

Algorithm of Self-provable Fairness Blockchain Blackjack

1. Introduction

The team of BCGame^[1] originate blackjack's self-provable fairness solution through the platform games Crash^[2] and Hashdice^[3].

We use hash [Hash_{eos}] of EOS's future N^[4]th block as a random factor plus server seed [Seed_{server}] as the seed of this game [Seed_{game}]. Because the future block hash of EOS block is not controlled by anyone, [Seed_{game}] is also uncontrollable.

We will show the hash [Hash_{server}] of the server seed [Seed_{server}] in advance as verification before the start of the game.

2. Logic of shuffling cards

【 I 】 Logic of shuffling single deck of cards

Import [Seed_{game}] for shuffling card (Seed_{game} = Hash_{eos} + Seed_{server})

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. Seedgame 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

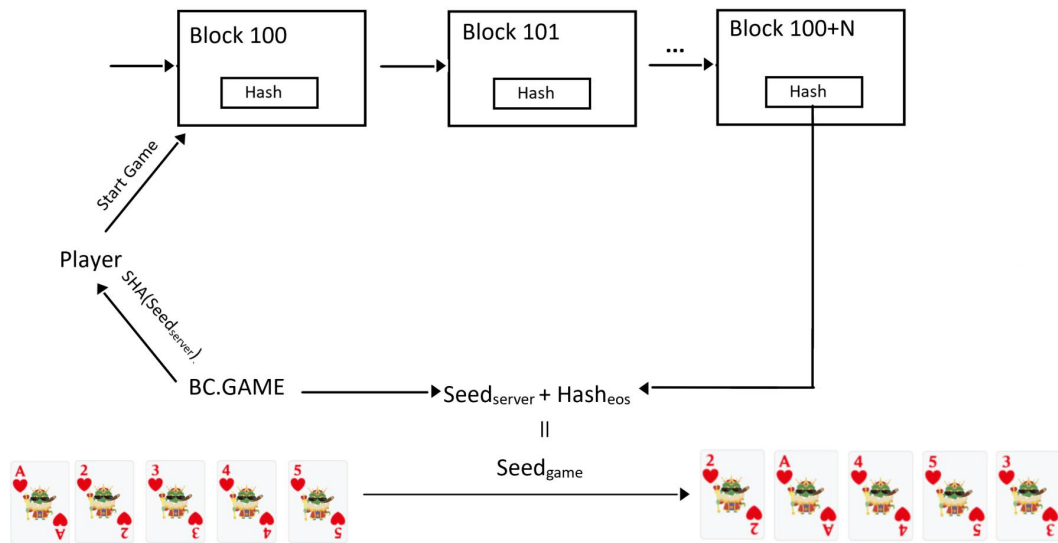
Import [Seed_{game}] for shuffling card (Seed_{game} = Hash_{eos} + Seed_{server})

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>