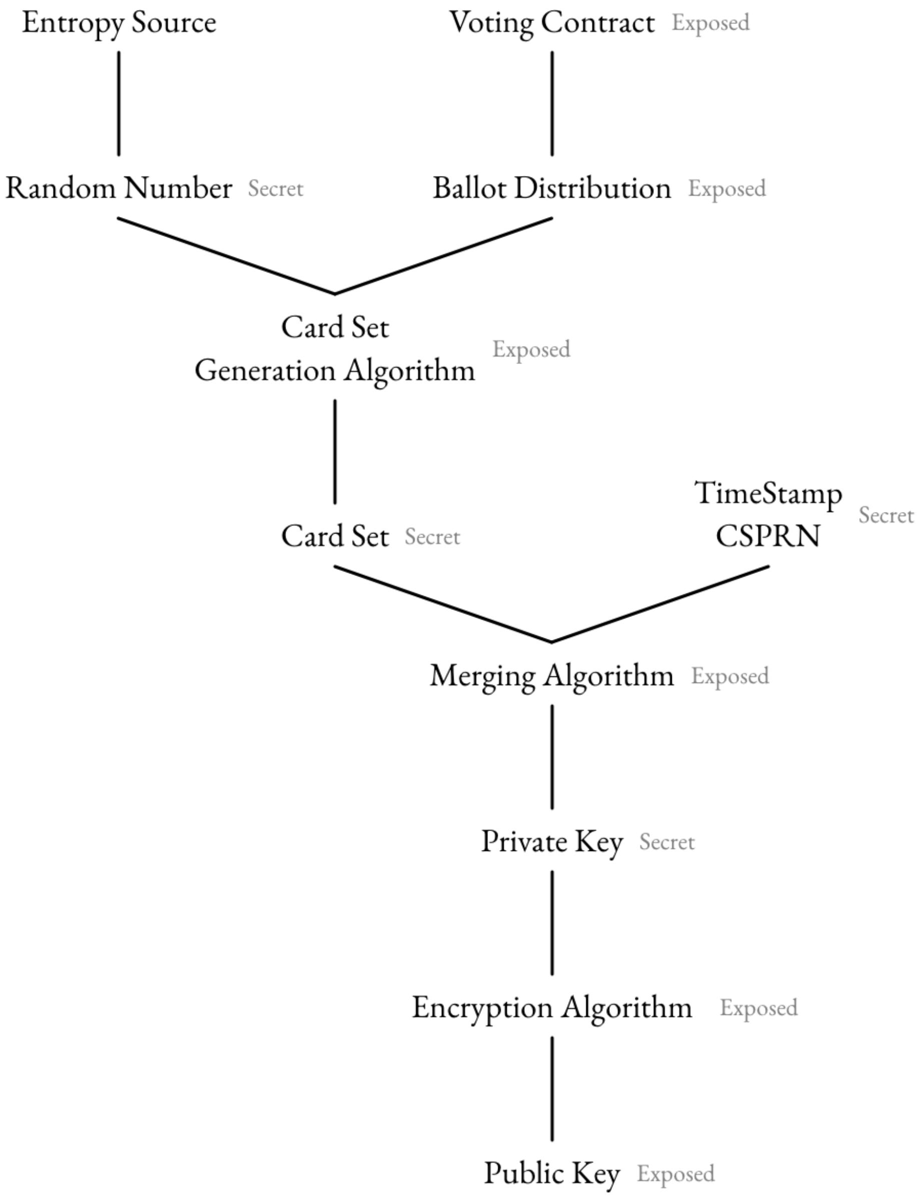
3) No Match

   The initiative player claims the funds, leaving no commission fee as the match never starts.

4. Anti-manipulation Solution

As introduced in Section 3.2, the card sets must remain secret offchain except for the players themselves before the match ends, so do the random numbers, which raises the concern of a manipulation risk by the offchain service. There has to be a way for players to verify their card sets that they have never be altered after generation.

The diagram below exhibits the logic on the card set verification after any match, without exposing card sets during competition.



4.1. Randomness

The BRPS game cannot integrate with onchain randomness since the card sets must be hidden during the matches. The project introduced several entropy sources where random numbers can be acquired safely. They are:

1) Amazon Braket QRNG – using quantum computers to generate random numbers
2) /dev/random & dev/urandom – using Linux default functions to generate random numbers
3) Other backup sources

The methods above are listed according to their priority depending to the availability.

4.2. Merging

There are only 27 types of card sets. The merging algorithm inserts uniqueness into the private key when converted from the card set array. The timestamp of fetching and a CSPRN string is accepted as the variable. Thus, the private key of every card set of every match is unpredictable.

Below is the merging format which merges the data into a 32-byte array, a.k.a. a private key:

```
(1) Defining an array A,
    $A_i$ is the No.i byte of the array
    $A_{i:j}$ is the segment of the array
(2) A0:3 is a player’s card set { R(0), P(1), S(2) }
(3) A3:11 is an 8-byte second-based timestamp in the big-endian order
(4) A11:19 is an 8-byte random string generated by CSPRN
(5) A19:32 is filled with 0
```

4.3. Encryption

The algorithm, Keccak-256, is imported to generate the public key of the merged data. The public key will be instantly published on the blockchain once the card set is fetched, leaving a proof for further verification, while the card set itself remains secret.

Below is how Keccak-256 works:

```
Given a fetching result:
(1) Card set { R(0), P(1), S(2) }
(2) Timestamp of fetching 1643328000 ( 2022-01-28 00:00:00 )
(3) Random String [ eeeeeeeeffffffff ]
The merged private key will be:
0001020000000061f33200eeeeeeeeffffffff00000000000000000000000000
The exposed public key will be:
keccak256('0001020000000061f33200eeeeeeeeffffffff00000000000000000000000000')
Which is cf8df0a82c93cac3919f81223a29d0c614abfdd9d6b2112686ad8a81209ff800
```

4.4. Verification

When a match ends, its secret data will all be exposed on the blockchain, including a pair of random numbers, card sets and private keys from two rivals. The players can verify them all. If:

1) the card sets can be verified by the random numbers

2) the private keys can be verified by the card sets and the timestamps

3) the public keys can be verified by the private keys

Then this match’s card sets are proven to be not tampered.

5. Parameters

According to the game design, there are a few parameters under governance. A native token of the Kakegurui.io project can be introduced for adjustment purpose on these issues (tokenomics are not included in this whitepaper).

Below are the default parameters. Please note that they are subject to changes in future.

1) BRPS(BG)NFT / BRPS(BD)NFT Weight

   BG Weight: 10 BD Weight: 1

2) BRPS(BG)NFT Minting Price & Limit

   Price: 0.1 / BG (native token based) Limit: 10,000 BG / Chain

3) BRPS(BD)NFT Minting Quota against Bet Size

   BD Minting Quota = Bet Size * 1

4) Card Set Generation Fees

   Vary on different chains

5) Commission Ratio

   Default Ratio: 10%

6) No-bet Countdown

   Time Limit: 10 minutes

7) No-match Countdown

   Time Limit: 48 hours

8) Time-out Countdown

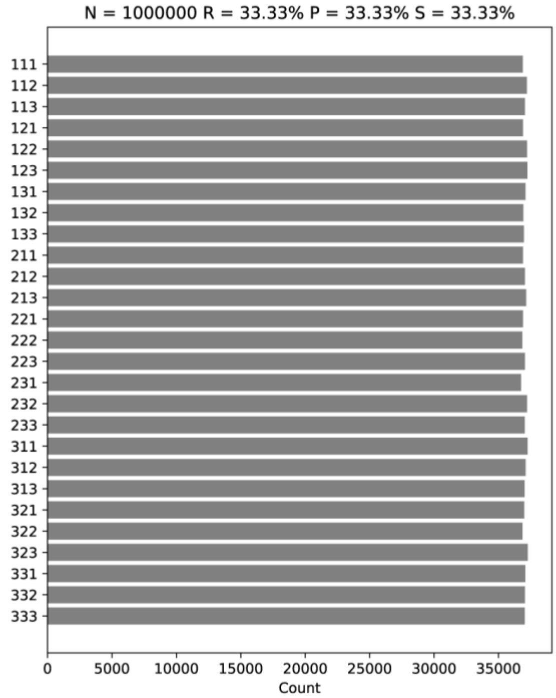
   Time Limit: 24 hours

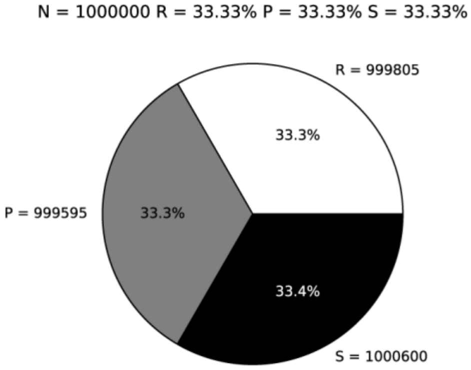
6. Appendix

The tests were performed to examine the reliability of the card set generation algorithm on two aspects:

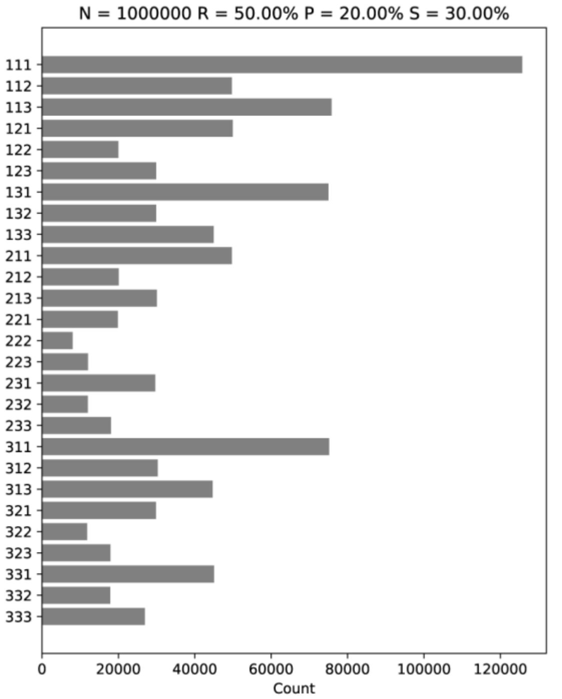
1) Consistency of Distribution – the tests showed that the appearing frequency of the three cards were dominated by the ballot data over the huge number of trials.
2) Effectiveness of Randomness – the tests showed that the appearing frequency of the 27 card sets was random over the huge number of trials.

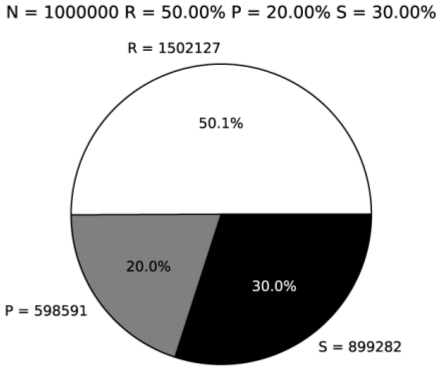
Test I



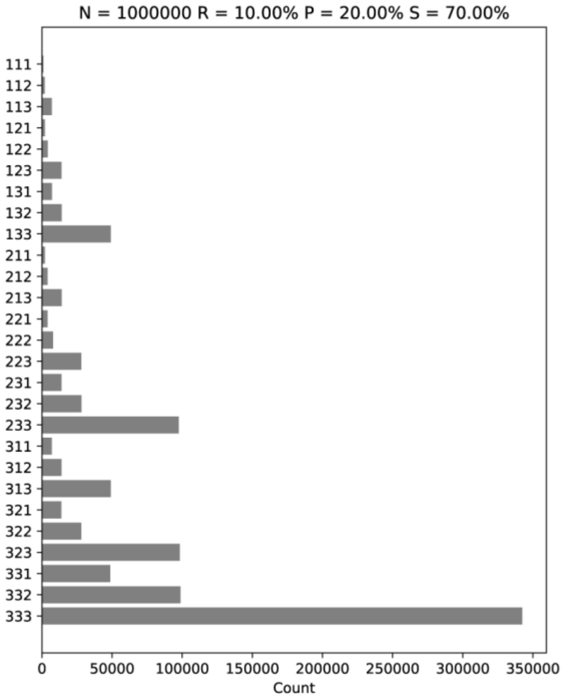


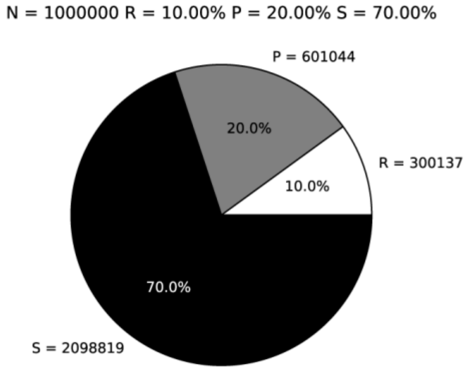
Test II





Test III


N = 1000000 R = 10.00% P = 20.00% S = 70.00%
Count


N = 1000000 R = 10.00% P = 20.00% S = 70.00%
P = 601044
20.0%
R = 300137
10.0%
70.0%
S = 2098819