An Implementation about Provably Fair of Shuffling Cards

1. Introduction

The team of BC.Game[1] originate Shuffling Cards' self-provable fairness solution through the platform games Crash[2] and Hashdice[3].
We will implement this shuffling program in BlackJack[4] .The verifiable logic is as follows:

First of all, we use a future hash of a block in BTC as a [Salt] and publish it in the community.
The game uses asymmetric encryption RSASSA-PKCS1-v1_5 mode.
The server has the [Privatekey] and announce the [Publickey].

1. Encrypt the [Issue] and [Salt] with HmacSHA256 to get [Hash].
2. Sign [Hash] with the [Privatekey] to get the [Seed].
3. Using the [Seed] to shuffle cards.
4. [Seed] is announced after the end of game.
5. The client can use the [Publickey] to verify the signature.

2. Logic of shuffling cards

【 I 】Logic of shuffling single deck of cards

Import [Seed] for shuffling card .
The shuffling steps are as follows:

1. Create a deck of cards called β , the initial sequence is Spade A-K Heart A-K Clubs A-K Dianmond A-K.
2. Seed generates hash [$Hash_{spadeA}$] through Sha256 algorithm, and [$Hash_{spadeA}$] is the weight of the first card (Spade A) in the card β .
3. Transfer the last character of the hash to the first character of the hash as the weight of the second card (Spade 2).
4. The rest can be done in the same manner until the last card Dianmond K .
5. Sorting the cards according to the corresponding weights from small to large.
6. Finally, getting a new card order.

Shuffling done.

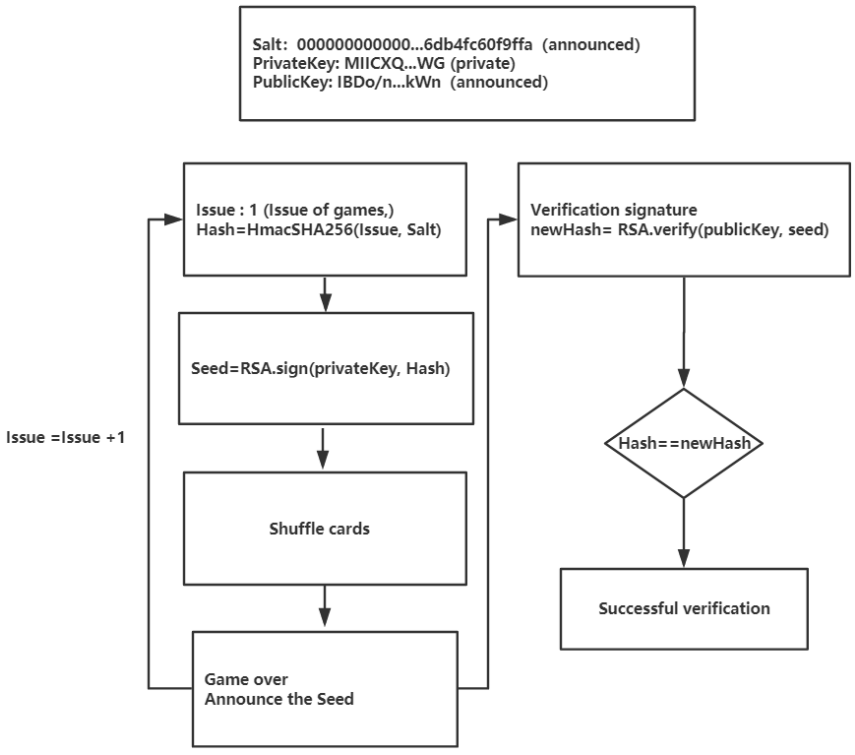
【Ⅱ】 Logic of shuffling multiple decks

Import [Seed] for shuffling card
The shuffling steps are as follows:

1. First shuffle the first deck of cards and perform steps 1-4 of【Ⅰ】.
2. The seed of the second deck is the hash generated by the seed of the first deck, repeating steps 1-4 of【Ⅰ】.
3. The seed of the third deck is the hash generated by the seed of the second deck, repeating steps 1-4 of【Ⅰ】.
4. The rest can be done in the same manner until all the decks have been shuffled.
5. Put all the cards together to perform the steps 5-6 of 【Ⅰ】at last.

Shuffling done

3. Simple flow chart



4. Note:

[1] https://bitcointalk.org/index.php?topic=5088875.0

[2] https://bc.game/atm

[3] https://bc.game/roll

[4] https://bc.game/blackjack