Nekoyume: Decentralized MMORPG

Abstract: Nekoyume is a decentralized MMORPG based on the blockchain. A large number of users can hunt monsters in the virtual world to gain experience, collect essential items from the adventure, and become stronger. The action information of the game is recorded in a blockchain so that a large number of users can participate without a centralized server. We have designed a separate random consensus called Hash random so that the game can be implemented on the blockchain. Hash random is a random consensus that is difficult to be predicted by combining the block hash which is created by the proof of work and the hash value of the individual action, minimizes the intentions of specific stakeholders, and is deterministic by each behavior.

Nekoyume: Decentralized MMORPG **1**
1. Background 2
2. Pseudo-random number generation (PRNG) 2
    2.1. Random generation using block values 3
3. Hash Random 4
    3.1. Combination of behavior information hash and block hash 4
    3.2. Behavior information that can be included in a block Time limit 4
4. Decentralized MMORPG 5
5. Economic Structure 6
    5.1. Adventurer 6
        5.1.1. Moves 6
    5.2. Cat 8
        5.2.1. Block generation consensus 8
        5.2.2. Compensation system 8
6. Limitations 9
    6.1. Limitation of Hash Random 9
    6.2. Proof of Work 9
7. Conclusion 9

1. Background

The bitcoin proposed by Satoshi Nakamoto introduced the concept of blockchain using techniques such as digital signature, hashing, and proof of work. The blockchain has shown that the decentralized main net is stable for nine years and that anyone can participate in creating a trustworthy virtual currency.[1] The vision of this trusted technology has inspired many software projects.

Now, the blockchain is being used in various places beyond cryptocurrency. Vitalik Buterin further developed bitcoin script to suggest Ethereum, a decentralized application platform based on Turing complete Smart Contract. [2] When we were able to create a variety of applications in the blockchain, attempts were made to make games. In particular, CryptoKitties, which can send and receive randomly generated cats, has shown an enthusiastic response so that Ethereum network showed temporary paralysis. [3] However, since the use of random on the blockchain is very limited, there are restrictions on the games that can be implemented at present. If a more general-purpose random number generation approach is proposed, we will be able to develop more kinds of game applications.

2. Pseudo-random number generation (PRNG)

Blockchain has the limitation that the data on the chain and its execution result must be deterministic because of the nature of everyone sharing the ledger and same effect. In other words, if you use a typical random value in an application on a blockchain, you will not be able to do it at all, because everyone can see different values based on the same data. However, many favorite games, including Tetris, have random elements, so implementing games on a blockchain without any restrictions is a significant limitation.

---

[1] https://bitcoin.org/bitcoin.pdf
[2] https://github.com/ethereum/wiki/wiki/%5BKorean%5D-White-Paper
[3] https://www.dropbox.com/s/a5h3zso545wuqkm/CryptoKitties_WhitePapurr_V2.pdf?dl=0

Therefore, there have been studies on pseudo-random number generation (PRNG) on blockchains to make blockchains more universal.

2.1. Random generation using block values

This strategy is simple to implement randomly, but since the miner can edit all the block variables, Therefore, it is not suitable for a blockchain where a miner and a user can be the same person. [4]

2.2. Random generation using external services

Random generation using external services allows you to hide the way the random is created completely, but because it is not a decentralized way, There is a trust issue.[5] Thus, the currently proposed random generation method has the disadvantage that it can intentionally intervene in a particular group. Just as dealers should not manipulate odds at a casino, randomness must be fairly created by minimizing the likelihood of intentional involvement of specific interest. To solve this problem, Nekoyume suggests a random generation method called Hash random.

[4] https://etherscan.io/address/0xa11e4ed59dc94e69612f3111942626ed513cb172#code
[5] http://www.oraclize.it/

3. Hash Random

Hash random is a random consensus presented by Nekoyume. Hash Random has designed to prevent stakeholders from attempting to make an intentional number, or even to try to do so, in a way that would be detrimental to interests. To this end, we present two fundamental concepts.

3.1. Combination of behavior information hash and block hash

The hash value derived from the user's behavior information contains the signature of the user, so the miner can not intentionally transform it. The block hash is a value that the miner creates, so the user can not deliberately intervene. Using the values of the two hash values XORed as a random seed, (1) the user cannot intervene on random values, and (2) all user actions in one block can be based on individual random seeds.

3.2. Behavior information that can be included in a block Time limit

Even if a combination of behavior information hash and block hash is used as a random seed, a miner can intentionally try to generate a favorable hash based on the behavior information of a user. To check this, the behavior information creation time that can be included in the block is limited to 10 times the maximum block creation time. A miner can spend more time than other miners to find a hash that has a good combination of specific behavioral information, but you must take the following damage.

- The miners will have a disadvantageous position in the competition of hash compensation.
- The process of intentionally looking for profitable blocks is longer because you need to receive new behavior information periodically.

4. Decentralized MMORPG

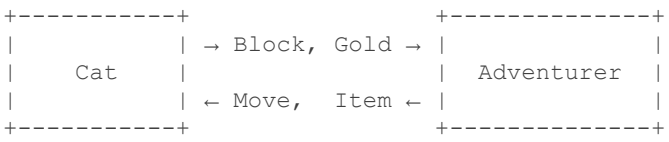
Nekoyume is a massively multiplayer online role-playing game (MMORPG) based on blockchain which is the first to apply the concept of Hash random. Participants become adventurers who can venture and trade in the world of games, or become cats who can navigate blocks that are key to the game's progress.

Because Nekoyume is an MMORPG based on a blockchain, there is no centralized server for a particular subject. This has the following advantages.

1. The centralized service operated by a specific entity has the possibility that the service cannot be run continuously depending on the profitability of the game. A blockchain-based game can continue the game if there are at least one participant left.
2. Because of the business intention of the operating entity, the fun factor of the game does not change greatly according to the profitability of the operating entity. The change in gaming is determined by the careful discussion of the participant-oriented community so that many of the participants can properly develop the fun elements of the desired game.
3. While centralized services have an economic advantage to the service operator, blockchain-based games are distributed according to the agreed token economic model.

5. Economic Structure

Here is a simple diagram of the elements that Nekoyume's cats and adventurers share.



5.1. Adventurer

Adventurers can set their own jobs, take an adventure, grow items and experience, and grow stronger.

5.1.1. Moves

You can perform the following actions.

- ⚔ Hack and Slash: Combats monsters from the current area.
- 💉 Sleep: Takes asleep and regains physical strength.
- 🆙 Level Up: Raises the level to improve your ability.
- 🗣 Conversation: I want to say something.

When you move, the behavior information is passed to the network, and the move is actually performed when the next block is created. Since the block creation cycle is about 15 seconds, and one block cannot contain two actions per user, the minimum action cycle is also about 15 seconds.

When the block creation is complete, the behavior contained in that block is evaluated. In the evaluation, the random value determined by the Hash random is reflected in the behavior result, and the process of creating the random value by the Hash random is as follows.

```
>>> move.hash
'42ff1bb9d4149463474a9c84cb1f580e3d78176038646d7bd66b135fa34bc739'

>>> move.block.hash
'0000009d0d9bdd3fdfcd5a39d6313c6454653d881a3a59068c8a026ddf4f5803'

>>> randoms = [ord(a) ^ ord(b) for a, b in zip(move.block.hash, move.id)]
[4, 2, 86, 86, 1, 82, 91, 93, ... 3, 10]

>>> randoms = randoms[int(move.block.difficulty / 4):]
[1, 82, 91, 93, ... 3, 10]
```

Adventurers can acquire various items through the adventure. However, since gold is only available through transactions, you have to grow through adventure and obtain good things through a battle with stronger monsters, so you receive a lot of gold in the market.

The life cycle of the adventurer adopted the Dungeon World rule. Dungeon World is a fantasy TRPG rule based on Apocalypse World Engine and Dungeons & Dragons by Sage LaTorra and Adam Koebel. Since Dungeon World inherits the characteristics of TRPG, where player interactions are very important, it is suitable for the characteristics of a blockchain involving multiple users, and since all of the user's actions are designed to be judged by rolling a hexahedral dice twice, we determined that it is suitable to use random element.

5.2. Cat

Cat is the same as the miner in the bitcoin. When the adventurer's move information comes in, the cat shares the move information with the other cats and explores blocks that package the move information.

5.2.1. Block generation consensus

Nekoyume has adopted the hashcash as a key consensus because it uses the Hash random require proof the work. Since the block generation cycle is aimed at 15 seconds, if the average of the recent block generation time is lower than 15 seconds, the demanding difficulty increases. Conversely, if it is higher than 15 seconds, the hard difficulty becomes lower.

5.2.2. Compensation system

Once you have completed the block search, you can receive gold for the miner's compensation. Gold rewards are initially awarded 16 gold per block, decrease to half every four years, and will be fixed at one gold per block after 16 years.

Total miner & client incentive / 4y	Reward gold per block
134,553,600	16
67,276,800	8
33,638,400	4
16,819,200	2
8,409,600	1

6. Limitations

Hash random is a random consensus that minimizes stakeholder intervention on the blockchain but has the following limitations.

6.1. Limitation of Hash Random

Hash random has removed random room for user intervention and added constraints on random intervention so that the proof of work, which does not intentionally involve random results in relation to the miner, can be the biggest benefit. However, if the benefit offered by the random in the game is a reward large enough to ignore this structural damage, the miner can attempt to create a deliberate hash considering the constraints. Therefore, even if you use Hash random, it is necessary to design the system so that excessive compensation is not made at random.

6.2. Proof of Work

Hash random is designed on the assumption that it should be used with proof of work. The use of Hash random is not appropriate if the ecosystems using proof of stake or other consensus methods because some stakeholders can easily intervene at random.

7. Conclusion

Nekoyume proposed a new random consensus called Hash random and implemented it by bringing the existing bitcoin and ethereum consensus system to make decentralized MMORPG. In this article, we have summarized the difference between the random generation method and the Hash random in the existing blockchain, and we looked at how Nekoyume is being developed. The Hash random should be worked with the proof of work consensus, and it will work as intended, so even if you use Hash random, you don't have to make too much compensation in the ecosystem by random values.