Random

Introduction

This specification describes the usage and scope of random numbers on IRIShub. This feature is currently in beta and please assess the risk yourself before using.

Concepts

Currently, IRIShub provides two random number generation methods: PRNG and TRNG.

Scope

Applicable to the application layer to obtain random numbers generated based on blockchain, such as gaming, games, etc.Not Applicable to private keys, blockchain consensus algorithms, etc.

PRNG

A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. -- Wikipedia

We use the multiple indicators generated by the blockchain as "factors" to calculate the random number, making this random number transparent and convenient for verification;

The random number "factor" specifically includes the following indicators:

- Last Block Hash
- : The generation of Block Hash depends on various factors of the block, such as block height, number of transactions, timestamp, etc., so the block Hash itself has certain unpredictability.
- Current Block Timestamp
- : The block timestamp uses the BFT time, that is, the weighted calculated distributed timestamp (millisecond level), based on the validator's weight, using the time of each Precommit in the previous block, also certain unpredictability [BFT Timeopen in new window
-].
- Consumer Address
- : mainly to achieve different random numbers for different people at the same block height.

Since the calculation of block Hash and BFT time is based on the information of the previous block, in order to avoid pre-calculating the result before requesting the random number, on the other hand, we strengthen the unpredictability of the random number through the "future block".

However, unpredictable does not mean that it is unmanipulable. For example, a new block proposer can selectively package transactions and accept Precommits to affect block Hash and BFT time.

Calculation Formula

seed= sha256(Int(timestamp) + Int(sha256(blockhash)) / Int(timestamp) + Int(sha256(consumer)) / Int(timestamp))
rand= seed mod10 ^20 /10 ^20

TRNG

A hardware random number generator (HRNG) or true random number generator (TRNG) is a device that generates random numbers from a physical process, rather than by means of an algorithm. -- Wikipedia

On the basis of PRNG, the external random number factorOracle Seed is introduced using the oracle machine method, implemented through IRIShub Service.

The random number "factor" specifically includes the following indicators:

- Last Block Hash
- : Same as PRNG.
- Current Block Timestamp
- : Same as PRNG.
- Consumer Address
- : Same as PRNG.
- Oracle Seed
- : The user requests a random number. After the specified block is reached, the system sends a service request. The reliable random number provider returns the Oracle Seed generated by the true random source.

TRNG introduces an external source of true randomness, eliminates the risk that block proposers manipulate random number generation in PRNG..

#

Calculation Formula

seed= sha256(Int(timestamp) + Int(sha256(blockhash)) / Int(timestamp) + Int(sha256(consumer)) / Int(timestamp) + Int(sha256(oracleSeed)) / Int(timestamp)) rand= seed mod10 ^20 /10 ^20

#

Actions

- Request Random Number
- Query Random Number
- Query Random Queue